LABORATORIO DIRITTI FONDAMENTALI

In collaborazione con l'Osservatorio sul rispetto dei diritti fondamentali in Europa

bollettino LDF

Luglio 2014

Il quadro generale europeo

La normativa italiana

La sentenza della Corte di giustizia dell'8 aprile 2014

E ora?

Bollettino N°13

La protezione e la raccolta dei dati personali: quale garanzie per i cittadini europei?

Sommario: 1. Il quadro generale europeo.- 2. La normativa italiana.- 3.La sentenza della Corte di giustizia dell'8 aprile 2014.- 4.E ora?

1. Il quadro generale europeo

Tra gli obiettivi dell'Unione europea vi è, da venti anni a questa parte, anche quella di offrire ai propri cittadini uno spazio di sicurezza (art. 3 TUE). L'art. 67 del TFUE specifica anche che il livello di sicurezza debba essere "elevato" e che venga conseguito *"...attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali."*

Tuttavia per lungo tempo l'azione dell'Unione è stata ostacolata dall'esigenza di unanimità per l'adozione di ogni provvedimento da parte del Consiglio dell'Unione. Dopo il Trattato di Lisbona questo regime tipicamente intergovernativo è cessato, con l'estensione di massima del regime legislativo e giurisdizionale ordinario alla cooperazione di polizia e giudiziaria in campo penale.
Il Trattato non ha tuttavia risolto alcune ambiguità sulle competenze a intervenire, quando coesistano esigenze di sicurezza interna (alle quali si applica il regime ordinario) ed esterna (per le quali sopravvive il regime intergovernativo) o quando le esigenze legate alla costruzione di uno spazio di sicurezza europeo si sovrappongano alla competenza esclusiva degli Stati membri in materia di sicurezza nazionale (materia che viene fatta tradizionalmente coincidere con le attività di *intelligence* a tutela della sicurezza della nazione).
Questa già difficile ripartizione di competenze diventa ancora più ardua da definire quando si sia in presenza di minacce come il terrorismo e il *Cybercrime,* (che possono incidere contemporaneamente su beni protetti a livello nazionale, europeo e internazionale), o in presenza di prassi di polizia che sconfinano spesso negli ambiti dell'*intelligence.* Complica ulteriormente il quadro la nozione di sicurezza nazionale in termini tanto estesi da giustificare lo spionaggio degli altri Stati membri, con ciò rimettendo in gioco il principio di cooperazione leale fra membri di una Unione in cui ogni Stato confida la propria sicurezza agli altri Stati membri (per esempio in materia di controllo delle frontiere).
Dai tempi dell'inchiesta sul sistema *Echelon* sino al recente caso Snowden, il Parlamento europeo ha cercato di riportare l'azione dell'Unione ai principi previsti dalla Convenzione europea dei diritti umani e dalla Carta dei diritti fondamentali dell'Unione europea. In questa prospettiva rientrano le risoluzioni adottate negli ultimi 14 anni in relazione agli accordi con gli Stati Uniti in materia di trattamento dei dati personali dei cittadini europei ("safe harbor" nel 2000; dati

dei passeggeri aerei "PNR", negli anni 2004, 2007, 2012; dati relativi ai trasferimenti interbancari " SWIFT", negli anni 2007 e 2010). In tutti questi casi il Parlamento europeo ha coerentemente contrastato la raccolta indiscriminata di informazioni personali da cui deriva il rischio di creare una società della sorveglianza. La raccolta indiscriminata di dati personali vìola infatti i diritti fondamentali delle persone nell'ambito dei Paesi membri.
Il cosiddetto caso Snowden e l'inchiesta che ne è seguita hanno portato al pettine i nodi irrisolti, come emerge dalla Risoluzione del Parlamento europeo del 12 marzo 2014, che ha promosso un «*Habeas Corpus* digitale europeo" articolato su più azioni quali:

- La riforma della protezione dei dati (che copre anche gli aspetti legati alla sicurezza);
- La definizione di un quadro transatlantico *("Umbrella" agreement)* nel quale siano preservate sia le esigenze comuni di sicurezza sia i diritti delle persone, garantiti dalle competenti giurisdizioni;
- La sospensione in via precauzionale degli accordi transatlantici in vigore (SafeHarbor, TFTP-SWIFT);
- Il rafforzamento del controllo democratico e giurisdizionale;
- La promozione dell' autosufficienza tecnologica europea e di una strategia coerente per quanto riguarda la *governance* di Internet.

