Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche

CONVEGNO

Verso una Costituzione per Internet?

Palazzo Montecitorio

Sala del Mappamondo

16 giugno 2014

Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche

CONVEGNO

Verso una Costituzione per Internet?

CAMERA DEI DEPUTATI

Palazzo Montecitorio - Sala del Mappamondo

16 giugno 2014

n. 124

SEGRETERIA GENERALE – Ufficio Rapporti con l'Unione europea
☎ 066760-2145 - ✉ *cdrue@camera.it*

SERVIZIO STUDI
☎ 066760-3403 - ✉ *st_segreteria@camera.it*

AVVOCATURA
☎ 066760-9360 - ✉ segreteria_avvocatura@camera.it

SERVIZIO BIBLIOTECA - Osservatorio della legislazione straniera
☎ 066760-2278 - ✉ *bib_segreteria@camera.it*

***File**: ID0012.docx*

I N D I C E

SCHEDE DI LETTURA

La protezione dei dati personali nel diritto dell'UE: i presupposti nelle fonti primarie: i Trattati, la Carta dei diritti fondamentali. La CEDU

- Premessa....3
- I Trattati e la Carta dei diritti fondamentali....4
- La CEDU....5

Prospetto sulla Giurisprudenza della Corte europea dei diritti dell'uomo

- Premesse giuridiche....6
- Casistica saliente sull'art. 8 della Convenzione....7
- Casistica saliente sull'art. 10 della Convenzione....7

La più recente giurisprudenza della Corte di giustizia dell'Unione europea

- a) L' annullamento della direttiva sulla conservazione dei dati personali....10
- b) L'applicabilità della normativa europea ai gestori di motori di ricerca....12

Le iniziative in corso: l'Unione europea

- Il pacchetto di riforma in materia di protezione dati: nuovi strumenti e potenziamento di quelli vigenti....14
- La discussione sulle attività di sorveglianza dei dati di massa....19
- La net neutrality – principi di libera fruizione di servizi e contenuti della rete....22

Le iniziative in corso: gli ordinamenti nazionali

- Italia....24
- Francia....29
- Germania....30
- Regno Unito....32
- Spagna....35
- Altri paesi europei....37
- *Focus: Le esperienze di alcuni Paesi dell'America latina*....40

Schede di lettura

LA PROTEZIONE DEI DATI PERSONALI NEL DIRITTO DELL'UE: I PRESUPPOSTI NELLE FONTI PRIMARIE: I TRATTATI, LA CARTA DEI DIRITTI FONDAMENTALI. LA CEDU

Premessa

In materia di tutela della riservatezza applicata alle nuove tecnologie dell'informazione e della comunicazione e, in particolare, di protezione dei dati personali la disciplina dell'Unione europea registra un progressivo affinamento. Tale processo si è andato realizzando, in primo luogo, attraverso la previsione di specifiche disposizioni nell'ambito dei Trattati cui si accompagnano le norma previste dalla Carta europea dei diritti fondamentali.

In secondo luogo, alla previsioni delle fonti primarie si sono accompagnati gli interventi del legislatore europeo che, a seguito dell'entrata in vigore del Trattato di Lisbona, si sono realizzati attraverso la procedura ordinaria che prevede il coinvolgimento su un piano di parità del Parlamento e del Consiglio europeo.

A ciò deve aggiungersi l'elaborazione in sede giurisprudenziale della Corte di giustizia dell'Unione europea, che nelle più recenti pronunce, rispettivamente di aprile e maggio 2014, ha assunto posizioni molto avanzate sul terreno della tutela della sfera dei diritti della persona, arrivando ad invalidare la normativa vigente in materia di conservazione dei dati in quanto non ritenuta sufficientemente garantista rispetto al rischio di una ingerenza della sfera giuridica dei soggetti interessati.

Questo complesso lavoro di continui e successivi adeguamenti della normativa trae origine dalla consapevolezza della delicatezza della materia e dei crescenti rischi che il progresso tecnico amplifica.

Le istituzioni europee hanno, peraltro, dimostrato, anche nella dialettica che si è innescata tra Commissione, Consiglio, Parlamento e Corte di giustizia, di non volersi limitare a rincorrere l'evoluzione tecnologica ma di rivendicare all'Unione europea la capacità di guidare il percorso di aggiornamento del regime giuridico per garantire elevati standard di tutela dei diritti dei cittadini. Esemplare è, al riguardo, il confronto tra l'Unione europea e gli Stati uniti per quanto concerne specificamente il cd scandalo Datagate, relativamente al quale il Parlamento europeo ha addirittura prospettato la sospensione delle trattative relative ad importanti accordi commerciali in assenza di risposte soddisfacenti da parte degli Stati uniti.

Più in generale, si può affermare che l'intervento del legislatore europeo e le pronunce della Corte di giustizia abbiano inteso individuare un accettabile punto di equilibrio tra istanze diverse e non facilmente conciliabili quali sono: la salvaguardia della riservatezza, le esigenze connesse alla sicurezza, al contrasto alle varie forme di criminalità e al terrorismo che possono intensamente avvalersi

della strumentazione informatica e le esigenze di mercato connesse all'ampliamento delle occasioni di scambio e dei potenziali vantaggi in termini di riduzione dei costi per gli utenti.

A complicare il quadro si aggiungono: il rilievo che i diritti in questione rivestono anche nell'ambito degli ordinamenti costituzionali dei singoli Stati membri e le difficoltà connesse alla individuazione dell'ambito soggettivo di applicazione della normativa europea in ragione del fatto che taluni operatori così come le attività di processione dati (tipicamente, le maggiori società gestori di motori di ricerca) hanno sede legale o vengono realizzate al di fuori del territorio dell'UE.

I Trattati e la Carta dei diritti fondamentali

Dall'entrata in vigore del trattato di Lisbona, l'Unione europea dispone di una specifica **base giuridica** esplicita ai fini della **protezione dei dati**.

In particolare **l'articolo 16**, paragrafo 1 del Trattato sul funzionamento dell'Unione europea stabilisce che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano**. Il paragrafo successivo conferisce al **Parlamento europeo e al Consiglio** (secondo la procedura legislativa ordinaria) il **potere di adottare norme** relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di **autorità indipendenti**. È comunque fatto salvo l'articolo 39 del Trattato sull'Unione europea, che conferisce al Consiglio il potere di adottare decisioni al fine di stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo della **politica estera e di sicurezza comune** e le norme relative alla libera circolazione di tali dati.

Oltre che nei Trattati, la sfera della riservatezza delle informazioni personali e della vita privata dell'individuo trovano particolare tutela agli **articoli 7 e 8** della Carta dei diritti fondamentali la quale ha lo **stesso valore** giuridico dei **Trattati**. In particolare:

- l'articolo 7 prevede che ogni persona ha diritto al rispetto della propria **vita privata e familiare**, del proprio **domicilio** e delle proprie **comunicazioni**;
- l'articolo 8 stabilisce che ogni persona ha **diritto** alla **protezione dei dati** di carattere **personale** che la riguardano; 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**; il rispetto di tali regole è soggetto al **controllo di un'autorità indipendente**.

La CEDU

La sfera della **riservatezza personale** è protetta altresì dalla **Convenzione europea dei diritti dell'uomo (CEDU) (**su cui vedi oltre), stipulata dagli Stati membri del Consiglio d'Europa e, dunque, in un ambito che non coincide con quello dell'UE, che, all'articolo 8 (**Diritto al rispetto della vita privata e familiare**), prevede che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. La CEDU precisa tale principio stabilendo il **divieto di 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.

Si ricorda che ai sensi dell'articolo 6 del Trattato sull'Unione europea i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, **fanno parte del diritto dell'Unione in quanto principi generali.** Lo stesso articolo prevede l'**adesione dell'Unione alla Convenzione europea per la salvaguardia dei diritti dell'uomo** e delle libertà fondamentali, adesione il cui processo è tuttora in corso di perfezionamento.

