I recenti sviluppi nel processo di riconoscimento della "privacy digitale" come diritto umano fondamentale[1]

Valentina Maria Ariemme[2]

1. Le nuove frontiere del diritto alla privacy nel ventunesimo secolo. Il concetto di "privacy digitale"

Il riconoscimento della *privacy* fra i diritti umani fondamentali risale ormai a molti anni fa, insieme al riconoscimento della necessità di proteggerla contro violazioni esterne[3].

Ad ogni modo, il diritto alla privacy ha attratto nuova attenzione nel 2013, quando l'utilizzo improprio di dati sensibili, l'attività di spionaggio internazionale e la diffusione non autorizzata di informazioni hanno richiamato l'interesse dei mezzi di comunicazione e suscitato controversie politiche in numerosi Paesi del mondo.

Questi eventi hanno evidenziato i nuovi rischi a cui è esposta la privacy nell'era di Internet, ed hanno determinato una forte reazione dell'opinione pubblica a livello politico sia nazionale che internazionale.

Uno dei dibattiti più importanti ha avuto luogo in sede ONU, con uno scambio di opinioni fra l'Alto Commissario per i Diritti Umani (Navanethem Pillay) e gli Stati Membri, le organizzazioni internazionali e regionali, e le organizzazioni per la tutela dei diritti umani[4].

---

[1] Come citare questo articolo: V.M. Ariemme, I recenti sviluppi nel processo di riconoscimento della "privacy digitale" come diritto umano fondamentale, in *Studi Tributari Europei*, n. 2/2014 (www.seast.it/rivista), pagg. 86-91.

[2] Valentina Maria Ariemme, Dottoranda di ricerca in Diritto Tributario Europeo presso l'Università di Bologna.

[3] La Dichiarazione Universale del Diritti dell'Uomo, proclamata dall'Assemblea Generale dell'ONU in data 10 dicembre 1948, nell'articolo 12 stabilisce che: "*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione*". Di nuovo, ancora di provenienza ONU, ma di circa vent'anni più recente (dicembre 1966) la Convenzione Internazionale sui Diritti Civili e Politici, all'articolo 17, ribadisce la stessa definizione di privacy, con l'aggiunta, nel comma 2, che "*Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*".
Si vedano il testo completo della Dichiarazione ed il sito internet dell'Alto Commissario per i Diritti Umani..

[4] Tutti i principali documenti sono rinvenibili sul sito internet dell'ONU, si veda, in particolare, la risoluzione adottata dall'Assemblea Generale in data 18 dicembre 2013, n. 68/167. Il

Il report finale del Commissario è stato pubblicato in data 30 giugno 2014 e ha fornito una visione generale delle problematiche principali.

Il punto di partenza è che lo sviluppo di Internet e delle sue tecnologie " *(…) offre la prospettiva di un maggior godimento dei diritti umani*". Però, allo stesso tempo "*(…) nell'era digitale, le nuove tecnologie di comunicazione aumentano altresì la possibilità che Governi, imprese e individui effettuino un controllo sui dati personali, li intercettino e li detengano*"[5].

Elemento centrale del discorso del Commissario è la preoccupazione che i diritti di cui godono i cittadini "offline" devono essere protetti in egual misura "online", specialmente in considerazione del fatto che le interferenze al godimento pacifico di tali diritti perpetrate online sono verosimilmente più facili, più veloci, meno evidenti, ed al tempo stesso più difficili da intercettare e da prevenire.

2. Interferenze: limiti, rischi e protezione

Tradizionalmente, la prima preoccupazione a proposito di possibili lesioni al diritto alla privacy sorge quando l'esercizio di un potere pubblico colpisce la vita privata dei cittadini e ne limita il pieno godimento.

In una società democratica ciò può avere luogo anche frequentemente, ma l'intervento statale non può essere né arbitrario né illegittimo[6].

Nessuna interferenza nella privacy è accettabile, eccetto nei casi stabiliti dalla legge, e la stessa normativa domestica deve necessariamente rispettare alcuni requisiti, per essere legittima sul piano internazionale: deve essere coerente con i Trattati internazionali; ragionevole in relazione al caso concreto; e proporzionale rispetto agli scopi perseguiti.

---

diritto alla privacy nell'era digitale. Si veda, anche per un approfondimento sulle tutele del diritto alla privacy il sito internet del Human Rights Watch..

[5] "*Il diritto alla privacy nell'era digitale. Report dell'Ufficio dell'Alto Commissario per i Diritti Umani dell'ONU*" è stato presentato alla 27esima Sessione del Consiglio per i Diritti Umani in data 30 giugno 2014.