A queste iniziative dell'assemblea parlamentare si sono recentemente aggiunte due importanti sentenze della Corte di Giustizia intese a rafforzare la protezione dei dati personali tanto in presenza di esigenze di sicurezza (sentenza Digital Rights Ireland dell'8 aprile 2014 – di cui *infra*), quanto della loro libera accessibilità e senza limiti di tempo attraverso la rete (sentenza "Google" del 13 maggio 2014). Con questa giurisprudenza la Corte ha posto in rilievo il nuovo ruolo della Carta dei diritti fondamentali nella tutela delle persone da possibili abusi da parte di soggetti sia pubblici che privati. La Corte ha anche dettato criteri che dovranno essere tenuti in conto tanto in sede legislativa che nei negoziati internazionali. Non siano mancati rilievi critici ad entrambe le decisioni: per la prima in ordine alla sua efficacia negli ordinamenti interni e per la seconda per avere forse sacrificato il diritto all'informazione rispetto a quello dei singoli di ottenere la cancellazione dei dati e per averne in sostanza rimessa la rimozione alla discrezionalità dei privati. In ogni caso le sentenze hanno reso comunque evidente che il controllo della comunicazione e dell'informazione sulla rete è oggi di cruciale importanza per la garanzia di diritti fondamentali e che appare urgente la predisposizione di regole " pubbliche" che realizzino un equo bilanciamento tra gli interessi in gioco.

2. La normativa italiana

1. Disposizioni generali

Il Codice della privacy (decreto legislativo 30 giugno 2003, n. 196), che ha raccolto in un testo unico le disposizioni della legge 31 dicembre 1996, n. 675, e la normativa integrativa e speciale esistente in materia, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato.
Per la particolare delicatezza delle situazioni che essi individuano, il Codice protegge in maniera rafforzata i dati "sensibili" (quelli che rivelano, o possono rivelare, l'origine razziale ed etnica, le

convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, ed inoltre i dati personali idonei a rivelare lo stato di salute e la vita sessuale) e i dati "giudiziari" (quelli che denotano la qualità di condannato per reati, o la qualità di imputato o indagato in un procedimento penale).
Il trattamento dei dati sensibili e dei dati giudiziari deve essere improntato ai principi di indispensabilità (rispetto alle finalità perseguite), minimizzazione (se è possibile il ricorso a dati personali comuni), separazione (dai dati comuni), cifratura.
Affinché il trattamento di dati possa considerarsi legittimo, il titolare è obbligato:
-a verificare il rispetto dei presupposti di liceità del trattamento (acquisendo, se necessario, il consenso dell'interessato o avvalendosi di condizioni equivalenti; rispettando le prescrizioni impartite dall'autorità di controllo, ecc.);
-ad informare l'interessato sulle principali caratteristiche del trattamento;
-a notificare, in casi particolari previsti dal codice (art. 37), il trattamento che intende svolgere;
-a richiedere, se necessario, un'autorizzazione specifica al trattamento di dati sensibili o giudiziari;
-ad adottare le misure di sicurezza idonee a ridurre al minimo il rischio di distruzione, alterazione, perdita, accesso non autorizzato o trattamento non conforme alle finalità della raccolta.
Con legge n. 675/1996 è stato istituito il Garante per la protezione dei dati personali, un'apposita Autorità amministrativa dotata di ampia autonomia, di poteri di controllo e di poteri sanzionatori. Il Garante ha inoltre poteri decisori e poteri cautelari, poteri ispettivi e di accertamento finalizzati alla prevenzione e alla repressione degli illeciti in materia.
Il Garante può autorizzare, anche rispetto a categorie di titolari o di trattamenti, l'utilizzo di dati sensibili o giudiziari, impartendo ai titolari prescrizioni relative alle misure ed agli accorgimenti da prendere a tutela dell'interessato
Per i soggetti privati, il trattamento di dati personali è di regola legittimo qualora sia stato prestato il consenso da parte dell'interessato.
Uno degli aspetti più importanti e innovativi della disciplina sulla privacy risiede nella previsione della possibilità per l'interessato di esercitare i diritti di controllo sulle banche dati (art. 7 del Codice), con il connesso diritto di ottenere direttamente dai soggetti che elaborano i dati la conferma dell'esistenza o meno delle informazioni che lo riguardano e la cancellazione delle informazioni trattate in violazione di legge, l'aggiornamento, la rettifica o l'integrazione dei dati stessi.
Nel caso in cui l'interessato non veda soddisfatte le sue richieste, la tutela può spostarsi nella sede giurisdizionale o, attraverso il ricorso al Garante, in quella amministrativa, la quale comporta l'eventuale esercizio dei poteri interdittivi del Garante anche sul piano cautelare. Il Codice mette dunque a disposizione dell'interessato un 'doppio binario' per la tutela dei diritti, rendendo alternativo alla via giurisdizionale il rimedio del ricorso al Garante. Quest'ultimo, destinato a concludersi in tempi rapidi (60 gg.), offre una efficace tutela anche a fronte della velocità di propagazione dei dati e alla potenziale ampiezza dei destinatari della diffusione, specie nel caso di trattamenti per via telematica. Anche al di fuori del meccanismo appena descritto, l'interessato può chiedere al Garante di pronunciarsi sulla legittimità del trattamento