Sempre nell'ambito del Consiglio d'Europa, merita ricordare anche la **Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale**, nell'ambito del **Consiglio d'Europa**, che ha lo scopo di tutelare le persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale, e che disciplina il flusso transfrontaliero dei dati, e il relativo Protocollo addizionale, concernente le autorità di controllo ed i flussi transfrontalieri.

La Convenzione, entrata in vigore il 1° ottobre del 1985, oltre alle garanzie previste per il trattamento automatizzato dei dati di carattere personale, bandisce il trattamento dei dati « delicati » sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale, le condanne penali, in assenza di garanzie previste dal diritto interno; essa garantisce inoltre il diritto delle persone di **conoscere le informazioni catalogate su di loro** ed ad esigere, se del caso, delle **rettifiche**. Unica restrizione a tale diritto può aversi solo in caso in cui sia presente un interesse maggiore (sicurezza pubblica, difesa, etc.).

La Convenzione impone anche delle **limitazioni ai flussi transfrontalieri** di dati negli Stati in cui non esiste alcuna protezione equivalente.

PROSPETTO SULLA GIURISPRUDENZA DELLA CORTE EUROPEA DEI DIRITTI DELL'UOMO

Premesse giuridiche

L'analisi della casistica è condotta essenzialmente alla luce dei seguenti articoli della Convenzione europea dei diritti dell'uomo: l'art. 8 (diritto alla vita privata e familiare) e l'art. 10 (diritto di libera manifestazione del pensiero).

All'esposizione sintetica degli sviluppi giurisprudenziali, si premetta che entrambi questi articoli attribuiscono alla persona i diritti a che la vita privata e familiare sia rispettata; e a la persona possa liberamente esprimente il proprio pensiero. Tali diritti non sono assegnati in via assoluta. Le medesime disposizioni contengono infatti la riserva che gli Stati sottoscrittori della Convenzione EDU possono limitare quei diritti, purché con provvedimento di legge e per il perseguimento di finalità legittime atte a garantire la tutela di una società democratica e nei limiti in cui ciò sia adeguato e proporzionato al conseguimento della menzionata finalità.

È proprio attraverso questo giudizio sull'adeguatezza e sulla proporzione dell'interferenza pubblica nel diritto del singolo che la Corte di Strasburgo ha sinora tracciato un percorso di elaborazione dello statuto giuridico della persona rispetto alle vie di comunicazioni digitale e alla grandi possibilità che l'informatica offre di accumulare, conservare e diffondere dati.

Laddove, nel caso specifico, la Corte ravvisi un complesso di azioni e provvedimenti proporzionati all'obiettivo dichiara la non violazione del diritto; altrimenti accerta la violazione. Da questo punto di vista, occorre anche chiarire che la Corte ha dilatato la nozione sia di 'vita privata e familiare' sia di 'diritto di espressione'.

Nella prima ha incluso una gamma di situazioni giuridiche assai ampia, che va dalla pretesa riconosciuta di non essere spiati e controllati a distanza, a quella di poter controllare la quantità e la qualità di dati propri che altri detenga, al diritto a veder tutelata la propria salute e sicurezza personale a quello di adottare figli senza discriminazioni e a crearsi una famiglia e a sceglierne il cognome.

Nella seconda, è ricompreso non solo il diritto di cronaca giornalistica e il diritto di critica ma altresì il diritto a essere informati, quello di poter attingere senza restrizioni alle fonti informative più varie e a quello di garantire e fruire del pluralismo informativo.

Si avverta altresì che la Corte europea fa carico agli Stati sottoscrittori non solo di rispettare quei diritti in chiave di astensione dalla loro violazione diretta – per opera di provvedimenti e comportamenti di pubblici agenti – ma fa loro obbligo anche di azioni positive di promozione e tutela.

Casistica saliente sull'art. 8 della Convenzione

Sotto l'aspetto del diritto alla vita privata e familiare, in relazione alle banche dati e agli usi di *Internet* come mezzo di conservazione, comunicazione e diffusione di dati, il caso più rilevante tra i recenti in chiave di protezione dall'interferenza diretta dei pubblici poteri è *S. and Marper* v. *United Kingdom* (4 dicembre 2008).

Durante un'indagine penale a carico di due soggetti, erano stati loro prelevati campioni genetici e impronte digitali. Successivamente, le indagini si erano concluse in modo assolutorio ma la banca dati della polizia britannica continuava a detenere i dati immagazzinati e la polizia medesima rigettava la richiesta di distruzione avanzata dagli interessati.

La Corte europea ha sottolineato come la protezione dei dati personali costituisca un aspetto essenziale del diritto alla vita privata e familiare (n. 103) e al contempo ha ritenuto legittimo lo scopo delle pubbliche autorità di conservare dati per finalità d'inchiesta penale e prevenzione dei reati; ma – nella circostanza specifica – si trattava di soggetti le cui posizioni erano state archiviate ragion per cui la schedatura biologica così profonda e temporalmente illimitata è stata ritenuta sproporzionata.

Di rilievo anche il successivo caso *Gardel* v. *France* (17 dicembre 2009), relativo al caso di un uomo condannato in via definitiva per violenza sessuale in danno di minore. Il nome del reo era stato inserito nel registro – previsto dalla legge francese – dei soggetti pericolosi in relazione ai reati sessuali (*Sex offenders*). Qui la Corte ha constatato che la normativa francese prevedeva un limite temporale (20 e 30 anni a seconda dei casi) e che comunque si trattava di soggetto definitivamente condannato. Di qui la non violazione.

Sotto l'aspetto del diritto alla vita privata e familiare, ma in relazione all'insufficiente protezione offerta dai pubblici poteri al diritto medesimo, appaiono di rilievo i casi:

1) K. U. *c.* Finlandia del 2 dicembre 2008, in cui è stata accertata la violazione dell'art. 8 del Paese scandinavo, in ragione dell'insufficiente protezione garantita dalla legislazione a un minore, i cui dati personali erano stati "postati" *on line* in un sito di appuntamenti. Il minore si era rivolto alle autorità nazionali per denunciare l'autore del post, ma si era sentito rispondere che il gestore non era obbligato a rivelarne il nome, per cui l'unico a essere punito sarebbe stato l'internet provider server.
2) Soderman *c.* Svezia del 12 novembre 2013, in cui è stata accertata la violazione dell'art. 8 del Paese convenuto, a motivo dell'insufficiente protezione garantita dalle decisioni giudiziali svedesi a una minore che era stata fraudolentemente ripresa da una telecamera mentre si spogliava.

Casistica saliente sull'art. 10 della Convenzione

Sotto l'aspetto del diritto di espressione in relazione a *Internet* come mezzo di conservazione, comunicazione e diffusione di dati, il caso più rilevante tra i recenti è *Times Newspaper* v. *United Kingdom* (10 marzo 2009).

Il quotidiano londinese aveva pubblicato, in forma sia cartacea sia sul proprio sito, due articoli che contenevano la notizia che una persona era implicata in sospette operazioni di riciclaggio di danaro proveniente dagli illeciti delle mafie russe.

Il soggetto in questione aveva proposto due distinte azioni giudiziarie, ritenendo la notizia diffamatoria e domandando il risarcimento del danno. Una prima azione era stata intentata nell'immediatezza del rilascio dell'informazione e una seconda un anno più tardi, basata sulla circostanza che gli articoli erano ancora disponibili sul sito *web* della testata. Successivamente alla notifica della seconda citazione per danni, il *Times* aveva apposto all'articolo, reperibile sul sito *web,* un'avvertenza del contenzioso in atto.