[6] L'articolo 8, comma 2 della Convenzione Europea dei Diritti dell'Uomo stabilisce che: "*Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*".

La proporzionalità è divenuta un concetto di fondamentale importanza, in special modo in questi ultimi anni che hanno visto l'intensificarsi della lotta contro il terrorismo, ed i Governi adottare misure di controllo di massa, con la giustificazione della sicurezza nazionale.

Nel suo report, il Commissario riconosce che "*(…) le tecnologie di comunicazione digitale possono essere usate, come lo sono state, da individui per perseguire finalità criminali*" e che "*(…) l'adozione di misure di sorveglianza di massa a tutela della sicurezza nazionale o per la prevenzione del terrorismo o altri crimini può essere legittima*".

Ma questo di per sé non è sufficiente: tali misure di sorveglianza adottate dagli Stati devono essere anche proporzionate (vale a dire, adottando le parole del Commissario, che va scelto "*lo strumento meno invasivo fra quelli che possono conseguire il risultato desiderato*"); in caso contrario, esse saranno considerate illegittime nonostante perseguano finalità legittime e siano state adottate in base a disposizioni di legge.

In altri termini, è necessario operare un bilanciamento fra le necessità dello Stato e la protezione della privacy.

Occorre altresì menzionare il fatto che i governi spesso richiedono che le imprese private diano loro diretto accesso alle comunicazioni ed alle informazioni personali dei propri clienti, e che detengano tali informazioni.

Misure di questo genere possono ingenerare un abuso di potere pubblico[7].

In conclusione, è chiaro che simili violazioni sono più frequenti e, nello stesso tempo, più difficili da scoprire, con il risultato che diventa altresì più complicato, per i cittadini, ottenere tutela[8].

---

[7] "*L'obbligo di conservazione dei dati è ormai un elemento ricorrente all'interno dei regimi di sorveglianza di molti Stati, dove i governi impongono che le compagnie telefoniche e i fornitori di servizi digitali conservino tutte le informazioni relative alle comunicazioni dei loro clienti affinché successivamente, in applicazione della legge, le agenzie di intelligence vi possano avere accesso. Questa misura non sembra né necessaria né proporzionata*". Estratto dalla conferenza stampa sul diritto alla privacy nell'era digitale, Alto Commissario ONU per I Diritti Umani.

[8] Si vedano su questo punto due editoriali dell'Oxford Journal, International Data Privacy Law, ai quali fa anche riferimento il Commissario nel suo report. Il primo editoriale, intitolato *Accesso sistematico da parte del governo ai dati del settore privato* (International Data Privacy Law, 2012, Vol. 2, N. 4) analizza le numerose problematiche che insorgono a causa delle costanti richieste, da parte dei governi, di avere accesso ai dati personali dei consumatori privati. L'editoriale si conclude con l'osservazione che:" *(…) anche nei Paesi dove è in vigore la più ampia e sistematica legislazione sulla protezione dei dati, la raccolta dei dati e il loro utilizzo per supposte ragioni di sicurezza nazionale e di applicazione della*

Come osservato dall'Alto Commissario: "*Rimedi effettivi alla violazione della privacy perpetrata tramite misure di sorveglianza digitale possono trovare applicazione in via giudiziale, legislativa o amministrativa*".

3. La decisione della Corte di Giustizia dell'Unione Europea (CGUE) sulla Direttiva per la Conservazione dei Dati

Il giudice mantiene chiaramente un ruolo di primo piano in materia di rimedi e tutele contro le violazioni del diritto alla privacy.

È importante tenere in considerazione questo legame alla luce della recente sentenza della CGUE nei casi congiunti C-293/12 e C-594/12[9], che proietta una nuova luce sul concetto di privacy digitale.

La Corte era stata chiamata a decidere se la Direttiva Europea 2006/24, che stabiliva l'obbligo, a carico dei fornitori di servizi di comunicazioni elettroniche, di conservare per un certo periodo di tempo i dati personali dei loro clienti[10], fosse compatibile con il diritto alla privacy statuito nell'articolo 7 della Carta dei Diritti Fondamentali dell'Unione Europea[11] e nell'articolo 8 della Convenzione Europa dei Diritti dell'Uomo; in aggiunta si doveva

---

legge eccedono generalmente lo scopo di queste stesse leggi o ne costituiscono un'evidente eccezione". Ad aprile 2014, dopo il noto scandalo della diffusione dei dati, è stato pubblicato un addendum del primo editoriale (International Data Privacy Law, 2014, Vol. 4, N. 1). Si vedano anche i contributi forniti dall'organizzazione non-governamentale sui diritti digitali, European Digital Rights.