dei dati personali che lo riguardano, mediante segnalazione, o reclamo contenente la specifica indicazione delle circostanze, delle disposizioni che si ritengono violate e delle misure di garanzia richieste.
Non è invece possibile chiedere il risarcimento del danno in sede di contenzioso di fronte al Garante.
Eventuali pretese risarcitorie possono essere fatte valere con ricorso al giudice competente.
La tutela successiva alla lesione del diritto alla protezione dei dati personali è affidata anche alla previsione di sanzioni amministrative in caso di mancato rispetto di alcune delle previsioni del Codice (omessa o inidonea informativa, omessa o incompleta notificazione, ecc.).
Il sistema di garanzie è integrato dalla previsione di sanzioni penali (per trattamento illecito di dati, falsità nelle dichiarazioni al Garante, ecc.) temperate dalla rilevanza, di regola, delle sole condotte dolose e dall'introduzione, per alcuni casi, di un dolo specifico rappresentato dal fine di trarre un profitto per sé o per altri o di recare ad altri un danno.

2. La durata della conservazione dei dati

In linea generale i dati legittimamente raccolti possono essere conservati solo fino alla realizzazione dello scopo per il quale sono stati raccolti.
Ma per dati che incidono particolarmente sulla vita privata delle persone sono stabiliti termini precisi: per esempio, le immagini registrate da apparecchi di videosorveglianza possono essere conservati al massimo per una settimana.
Quanto ai dati di traffico relativi alle comunicazioni elettroniche (cioè i dati che indicano chi ha comunicato con chi, e quando, non certamente i contenuti delle comunicazioni che sono assolutamente riservati), possono essere conservati a fini di fatturazione per l'abbonato per un periodo non superiore a sei mesi (art.123 Codice privacy).
Tuttavia, ai soli fini dell'accertamento e della repressione dei reati, i dati relativi al traffico telefonico sono conservati dal fornitore del servizio per ventiquattro mesi e quelli relativi al traffico telematico per sei mesi. Allorché si tratti dell'accertamento e della repressione di delitti di particolare gravità o in danno degli stessi servizi informatici o telematici il periodo anzidetto è raddoppiato (art.132 Codice privacy). Specifiche disposizioni sono adottate per il trattamento e la successiva distruzione di questi dati.

3. La sentenza della Corte di giustizia dell'8 aprile.

Veniamo ora alla sentenza della Corte di giustizia dell'Unione europea con la quale è stata esaminata la legittimità della Direttiva 2006/24/CE che obbligava i gestori di servizi di telecomunicazione a conservare tutti i dati connessi alle comunicazioni elettroniche e, su richiesta, a fornirli, alle autorità investigative ed alla magistratura. Si tratta di una Direttiva emanata in tutta fretta sull'onda dell'attacco terroristico a Londra dell'anno prima che introduceva deroghe, motivate dall'esigenza di combattere in primo luogo il terrorismo internazionale e segnatamente quello islamico, alle stesse direttive dell'Ue in materia trattamento dei dati personali, protezione della privacy, rispetto della vita privata nel settore delle comunicazioni elettroniche (in particolare la direttiva 2002/58/Cee).
Ad investire della questione la Corte di giustizia sono state, sia la Corte suprema irlandese che, su ricorso di una ONG, chiedeva di verificare se la disciplina europea avesse compiuto un