I tribunali britannici, in conclusione, avevano accertato la responsabilità del quotidiano e lo avevano indotto ad accettare la quantificazione in sede stragiudiziale del danno da risarcire. Essi avevano argomentato - in particolare - che l'azione giudiziaria iniziata per seconda non poteva dirsi prescritta (come la difesa del quotidiano pretendeva) in ragione del decorso di un anno dalla prima pubblicazione. Il termine annuale di prescrizione (previsto dalla legislazione britannica per la diffamazione a mezzo stampa) non poteva dirsi applicabile – secondo i giudici inglesi – poiché su *Internet* la diffamazione è permanente e il termine ricomincia a decorrere a ogni visualizzazione.

Adita sulla base dell'art. 10 dagli avvocati del *Times*, la Corte europea ha deciso per la non violazione a motivo che:

- è ben vero che la regola dell'azzeramento del termine di prescrizione a ogni nuova visualizzazione deriva da antiche decisioni di *common law* relative alla ripubblicazione dei libri e che tale regola è rifiutata, per esempio, negli Stati Uniti, dove viceversa si riconosce come momento iniziale solo la prima pubblicazione (nn. 20-24);
- è altresì vero che *Internet* ha dato un positivo impulso alla circolazione delle informazioni e alla ricerca storica, così enucleando un secondo scopo del giornalismo, da aggiungere a quello primario di essere il cane da guardia dell'opinione pubblica (n. 45);
- tuttavia, nel caso specifico, l'archivio delle notizie era gestito proprio dal *Times* e non da un'autorità terza e non sarebbe costato molto apporre l'avvertenza sulla pubblicazione *web* nell'immediatezza della prima citazione per danni (n. 47). Sebbene consentire azioni per diffamazione anche a grande distanza di tempo dalla prima pubblicazione possa configurare un'interferenza sproporzionata sul diritto di libera manifestazione del pensiero, in questo caso una simile circostanza non si era data. Pertanto, limitatamente a questo caso, la Corte non ha ritenuto violato l'art. 10 (nn. 48 e 49).

Il caso *Times* è in buona sostanza un *leading case*.

Nella sentenza *Pravoie Delo* c. *Ucraina* del 5 maggio 2011, la Corte europea ha ritenuto violato l'articolo 10 in relazione alla vicenda di un quotidiano che aveva pubblicato il testo di una lettera anonima, scaricato da *Internet* e considerato diffamatorio da terzi, e che per questo era stato condannato a risarcire il danno, ragione per cui – in definitiva – aveva successivamente chiuso. Qui l'interferenza dello Stato sull'attività del giornale (in particolare, sulla ricerca delle fonti) è stata considerata sproporzionata.

Nella sentenza *Yildirim* c. *Turchia* (18 dicembre 2012), la Corte europea – rifacendosi alle argomentazioni della *Times* - ha poi constatato la violazione dell'art. 10 a carico della Turchia.

Si trattava dell'oscuramento di un sito da cui un ricercatore traeva le informazioni per sua attività scientifica e accademica. Il sito era stato oscurato in ragione delle presunte

opinioni ivi contenute di critica (e di vilipendio) di Kemal Ataturk. Nell'occasione la Corte ha chiarito i requisiti in presenza dei quali sono compatibili con la Cedu interventi diretti a censurare la diffusione di dati su *Internet*.

Occorre che la legge nazionale:

1) indichi quali siano i soggetti i cui siti possano essere censurati od oscurati, come per esempio proprietari interni o esteri di contenuti illeciti, siti *web*, piattaforme, utenti, soggetti che forniscono *iper-links* a quei siti o piattaforme, eccetera;
2) precisi i tipi di provvedimento adottabile (blocco del sito, dell'indirizzo IP, di particolari modalità d'utilizzo, eccetera);
3) fissi l'ambito di applicazione territoriale del provvedimento;
4) determini la durata dell'intervento censorio;
5) indichi le ragioni e gli interessi che il provvedimento è volto a tutelare;
6) rispetti il principio di proporzionalità tra il provvedimento e il relativo scopo;
7) rispetti il principio di necessità;
8) determini l'autorità competente;
9) preveda una procedura apposita;
10) prescriva la notifica del provvedimento al destinatario;
11) contempli forme d'impugnazione.

Successivamente, degni di nota sono i casi:

1) *Delfi AS* c. *Estonia* (10 ottobre 2013), in cui è stata dichiarata la non violazione dell'art. 10 del Paese baltico, in una vicenda di pubblicazione sul sito *web* di un periodico che aveva aperto a commenti una notizia di cronaca, con la raccolta di molti insulti a carico di un soggetto determinato e la conseguente condanna risarcitoria dei responsabili del sito;
2) *Ringier Axel Springer* c. *Slovacchia* n. 3 (7 gennaio 2014) ha ritenuto violato l'art. 10 in relazione a una condanna al risarcimento dei danni a carico di un quotidiano che aveva diffuso – in via cartacea e su *Internet* – notizie e opinioni su un fatto di cronaca. Più in particolare, era insorta una controversia tra un concorrente a una trasmissione televisiva a *quiz* e gli organizzatori del *quiz* medesimo. Costoro ebbero ad accusare il concorrente di tentata truffa ma questi era risultato poi esentato da qualsiasi rilievo penale. Nondimeno, della larga diffusione a stampa e su *Internet* del contenzioso, il concorrente si era doluto in sede giudiziale, ottenendo soddisfazione risarcitoria dalla testata giornalistica, in via definitiva. Sul ricorso del giornale, la Corte ha valutato che i tribunali nazionali non avevano compiutamente affrontato la questione del pubblico interesse che la vicenda del *quiz* aveva suscitato (v. 83 della sentenza). Per questo, secondo la Corte europea, sebbene la cronaca del fatto e dei suoi sviluppi potesse lasciare nel lettore l'impressione che il concorrente fosse in effetti implicato in una vicenda non chiara, le autorità giudiziarie slovacche non avevano colto il giusto equilibrio tra il diritto all'informazione e il libero dibattito su questioni di pubblico interesse, per un verso, e le aspettative di tutela del preteso diffamato, per l'altro; né esse avevano esaminato il profilo dell'eventuale buona fede delle pubblicazioni e del grado di diligenza nella selezione delle fonti profuso dai giornalisti nella loro attività. Di qui l'accertamento della violazione dell'art. 10 Cedu (v. nn. 84 e ss. della sentenza).

LA PIÙ RECENTE GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

a) L' annullamento della direttiva sulla conservazione dei dati personali

Con sentenza del 13 maggio 2014, nella cause riunite C-293/12 e C-594/12, la Corte di giustizia dell'Unione europea ha dichiarato invalida la direttiva sulla conservazione dei dati[1] in quanto comportava **un'ingerenza di vasta portata** e di **particolare gravità** nei **diritti fondamentali** al rispetto della vita privata e alla protezione dei dati di carattere personale, **non limitata allo stretto necessario[2].**

In sintesi la normativa oggetto di annullamento prevede che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione **debbano conservare i dati** relativi al **traffico,** all'**ubicazione** e i dati connessi per **identificare l'abbonato** o l'**utente**, mentre **non autorizzano** invece la conservazione del **contenuto** delle comunicazioni e delle informazioni consultate.

La Corte ha preso le mosse dalla considerazione che **i dati** da conservare ai sensi della direttiva in questione (**l'abbonato/utente** vive il **momento e il luogo** da cui ha origine la comunicazione nonché **la frequenza** con cui si comunica con determinate persone nel periodo considerato), **pur non ricomprendendo** il **contenuto** della comunicazione, possono fornire indicazioni circa le **abitudini** quotidiane, i **luoghi di soggiorno** permanente o temporaneo, gli spostamenti giornalieri o di diversa frequenza, le **attività svolte**, le **relazioni** e gli **ambienti sociali** frequentati.

---

1 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.