[9] CGUE, casi C-293/12 e C-594/12 sentenza del 8 aprile 2014.

[10] Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

L'articolo 5 elenca le categorie di dati che devono essere conservati, fra cui quelli necessari per tracciare ed identificare la fonte delle comunicazioni (vale a dire, numero di telefono, indirizzo e-mail, Internet user-ID).

L'articolo 6 stabilisce che il periodo di conservazione dei dati debba essere non inferiore a sei mesi e non superiore a due anni a partire dal giorno della comunicazione.

[11] Si veda il testo completo della Carta dei Diritti Fondamentali della UE (2010/C 83/02). L'articolo 7 (Rispetto della vita privata e della vita familiare) stabilisce che: "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*".

L'articolo 8 (Protezione dei dati di carattere personale) statuisce che: "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*".

stabilire se fosse compatibile con l'articolo 8 della Carta, che disciplina la protezione dei dati personali.

Il primo passaggio del ragionamento sviluppato dalla Corte è stato di verificare se lo scopo e le disposizioni della Direttiva soddisfacessero un interesse di carattere generale:questa verifica, ad opinione della Corte, ha avuto esito positivo[12].

Ad ogni modo, è ampiamente riconosciuto che l'obiettivo della *sicurezza nazionale* non sia sufficiente, e che qualsiasi interferenza perpetrata da un'autorità pubblica debba avvenire entro certi limiti; in caso contrario, i diritti fondamentali dei cittadini sarebbero violati.

Alla legislazione europea si richiedeva di stabilire *"(…) norme precise per regolare la finalità e l'applicazione delle misure"*[13] contenute dalla Direttiva; su questo punto, la Corte ha riscontrato numerose criticità.

In primo luogo, la Corte ha sottolineato come la Direttiva non specificasse chiaramente quale dovesse essere la relazione fra i dati personali e la minaccia alla sicurezza pubblica; in secondo luogo, non è stata rilevata alcuna previsione che ponesse un limite all'accesso ai dati personali nei confronti delle autorità nazionali; infine, e a maggior ragione, la problematica della garanzia di protezione dei dati stessi appariva drammaticamente ignorata[14].

La conclusione della Corte era, pertanto, che la legislazione europea non rispettasse il principio di proporzionalità in relazione allo scopo e tenendo conto delle concrete misure di applicazione della disciplina stessa; da cui risultava che la Direttiva fosse invalida.

---

[12] Su questo punto, i paragrafi 43 e 44 della sentenza osservano che: " *A causa della crescita significativa delle possibilità offerte dalle comunicazioni elettroniche, (…) i dati relative all'utilizzo di queste comunicazioni sono particolarmente importanti e pertanto costituiscono un valido strumento nella prevenzione e nella contro il crimine, in particolare contro il crimine organizzato. (…) Da ciò si deve ritenere che la conservazione di dati allo scopo di permettere alle autorità nazionali competenti di avere accesso ai medesimi (…) soddisfi genuinamente un obiettivo di interesse generale*".

[13] Si veda il paragrafo 54 della sentenza.

[14] Dopo aver elencato le sopraccitate criticità all'interno della Direttiva, la Corte perveniva alla conclusione che questa *"(…) non fornisse sufficienti garanzie, così come richiesto dall'articolo 8 della Carta, affinché fosse assicurata l'effettiva protezione dei dati conservati contro ogni rischio di abuso e ogni accesso ed utilizzo illegittimi*". In uno degli ultimi paragrafi della sentenza, la Corte ha affrontato anche la tematica della territorialità, osservando che *"(…) la Direttiva non prevede che I dati in questione siano conservati all'interno dei confine dell'Unione Europea*", il che causava evidenti problemi di mancanza di controllo sulla loro protezione.

4. Conclusioni

Nel suo report il Commissario ha fatto spesso riferimento alle sentenze delle Corti europee, sottolineandone l'efficacia nell'identificare i problemi principali in materia di privacy digitale, e nel fornire un rimedio.

Tuttavia, è evidente come lo sforzo necessario per trovare una soluzione a questi problemi debba essere collettivo.

I primi passi fondamentali da compiere sono: incentivare una maggiore chiarezza fra gli Stati ed intensificare la collaborazione con le imprese private. Tali affermazioni appaiono essere, per il momento, più una dichiarazione d'intento che un effettivo rimedio contro le violazioni.