bilanciamento adeguato tra la necessità di garantire la sicurezza ed il corretto funzionamento del mercato interno e la necessità di salvaguardare la libertà di circolazione, il rispetto della vita privata (sancito dagli artt. 7 della Carta dei diritti Ue e dall'art. 8 della Cedu), la libertà di espressione (artt. 10 della Carta Ue e 10 della Cedu), sia la Corte costituzionale austriaca che, su ricorso del governo della Carinzia, chiedeva analogamente se il sistema di raccolta dei dati previsto dalla Direttiva del 2006 fosse compatibile con il rispetto dei diritti fondamentali prima citati. I passi essenziali del ragionamento della Corte sono i seguenti. I dati sottoposti all'obbligo di conservazione (non riguardanti il contenuto delle comunicazioni elettroniche, ma concernenti mittente e numero chiamato, indirizzi IP, localizzazione del chiamante ed apparecchiature utilizzate) consentono " di tracciare profili abbastanza definiti riguardo le persone che utilizzano i mezzi di comunicazione interessati alla raccolta". Pertanto tale pratica di conservazione può interferire con i diritti della Carta come la libertà di espressione, la riservatezza della vita privata e la protezione dei dati personali. Non può dirsi però che tutte le possibili lesioni di tali diritti violino anche il loro contenuto essenziale (art. 52 della Carta dei diritti Ue). Tuttavia la Corte ritiene sia stato violato il principio di proporzionalità (prioritario canone di valutazione della legittimità dell'azione dell'Unione, soprattutto in questo campo), cioè che l'interferenza nella sfera dei diritti fondamentali sia stata eccessiva e troppo invasiva rispetto al perseguimento del dichiarato intento del contrasto del crimine e del terrorismo internazionale. Sebbene questa finalità sia certamente ammissibile come ragione di una certa limitazione delle prerogative individuali, la Direttiva eccede il limite di ciò che appare strettamente necessario per garantire la sicurezza collettiva. La Corte indica svariati aspetti di questa violazione del principio di proporzionalità; innanzitutto la vaghezza dei criteri utilizzati per indicare quali crimini vadano perseguiti attraverso la conservazione dei dati; l'insufficienza delle procedure e dei rimedi previsti per evitare che attraverso la detta raccolta si possano realizzare abusi di varia natura visto che la raccolta non deve essere preceduta da una richiesta dell'Autorità giudiziaria; l'assenza di un elenco di situazioni eccezionali escluse dall'obbligo di conservazione; la mancanza di norme che stabiliscano modalità sicure di immagazzinamento dell'informazione (ed anche la successiva distruzione irreversibile di questa). Si censura anche, in via generale, la scelta di un monitoraggio che coinvolge indistintamente tutti i soggetti, tutti i mezzi di comunicazione elettronica e ogni tipo di dati, dando luogo quindi un sistema di osservazione non strettamente indispensabile al perseguimento degli obiettivi dichiarati nella Direttiva. Conseguentemente l'indebita compressione dei diritti fondamentali stabiliti nella Carta dei diritti dell'Unione europea e nella Cedu comporta l'invalidità nella sua interezza dell'intera Direttiva, che viene conseguentemente annullata senza alcuna distinzione tra le sue parti e le sue specifiche norme. Ora va ricordato che questa importante decisione è intervenuta in un momento in cui l'opinione pubblica europea era ancora molto turbata dalle rivelazioni sullo spionaggio di massa compiuto dai servizi di sicurezza USA (NSA) nei confronti di cittadini del vecchio continente ed anche della Cancelliera Merkel. La vicenda aveva portato a reazioni assai vivaci non solo dei Governi, ma anche del Parlamento dell'Unione, cui ha fatto seguito la promessa del Presidente USA di far cessare tale attività spionistica.