2 Nel procedimento confluivano le domande in via pregiudiziale trasmesse dall'Alta Corte irlandese e dalla Corte costituzionale austriaca rispettivamente originate da:

- la controversia tra una **società irlandese** per la promozione e la protezione dei diritti civili e dei diritti dell'uomo, in particolare nel contesto delle moderne tecnologie di comunicazione, e diverse **autorità pubbliche irlandesi**, avente ad oggetto la legittimità di misure legislative ed amministrative in attuazione della direttiva citata;
- In particolare, il giudice del rinvio chiedeva alla Corte del Lussemburgo chiarimenti in merito alla compatibilità della direttiva con il **principio di proporzionalità** ex articolo 5, paragrafo 4, TUE considerate, tra l'altro, le tutele in materia di vita privata e di protezione dei dati personali previste agli **articoli 7 e 8 della Carta dei diritti fondamentali** (in linea peraltro con i simili principi contenuti nella **Convenzione europea dei diritti dell'uomo**).
- numerosi ricorsi volti ad annullare la disciplina nazionale austriaca di trasposizione della direttiva citata in quanto in violazione del diritto fondamentale dei privati alla protezione dei propri dati;
- Similmente alla prima domanda, secondo il giudice del rinvio vi erano dubbi sul idoneità della direttiva al raggiungimento degli obiettivi da essa perseguiti e, dall'altro lato, circa la proporzionalità dell'ingerenza nei diritti fondamentali interessati.

La Corte:

- **da un lato**, valuta l'obbligo di conservazione di tali dati e l'accessibilità ad essi da parte delle autorità nazionali quale **ingerenza grave** nei diritti fondamentali**;**
- **dall'altro,** considera tale ingerenza di per sé **non idonea** ad arrecare pregiudizio al **contenuto essenziale** dei diritti fondamentali atteso che **non consente astrattamente l'accesso** al **contenuto** delle comunicazioni e considerato che i fornitori di servizi e di reti debbono rispettare **determinati principi di protezione e di sicurezza dei dati**. Inoltre la Corte ritiene che la conservazione dei dati ai fini della loro eventuale trasmissione alle autorità nazionali competenti **risponde effettivamente a un obiettivo di interesse generale**, vale a dire la **lotta alla criminalità grave** e la salvaguardia della **pubblica sicurezza**.
- **tuttavia** la Corte ritiene **che il legislatore dell'Unione,** con l'adozione della direttiva sulla conservazione dei dati**, abbia ecceduto i limiti** imposti dal rispetto del **principio di proporzionalità.**

In sostanza la Corte ha rilevato che la materia **non è regolamentata in modo da essere effettivamente limitata allo stretto necessario.**

In particolare i rilievi riguardano:

- **l'applicazione generalizzata** della disciplina all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, **senza alcuna differenziazione**, limitazione o eccezione in ragione **dell'obiettivo della lotta contro i reati grav**i;
- la **mancanza di criteri oggettivi** che consentano di garantire che le autorità nazionali competenti abbiano accesso ai dati e possano utilizzarli solamente per prevenire, accertare e perseguire penalmente **reati** che possano essere considerati, tenuto conto della portata e della gravità dell'ingerenza nei diritti fondamentali summenzionati, **sufficientemente gravi** da giustificare una simile ingerenza (la direttiva si limita a fare generico rinvio ai «**reati gravi**» definiti da ciascuno Stato membro nella propria **legislazione nazionale**). La mancanza di **presupposti materiali e procedurali** che consentano alle autorità nazionali competenti di avere **accesso** ai dati e di farne successivo uso, atteso che **tale accesso**, tra l'altro non è nemmeno subordinato al **previo controllo di un giudice** o di un **ente amministrativo indipendente**;
- il regime circa la **durata della conservazione**, fissata tra un **minimo di 6** e un **massimo di 24 mesi** senza che la direttiva precisi **i criteri oggettivi** in base ai quali la **durata** della conservazione debba essere **determinata**, in modo da garantire la sua limitazione allo **stretto necessario** (e senza operare **distinzioni** tra le **categorie di dati** a seconda delle **persone interessate** o dell'eventuale **utilità dei dati** rispetto all'obiettivo perseguito);
- la mancanza di garanzie sufficienti ad assicurare una protezione efficace dei dati contro i **rischi di abusi** e contro qualsiasi **accesso e utilizzo illeciti dei dati**, atteso – tra l'altro - che la direttiva autorizza i fornitori di servizi a tenere conto di **considerazioni economiche** in sede di determinazione del **livello di sicurezza** da

applicare (in particolare per quanto riguarda i costi di attuazione delle misure di sicurezza) e **non garantisce** la **distruzione** irreversibile dei dati al **termine** della loro durata di **conservazione**;

- il fatto che la direttiva **non imponga che i dati siano conservati sul territorio dell'Unione,** non garantendo pertanto la direttiva **il pieno controllo da parte di un'autorità indipendente** del rispetto delle esigenze di protezione e di sicurezza, elemento essenziale del rispetto della protezione delle persone con riferimento al trattamento dei dati personali, considerato tra l'altro che si tratta di requisito **espressamente richiesto dalla Carta**.

b) L'applicabilità della normativa europea ai gestori di motori di ricerca

Con la sentenza del 13 maggio 2014 **la Corte[3] ha stabilito** che:

- **quanto all'ambito territoriale** di applicazione della normativa UE, nonostante il server dell'azienda di elaborazione dati si trovi fisicamente al di fuori dell'Europa, le norme UE si applicano ai motori di ricerca se hanno una succursale o una filiale in uno Stato membro;
- quanto all'**applicabilità delle norme UE** sulla protezione dei dati a un **motore di ricerca**, i gestori dei motori di ricerca devono considerarsi responsabili del trattamento dei dati personali; Google non può quindi sottrarsi alle proprie responsabilità derivanti dalla direttiva europea, nella sua attività di trattamento di dati personali invocando la sua natura di motore di ricerca, ed è soggetto in tal senso alla disciplina europea;
- quanto al diritto di **essere dimenticati** (**oblio**): gli individui hanno il diritto - a determinate condizioni – di chiedere ai motori di ricerca di **rimuovere i collegamenti alle informazioni personali** che li riguardano. Il principio si applica quando le informazioni sono **imprecise**, **inadeguate**, **non** (o non più)

[3] Nel 2010 un cittadino spagnolo presentava all'Agenzia spagnola per la protezione dei dati un **reclamo** nei confronti di un giornale diffuso in Spagna, nonché contro **Google Spagna** e **Google *Inc***.. In sintesi, l'uomo lamentava che gli **annunci di vendita all'asta** (a seguito di pignoramento) risalenti al **1998** e che tuttora comparivano come **risultati del motore di ricerca Google** violavano il suo **diritto alla privacy**, atteso che il procedimento esecutivo nei suoi confronti era stato completamente risolto da un **certo numero di anni** e quindi il **riferimento** alle tesi era diventato del tutto **irrilevante**.
Il cittadino spagnolo chiedeva, in primo luogo, che il giornale fosse obbligato a rimuovere o modificare le pagine in questione in modo che i relativi dati personali non apparissero; in secondo luogo, che Google Spagna o Google Inc. fossero obbligati a rimuovere i dati personali che lo riguardavano, in modo tale che non apparissero più nei risultati di ricerca.
Investita della questione, l'Audiencia Nacional ha proposto alla Corte di giustizia UE **domanda di pronuncia pregiudiziale**, chiedendo in sostanza (Causa C-131/12):

- se la direttiva sulla protezione dei dati del 1995 si **applichi** ai **motori di ricerca** come Google;
- se il diritto dell'Unione (nel caso di specie la direttiva) si applichi a Google Spagna, considerato che il server della società di elaborazione dati **si trova negli Stati Uniti**;
- se un individuo ha il **diritto di chiedere** che i propri dati personali vengano **rimossi** dall'**accessibilità** tramite un **motore di ricerca** (il **'diritto di essere dimenticat**i' o **diritto all'oblio**").

pertinenti, o **eccessive** in rapporto alle **finalità** per le quali **sono state trattate** e al tempo trascorso. La Corte ha inoltre osservato che nella fattispecie specifica **l'interferenza con il diritto della persona** alla protezione dei dati non può essere giustificata meramente **dall'interesse economico** del **motore di ricerca**. Nello stesso tempo la Corte ha chiarito in modo esplicito che il **diritto all'oblio non** è da ritenersi **assoluto**, ma deve sempre essere **bilanciato** con altri **diritti fondamentali** come la libertà di **espressione** e di **informazione**. Occorre dunque una valutazione caso per caso, con particolare riferimento al **tipo di informazione** in gioco, al suo carattere **sensibile** per la **vita privata** dell'individuo e **all'interesse del pubblico** ad accedere a tale informazione, oltre alla **rilevanza** del **ruolo** che riveste una persona nella **vita pubblica.**

LE INIZIATIVE IN CORSO: L'UNIONE EUROPEA

Il pacchetto di riforma in materia di protezione dati: nuovi strumenti e potenziamento di quelli vigenti

Sintetica rassegna dei contenuti principali e sullo stato del negoziato

Il quadro vigente è costituito dalla direttiva 95/46/CE relativa alla **tutela delle persone fisiche** con riguardo al **trattamento dei dati personali**, nonché alla libera circolazione di tali dati, e dalla decisione quadro 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito ambito della **cooperazione giudiziaria e di polizia in materia penale**. Entrambi gli atti normativi citati sono attualmente in **fase di revisione**.

La Commissione europea ha presentato un pacchetto costituito da:

una proposta di regolamento COM(2012)11, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (**regolamento generale sulla protezione dei dati**), volta a sostituire la direttiva 95/46/CE);

una proposta di direttiva COM(2012)10, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, volta a sostituire la decisione quadro 2008/977/GAI citata.

Il pacchetto è all'esame delle Istituzioni europee. Le due proposte sono state oggetto di approvazione in prima lettura da parte della Assemblea plenaria del Parlamento europeo nella sessione dell'11-14 marzo 2014 (vedi infra).

Rispetto all'impianto originario delle proposte pubblicate dalla Commissione europea, il **Parlamento europeo** ha modificato le norme sul coinvolgimento delle imprese (per esempio un motore di ricerca, un social network o un fornitore di cloud): tali soggetti, secondo le nuove norme dovrebbero chiedere un'**autorizzazione preventiva all'autorità nazionale di protezione** dei dati prima di poter **divulgare** i dati personali di un cittadino dell'Unione in uno Stato n**on membro;** l'azienda dovrebbe anche informare la persona interessata della richiesta. Inoltre il testo emendato della riforma prevede che le società che infrangono le regole incorrano in multe **fino a 100 milioni di euro o fino al 5%** del **fatturato mondiale annuo** (si applicherebbe la sanzione più gravosa delle due), laddove la Commissione aveva proposto sanzioni fino a **1 milione di euro o fino al 2%** del fatturato mondiale annuo.

Quanto al **Consiglio**, gli Stati membri **non hanno ancora raggiunto un orientamento comune complessivo** (sulla cui base dovrebbero successivamente svolgersi i negoziati con il Parlamento ai fini della formulazione di un testo di compromesso), sollevando rilievi critici con particolare riferimento alla proposta di regolamento generale protezione dati.

Tra le questioni più rilevanti dibattute al Consiglio si ricorda il tema relativo all'introduzione di uno **sportello unico**, ovvero un'autorità unica in grado di giudicare i casi transnazionali e garantire l'applicazione coerente ed omogenea della normativa,

riducendo gli oneri amministrativi a beneficio delle imprese che operano nel commercio internazionale (*vedi infra).*

Rispetto alla **direttiva 95/46/CE**, la proposta di **regolamento generale sulla protezione dei dati** ne riorganizza il contenuto[4], ampliandolo notevolmente (si passa dai sette capi e 34 articoli della direttiva a 91 articoli suddivisi in undici capi contenuti nella proposta di regolamento.

La Commissione europea ha previsto che le nuove norme UE si applichino anche ai dati personali **trattati all'estero** da **imprese** che sono attive sul mercato unico e **offrono servizi ai cittadini dell'Unione**.

La **proposta di direttiva** COM(2012)10 è diretta a disciplinare la materia del trattamento dei dati personali a fini di **prevenzione e indagine, accertamento e perseguimento di reati ovvero di esecuzioni e sanzioni penali**. I contenuti della proposta di direttiva **corrispondono in larga parte** a quelli della **proposta di regolamento**, fatto salvo il minor dettaglio derivante dalla natura dello strumento giuridico prescelto che implica quasi inevitabilmente l'attribuzione a ciascuno Stato membro di un certo margine di discrezionalità per la definizione di alcuni specifici profili.

Le principali novità in discussione

Consenso esplicito al trattamento

La riforma chiarisce che per "**consenso dell'interessato**" deve intendersi qualsiasi manifestazione di volontà informata ed **esplicita** con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Diritto alla cancellazione e diritto all'oblio

La direttiva del 1995 aveva già previsto uno strumento volto alla cancellazione – a determinate condizioni – dei dati personali.

La riforma amplia le possibilità di esercizio del **diritto alla cancellazione** e **introduce il cosiddetto diritto all'oblio**. In particolare l'interessato (qualora sussistano i motivi indicati nella diposizione: ad esempio, **dati non** più **necessari** per le finalità per cui sono stati trattati, dati **trattati illecitamente**, **revoca del consenso**, **scadenza** del periodo di **conservazione**, etc.) avrà il **diritto di ottenere** dal responsabile del trattamento **la cancellazione di dati personali** che lo riguardano e **la rinuncia a un'ulteriore diffusione di tali dati**.

Qualora abbia reso pubblici dati personali, il responsabile del trattamento di è tenuto ad **informare i terzi** che stanno trattando tali dati **della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi**

[4] Per l'approfondimento si rinvia alla Scheda di valutazione n. 22/2012 del Servizio Affari internazionali -Ufficio dei rapporti con le istituzioni dell'Unione europea del Senato, e al Dossier di documentazione n. ES 120 "Nuovo quadro giuridico per la protezione dei dati personali nell'Unione europea" del 19 marzo 2012 dell'Ufficio Rapporti con l'Unione europea della Camera dei deputati.

dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è **ritenuto responsabile di tale pubblicazione**.

*Si segnala che il Parlamento europeo ha proposto una serie di emendamenti volti a **rafforzare la previsione indicata**. In particolare con la risoluzione legislativa detta è, tra l'altro, stabilito l'obbligo per il responsabile del trattamento di **assicurare la cancellazione di tali dati**, ed è altresì introdotta la previsione del diritto alla cancellazione dei dati qualora tale **misura sia decisa in via definitiva da un tribunale** o da **un'autorità di regolamentazione** con sede nell'Unione*.

Esimenti

Similmente alla direttiva vigente, sono previste dalla riforma **eccezioni** all'obbligo di cancellazione, in particolare ,ove la conservazione dei dati sia necessaria per: l'esercizio del **diritto alla libertà di espressione;** motivi di **interesse pubblico nel settore della sanità pubblica,** per finalità **storiche, statistiche e di ricerca scientifica;** adempiere un **obbligo legale** di conservazione di dati personali previsto dal diritto dell'**Unione** o dello **Stato membro** cui è soggetto il responsabile del trattamento (il diritto dello Stato membro deve perseguire un **obiettivo di interesse pubblico**, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo). Sono altresì previste fattispecie in cui i responsabile invece di provvedere alla cancellazione è tenuto alla **limitazione** del trattamento dei dati personali.

Diritto alla portabilità dei dati

La riforma introduce il diritto dell'interessato alla portabilità dei dati, vale a dire il **diritto di trasferire i propri dati** da un sistema di trattamento elettronico a un altro, senza che il responsabile del trattamento possa impedirlo. Secondo la Commissione il diritto alla portabilità dei dati, grazie al quale ad esempio dovrebbe essere possibile da un service provider, come i social network, a un altro (allo stesso modi in cui è oggi possibile trasferire il o numero telefonico quando si cambia gestore) dovrebbe comportare un **miglioramento della concorrenza** tra i servizi.