L'8 aprile 2014 la Corte di giustizia ha emanato un'altra sentenza (C-288/12, *Commissione c. Ungheria*, sull'indipendenza delle autorità responsabili della protezione dei dati personali) sempre in materia di rispetto della *privacy*, certamente di minore rilievo rispetto alla prima, ma che

segnala l'interesse ed il rigore con cui la Corte del Lussemburgo tratta le vicende in questa materia alla luce del prioritario impegno a far rispettare almeno il nucleo intangibile dei diritti protetti dalle due Carte sovranazionali. Va ancora rimarcato il metodo che ha scelto la Corte che, pur in una pronuncia di annullamento totale di un provvedimento legislativo dell'Unione, individua con cura gli aspetti ritenuti inaccettabili di tale provvedimento, quasi a delineare un possibile nuovo quadro legislativo che, nel salvaguardare le esigenze della sicurezza attraverso l'informazione, sia più rispettoso delle prerogative individuali e tale da consentire un maggior controllo da parte delle Autorità giudiziarie nazionali. La decisione va anche ricordata come un esempio di " fusione costituzionale" tra ordinamenti diversi in quanto la Corte di giustizia utilizza, integrandole tra di loro, sia le fonti normative e la giurisprudenza dell'Unione europea che quelle del Consiglio d'Europa (la cosiddetta "Grande Europa" a 47 membri), così da mostrare che almeno in questa materia sussiste un patrimonio costituzionale comune piuttosto saldo e radicato. Infatti la Corte di giustizia finisce con il recepire alcuni argomenti già sviluppati dalla Corti costituzionali nazionali di Germania. Bulgaria, Romania e Repubblica ceca in decisioni sulle legislazioni nazionali di attuazione delle Direttiva europea annullata. **Va poi sottolineato che, come accennato nel par. 1), la Corte di Giustizia nel caso Google del 13 maggio 2014 ha valutato che gli artt. 7 e 8 della Carta dei diritti dell'Ue implichino un certo riconoscimento di quello che giornalisticamente è stato definito come " diritto all'oblio" cioè la pretesa del cittadino a rimuovere dalla rete informazioni ritenute dannose alla sua reputazione o comunque pregiudizievoli in mancanza di un interesse di natura pubblica all'accesso generalizzato. E' da rimarcare come sulla *homepage* delle società sia comparso quasi subito un modulo che consente ai cittadini di richiedere la rimozione dei dati ritenuti non graditi. Anche in questa controversia la Corte di giustizia ha tenuto conto della giurisprudenza della Corte europea dei diritti umani, sebbene l'orientamento di quest'ultima dia, rispetto al diritto del singoli, un rilievo più marcato al diritto di informazione ed al libero accesso ai dati.**

4. Ed ora?

Come abbiano già ricordato la sentenza della Corte di Giustizia ha annullato la direttiva del 2006, ma tale cancellazione non incide direttamente sulle legislazioni nazionali che sono tutte rimaste in vigore. La decisione cancella una "deroga" alla normativa europea di carattere generale che pertanto vien ripristinata nel suo precedente ambito di applicazione. Le conseguenze, quindi, della sentenza dell'8 aprile 2014 sono duplici. Da un lato i giudici nazionali potranno e dovranno verificare, una volta investiti della questione, se le normative interne sono coerenti con la legislazione sovranazionale in materia di *privacy*, anche interpretata alla luce dei diritti fondamentali della Carta Ue (trattandosi di materia in cui l'Unione ha esercitato al sua competenza la Carta è comunque applicabile). Dovranno altresì verificare se sussistono ulteriori esigenze che giustifichino l'esistenza della normativa nazionale, oltre quella di recepire la Direttiva che è stata annullata, in quanto il contrasto del crimine e del terrorismo internazionale ben può avere anche un fondamento di ordine interno. Sotto questo profilo alcuni primi commentatori della decisione della Corte di giustizia hanno ipotizzato che l'art. 132 del cosiddetto Codice della *privacy* italiano potrebbe non essere in linea con la normativa sovranazionale. Sono questioni che appaiono ancora da approfondire e che potrebbero portare

anche a soluzioni diverse nei singoli paesi. Molto interessante, però, appare la reazione politico-istituzionale europea alla decisione della Corte di Giustizia, in quanto sembra nata una discussione molto vivace proprio per la "tecnica motivazionale" della sentenza che ha posto alcune questioni molto specifiche agli organi dell'Unione come il Parlamento o la Commissione in vista di una eventuale riscrittura della Direttiva.
Il 4 giugno 2014 è intervenuto il Supervisor europeo sulla protezione dei dati con un importante documento sul futuro assetto dell'intero sistema alla luce della decisione della Corte e della garanzie degli artt. 7 e 8 della Carta dei diritti, così come il giorno dopo il Consiglio d'Europa ha emanato una Risoluzione per una nuova Convenzione sulla protezione dei dati più rispettosa dei diritti come sanciti dalle due Carte europee.