Divieto di profiling

La nuova disciplina sancisce il **diritto di non essere sottoposto a misure basate sulla profilazione** (in sostanza, i tentativi di analizzare o prevenire il comportamento di una persona ad esempio sul posto di lavoro, la situazione economica, la posizione). Ampliando il contenuto della direttiva 95/46/CE, sulla base della raccomandazione del Consiglio d'Europa sulla profilazione: si stabilisce che chiunque ha il diritto di non essere sottoposto a una **misura** che produca **effetti giuridici** o significativamente **incida** sulla sua persona, basata unicamente su un **trattamento automatizzato** destinato a **valutare** taluni aspetti

della sua **personalità** o ad **analizzarne** o **prevederne** in particolare il rendimento professionale, la situazione economica, **l'ubicazione**, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento.

La proposta consente le pratiche di profilazione **soltanto** se il trattamento:

a) è effettuato nel **contesto della conclusione o dell'esecuzione di un contratto**, oppure
b) è espressamente autorizzato da disposizioni del diritto dell'Unione o di uno Stato membro che precisi altresì misure adeguate a salvaguardia dei legittimi interessi dell'interessato, oppure
c) si basa **sul consenso dell'interessato**.

Il responsabile della protezione dei dati personali

La riforma introduce la figura **obbligatoria** del **responsabile** della **protezione dei dati** per il **settore pubblico** e, nel settore privato, per le **grandi imprese** o allorquando le attività principali del responsabile del trattamento e dell'incaricato del trattamento consistono in trattamenti che richiedono il controllo regolare e sistematico degli interessati.

Si segnala che rispetto al testo presentato dalla Commissione, che fissa un parametro dimensionale delle grandi imprese (250 dipendenti) per l'attivazione dell'obbligo di nomina della figura indicata, il Parlamento europeo ha adottato una serie di emendamenti la cui ratio consiste nel fatto che, nell'epoca del "cloud computing", il livello minimo per la nomina obbligatoria di un responsabile della protezione dei dati ***non dovrebbe basarsi sulle dimensioni dell'impresa****, ma piuttosto sulla* ***pertinenza del trattamento dei dati*** *(categoria di dati personali, tipo di attività di trattamento e numero di individui i cui dati sono oggetto di trattamento).*

Lo sportello unico per il controllo della protezione dei dati

La riforma mira a riscrivere anche la disciplina in materia di **autorità di controllo indipendenti** (la cui istituzione è già prevista dalla disciplina vigente, in particolare **potenziandone il ruolo con l'attribuzione dei nuovi poteri di sanzione** di illeciti amministrativi, nonché stabilendo una forma di coordinamento attraverso la previsione della nuova competenza di **autorità capofila** nel caso di un responsabile del trattamento o incaricato del trattamento stabilito in più Stati membri, al fine di assicurare un'attuazione uniforme della disciplina (cosiddetto **sportello unico**).

La Commissione ritiene che la creazione di uno "sportello unico" per il controllo della protezione dei dati possa rafforzare il mercato interno, in particolare grazie all'eliminazione delle divergenze tra le formalità amministrative, stimando un ***risparmio globale di circa 2,3*** *miliardi di euro all'anno.*

Il tema dello sportello unico è stato oggetto di particolare approfondimento in seno al Consiglio de Ministri competenti dell'UE; alcuni Stati membri hanno infatti espresso perplessità sull'attribuzione di ***poteri correttivi esclusivi*** *all'Autorità garante dello Stato membro dello* ***stabilimento principale*** *(nei casi in cui sia sotto osservazione un'impresa con sedi e attività dislocate in più Stati membri), poiché ciò potrebbe limitare l'accesso dei cittadini a mezzi adeguati di ricorso giurisdizionale (obbligati ad andare all'estero per contestare una decisione di un'autorità straniera).*

Il trasferimento dei dati all'estero

La riforma prevede che il trasferimento debba essere subordinato alla preventiva adozione, da parte della Commissione, di una **decisione** che verifichi **l'adeguatezza** del livello di **protezione** accordato dallo **Stato terzo destinatario** delle informazioni; è peraltro previsto che anche in assenza di una decisione della Commissione si possa procedere al trasferimento purché si verifichino talune circostanze che nella proposta di regolamento sono puntualmente indicate.

La discussione sulle attività di sorveglianza dei dati di massa

Le iniziative presso le Istituzioni europee e il dialogo transatlantico

A seguito della divulgazione da parte di alcuni organi di comunicazione delle notizie relative al cosiddetto **scandalo Datagate** (con particolare riferimento ai casi PRISM, Tempora, e ad analoghi programmi di sorveglianza informatica), le Istituzioni europee hanno intrapreso alcune iniziative volte ad approfondire l'effettiva portata di alcuni programmi di intelligence utilizzati dagli Stati Uniti e da alcuni Stati membri.

In estrema sintesi, secondo quanto riportato dagli organi di stampa, la National Security Agency (NSA) statunitense, grazie al programma PRISM, avrebbe ottenuto **la fornitura di dati** (ad esempio email, file, notifiche di accesso, etc.) da parte delle **principali aziende tecnologiche USA** che gestiscono informazioni, comunicazioni e dati-utente in formato digitale (anche relativamente a **cittadini UE**). Lo scandalo si è ulteriormente arricchito con la diffusione di notizie secondo le quali l'Agenzia del Governo americano **avrebbe violato le reti informatiche** delle stesse **Istituzioni europee e degli Stati membri**. Infine, ulteriori rivelazioni sono emerse in ordine ad eventuali **intercettazioni della NSA** di dati internazionali sui **bonifici bancari** gestiti dal consorzio SWIFT. Ulteriori motivi di preoccupazione sono altresì sorti in relazione al programma di intelligence **Tempora**, seguito dai **servizi britannici**.

Al riguardo, le Istituzioni europee hanno sin da subito sollevato due ordini di critiche, afferenti: al **corretto svolgimento delle relazioni internazionali diplomatiche**; alla violazione **della sfera dei diritti fondamentali dei cittadini UE** (con particolare riferimento alla **protezione dei dati personali)**.

A seguito delle richieste di chiarimenti della Commissione europea (in particolare della Vicepresidente/Commissaria per la Giustizia Viviane Reding al segretario alla giustizia (Attorney general) degli Stati Uniti, Eric Holder, il 14 giugno 2013, si teneva a Dublino un vertice USA-UE dei responsabili dei settori della giustizia e affari interni, in esito al quale istituiva un **gruppo transatlantico** (UE- USA) **di esperti di sicurezza e di privacy**, con il compito di approfondire le questioni non ancora chiarite relative al programma PRISM.

L'attività della Commissione

Il 27 novembre 2013 la Commissione europea ha presentato una serie di documenti relativi alle **azioni da intraprendere per ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA**. L'iniziativa della Commissione comprende: **a)** un'analisi del funzionamento dell'accordo "**Approdo sicuro**" che regola il trasferimento di dati a scopo commerciale fra l'UE e gli USA; **b)** una relazione **sui risultati del gruppo di lavoro UE-USA** sulla protezione dei dati, costituito nel luglio 2013; **c)** una relazione di valutazione sul **programma di controllo delle transazioni finanziarie dei terroristi** (Terrorist Finance Tracking Programme, TFTP); **d)** una relazione sulla **verifica congiunta dell'accordo con gli USA sui dati del codice di prenotazione** (Passenger Name Record, PNR).

Il C.D Safe Harbour

L'Accordo sull'approdo sicuro è un accordo concluso nel 2000 tra Unione europea e Stati Uniti per garantire la protezione dei dati dei cittadini europei, **anche quando i dati sono in possesso di aziende americane**, **fuori dal territorio europeo**; tale accordo chiedeva il rispetto dei principi di privacy europei alle azienda americane che utilizzavano o raccoglievano dati europei.

Il funzionamento dell'accordo si basa sulla richiesta di **autocertificazione** alle aziende americane circa il rispetto delle regole.

A seguito di una verifica da parte di esperti dell'UE e degli Stati Uniti, la Commissione è giunta alla conclusione che le autorità statunitensi hanno applicato l'accordo nel rispetto delle norme e delle condizioni contenute. La prossima revisione congiunta avrà luogo nel primo semestre del 2015.

Programma di controllo delle transazioni finanziarie dei terroristi (TFTP)

Il programma controllo TFTP consente di raccogliere informazioni relative alla messaggistica finanziaria, in particolare, **informazioni relative all'identità dell'ordinante e/o beneficiario di una transazione, compreso il nome, il numero di conto, l'indirizzo e il numero d'identificazione nazionale**. L'accordo TFTP tra l'Unione europea e gli Stati Uniti è entrato in vigore il 1° agosto 2010. L'accordo contempla misure che garantiscono la protezione dei dati dei cittadini dell'UE e prevede una verifica periodica delle disposizioni "riguardanti le salvaguardie, i controlli e la reciprocità.

In sintesi, la Commissione ha proposto azioni in sei ambiti:

- adottare rapidamente la **riforma europea sulla protezione dei dati**;
- rendere **più sicuro** il regime "Approdo sicuro**":** in tale ambito la Commissione ha formulato alcune raccomandazioni volte a garantire la **trasparenza** delle politiche in materia di privacy dei membri dell'Approdo sicuro (le imprese del web), nonché **l'applicazione dei principi in materia di riservatezza** da parte delle imprese negli Stati Uniti e il carattere effettivo dell'applicazione;
- rafforzare **le salvaguardie** in materia di protezione dei dati nel **settore delle attività di contrasto:** in particolare la Commissione ha evidenziato la necessità di concludere rapidamente gli attuali negoziati su un **accordo quadro per i trasferimenti e il trattamento dei dati nell'ambito della cooperazione di polizia e giudiziaria** (la Commissione ha insistito sulla necessità che i cittadini dell'UE non residenti negli Stati Uniti possano avvalersi di meccanismi di ricorso giudiziario);
- usare **la reciproca assistenza giuridica e gli accordi settoriali** per ottenere i **dati**: in particolare, secondo la Commissione, occorre che l'amministrazione americana si impegni, in linea di principio, a utilizzare un quadro giuridico come la reciproca assistenza giuridica e gli accordi settoriali UE-USA, quali quelli sui dati del codice di prenotazione e sul programma di controllo delle transazioni finanziarie dei terroristi, ogni volta che i trasferimenti di dati sono richiesti a fini di attività di contrasto;
- affrontare le preoccupazioni europee sul **processo di riforma statunitense** in corso, con particolare riferimento al processo di revisione annunciato dal Presidente americano Obama delle attività delle autorità nazionali di sicurezza statunitensi; in particolare, la Commissione europea ha posto l'accento sul fatto che i cambiamenti

più importanti dovrebbero essere **l'estensione**, ai **cittadini europei non residenti negli USA**, delle **garanzie** di cui godono i **cittadini americani**, una maggiore trasparenza e un migliore controllo;

- promuovere **a livello internazionale le norme sulla privacy:** secondo la Commissione europea occorre che gli Stati Uniti aderiscano alla **Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale** ("Convenzione 108"), così come hanno aderito alla Convenzione sulla criminalità informatica del 2001.

*La Commissione europea ha invece escluso di voler far rientrare le norme sulla protezione dei dati **nei negoziati** in corso per una partnership per gli **scambi e gli investimenti transatlantici.***

L'attività del Parlamento europeo

Anche **il Parlamento** ha espresso preoccupazione per il programma PRISM e per gli altri programmi di sorveglianza (degli stati Uniti e di alcuni Stati membri), e condannato le azioni di spionaggio ai danni delle rappresentanze dell'Unione, chiedendo alle autorità statunitensi di fornire informazioni sulle vicende in questione senza ritardi.

Con una risoluzione del 4 luglio 2014 il Parlamento ha inoltre incaricato la Commissione parlamentare per le libertà civili - LIBE di avviare **un'indagine approfondita** sui programmi di **sorveglianza degli Stati uniti** (**e di quelli degli Stati membri**).

I **principali risultati** dell'inchiesta sono stati presentati in una serie di documenti di lavoro[5] nonché nella relazione adottata dalla LIBE il 21 febbraio 2014, secondo la quale vi sarebbero **prove convincenti** riguardo l'**esistenza di sistemi** complessi tecnologicamente avanzati e di vasta portata progettati da **servizi segreti americani e di alcuni Stati membri** volti a raccogliere, archiviare e analizzare **i dati di comunicazione** (compresi i dati contenuti, i dati di posizione e i metadati) di cittadini di tutto il mondo, su una scala senza precedenti e in modo indiscriminato.

Il 12 marzo 2014 l'Assemblea plenaria del Parlamento europeo ha approvato a larghissima maggioranza (544 voti favore contro 78) **la risoluzione conclusiva del lavoro d'inchiesta** recante **conclusioni e raccomandazioni per migliorare la tutela della privacy dei cittadini UE**.

[5] In particolare: il Documento di lavoro di lavoro concernente i programmi di sorveglianza degli USA e dell'UE e il loro impatto sui diritti fondamentali dei cittadini dell'UE; il documento di lavoro sul controllo democratico dei servizi di intelligence degli Stati membri e degli organismi di intelligence dell'UE; il documento di lavoro sulla relazione tra le prassi di sorveglianza nell' UE e negli Stati Uniti e le disposizioni dell'UE sulla protezione dei dati; il documento di lavoro sulle attività di sorveglianza degli Stati Uniti relativamente ai dati dell'UE e sulle possibili implicazioni per gli accordi e la cooperazione transatlantica.

Secondo la risoluzione il consenso del Parlamento **all'accordo finale sul commercio e gli investimenti (TTIP) con gli Stati Uni**ti "potrebbe essere **minacciato** fino a quando la coltre delle attività della sorveglianza di massa, le intercettazioni delle comunicazioni nelle istituzioni dell'UE e le rappresentanze diplomatiche non saranno completamente fermate"; gli eurodeputati hanno concluso quindi che il Parlamento dovrebbe, pertanto, **rifiutare il suo consenso all'accordo TTIP finché non siano pienamente rispettati i diritti fondamentali UE**, aggiungendo che la protezione dei dati dovrebbe essere comunque esclusa dai negoziati commerciali.

I deputati, inoltre, hanno chiesto **l'immediata sospensione** dei **principi sulla privacy del Safe Harbou**r in quanto tali principi non provvedono a un'adeguata protezione dei cittadini europei; gli eurodeputati hanno inoltre esortato gli Stai Uniti a proporre nuove regole per il trasferimento dei dati personali che soddisfino i requisiti UE.

Secondo la risoluzione anche il **programma finanziario di controllo del terrorismo** (TFTP) **dovrebbe essere sospeso** finché le accuse nei confronti delle autorità statunitensi riguardo l'accesso a dati bancari dei cittadini europei fuori dal contratto siano chiarite, insistono i deputati.

La risoluzione prevede inoltre un "**Programma europeo di protezione informatori**", che dovrebbe prestare particolare attenzione alla "complessità della denuncia delle irregolarità nel campo dell'intelligence". Si invitano dunque gli Stati membri a esaminare la **possibilità di concedere agli informatori** ("whistleblowers") **protezione internazionale**.

I deputati chiedono, inoltre, "un nuovo corso digitale" in UE ed evidenziano che l'Europa dovrebbe **sviluppare una propria cloud e soluzioni IT**, includendo tecnologie di sicurezza informatica e crittografia per assicurare un alto livello di protezione di dati.

La net neutrality – principi di libera fruizione di servizi e contenuti della rete

Regole comuni per la neutralità della rete[6] sono state inserite nel pacchetto "Un continente connesso" presentato dalla Commissione a settembre 2013 e composto da una comunicazione che illustra e giustifica l'intervento legislativo, in vista dell'obiettivo del **mercato unico delle telecomunicazioni**, e una proposta di regolamento che: **semplifica il regime di autorizzazione e le norme UE per gli operatori delle telecomunicazioni**; **elimina i costi del *roaming***; **abolisce la maggiorazione del prezzo delle chiamate internazionali in Europa**; **aumenta il livello di tutela dei diritti dei consumatori**; garantisce condizioni di assegnazione prevedibili e tempistiche coordinate per l'**accesso allo spettro delle frequenze**. Completa il pacchetto una raccomandazione, che intende promuovere la concorrenza e incoraggiare gli investimenti nelle reti ad alta velocità, garantendo la stabilità a lungo termine dei

[6] Con neutralità della rete si intende il principio in base al quale tutto il traffico internet riceve lo stesso trattamento, senza discriminazioni, restrizioni o interferenze, indipendentemente dalla fonte, dalla destinazione, dal tipo, dai contenuti, dal dispositivo, dal servizio o dall'applicazione.

prezzi di accesso alle reti in rame e assicurando condizioni di parità ai richiedenti l'accesso alle reti degli operatori storici.

Per quanto riguarda la neutralità della rete, sulla base delle disposizioni dell'articolo 23 della proposta di regolamento (su *Libertà di fornire e di usufruire di un accesso a internet aperto e gestione ragionevole del traffico)* **ai fornitori di servizi sarà vietato bloccare, rallentare, degradare o discriminare specifici contenuti, applicazioni o servizi di internet**. Agli utenti andrà garantito un accesso alla rete completo e aperto, indipendentemente dal costo dell'abbonamento o dalla velocità della connessione, fatta eccezione per i casi in cui sarà necessario applicare misure di gestione ragionevole del traffico. Tali misure dovranno essere trasparenti, non discriminatorie, proporzionate e necessarie a:

- attuare una disposizione legislativa o un provvedimento giudiziario, oppure impedire od ostacolare reati gravi;
- preservare l'integrità e la sicurezza della rete, dei servizi erogati tramite tale rete, e dei terminali degli utenti finali;
- impedire la trasmissione di comunicazioni indesiderate agli utenti che abbiano espresso previamente il loro consenso a tali misure restrittive;
- minimizzare gli effetti di una congestione della rete temporanea o eccezionale, purché tipologie di traffico equivalenti siano trattate allo stesso modo.

Le imprese del ramo potranno ancora fornire "servizi specializzati" di qualità avanzata (quali la TV via internet, i servizi di video su richiesta, le applicazioni per la diagnostica per immagini ad alta risoluzione, per le sale operatorie virtuali e per i servizi *cloud* ad alta intensità di dati), purché ciò non interferisca con la velocità di connessione a internet promessa ad altri clienti. I consumatori avranno il diritto di verificare se la velocità di connessione corrisponde effettivamente alla tariffa pagata e di recedere dal contratto se le condizioni pattuite non sono rispettate.

La citata proposta di regolamento è stata **esaminata in prima lettura dal Parlamento europeo**, che il 3 aprile 2014 ha approvato una risoluzione legislativa, introducendo alcune modifiche al testo della Commissione. In particolare, si **rafforza il principio di neutralità della rete**, specificando che l'accesso ad Internet deve essere garantito, "indipendentemente dalla sede dell'utente finale o del fornitore e dalla localizzazione, dall'origine o dalla finalità del servizio, delle informazioni o dei contenuti".

Inoltre, il Parlamento europeo ha **limitato la possibilità di fornire servizi specializzati agli utenti finali**: la capacità della rete deve essere sufficiente per fornire tali servizi in aggiunta ai servizi di accesso a internet e non deve essere pregiudicata la disponibilità o la qualità dei servizi di accesso a internet.

LE INIZIATIVE IN CORSO: GLI ORDINAMENTI NAZIONALI

Italia

Diritto alla cancellazione e diritto all'oblio

Il Presidente dell'Autorità Garante dei dati personali, in occasione della presentazione – il 10 giugno 2014 - della relazione 2013, ha osservato che l'equilibrio tra tecnologie e tutela dei diritti fondamentali nello spazio digitale deve trovare un'efficace risposta ultrastatuale.

Ha inoltre evidenziato il rilievo del ricorso, sul piano nazionale, a protocolli d'intesa tra la stessa Autorità Garante e i soggetti coinvolti nella raccolta dei dati, quali l'*intelligence* o la magistratura inquirente.

In questo quadro, dopo che il Garante della privacy aveva registrato un notevole aumento di richieste di intervento in materia di diritto all'oblio in Internet, la **Corte di cassazione** ha avuto il suo primo *landmark case* (la **sentenza 5 aprile 2012, n. 5525**) che anticipa parzialmente le posizioni della Corte di giustizia UE emerse con la nota decisione del 13 maggio 2014 nella causa Google-Spain.

Il caso discusso davanti alla Suprema Corte è emblematico. Una persona nota aveva chiesto senza successo al Garante prima, e all'autorità giudiziaria poi, di ordinare a un editore (RCS) l'aggiornamento di un vecchio articolo presente nell'archivio on-line del Corriere della Sera (e comparente ai primi posti nelle ricerche fatte in "Google" usando il nome e cognome del ricorrente) che dava conto di un suo arresto, senza ovviamente dare conto – perché all'epoca non era ancora intervenuto – del suo successivo proscioglimento da ogni accusa. Il giudice di merito aveva negato la tutela sulla base della considerazione che la notizia, all'epoca in cui era stata data, era veritiera e di pubblico interesse, per cui la sua pubblicazione aveva costituito legittimo esercizio del diritto di cronaca; mentre la presenza attuale dell'articolo in Internet assolveva a una funzione storico-documentaristica, che sarebbe stata tradita da un'integrazione del testo, la quale avrebbe fatto venir meno il valore di documento storico dell'articolo. Era, anzi, arrivato ad escludere in radice l'esistenza di un diritto all'oblio del ricorrente, dato il suo status di personaggio pubblico, e di conseguenza la sussistenza di "un persistente interesse pubblico all'apprendimento di notizie relative alla storia personale, anche giudiziaria, dell'interessato". La Corte ha quindi concluso per la sussistenza nel caso di specie di un obbligo a carico dell'editore di predisporre un sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia, consentendone il rapido accesso. Quasi di passaggio, la Corte ha peraltro rilevato che il fornitore del servizio di motore di ricerca non avesse alcun ruolo o responsabilità nella vicenda, spettanti invece al responsabile del sito sorgente, e rigettando così una delle difese dell'editore, che aveva sostenuto il proprio difetto di legittimazione passiva in favore di Google.

La Corte Suprema ha riconosciuto espressamente l'esistenza di un diritto all'oblio, inteso nel senso di cui sopra di diritto alla tutela della propria (attuale) identità personale

e morale nella sua proiezione sociale. Ha rimarcato la differenza tra un archivio in senso tradizionale e la Rete, dove tutte le notizie sono presentate in maniera non strutturata, "piatta", e decontestualizzate. Ha osservato che se la finalità di documentazione storica può legittimare, dal punto di vista del Codice della privacy, la conservazione e pubblica accessibilità dell'articolo che riporta una determinata notizia e la persistente identificabilità del protagonista – la non eccedenza e persistente compatibilità del trattamento dei dati rispetto al legittimo fine del trattamento stesso è uno dei capisaldi del diritto della privacy – è però coerente con questa finalità, e al tempo stesso rispettoso del diritto all'oblio, che la notizia sia aggiornata e contestualizzata, o financo cancellata dall'archivio, se non risponde più a verità. Si può osservare incidentalmente che, quando la tutela assume questa seconda (estrema) forma, viene ripristinata la coincidenza tra l'espressione "diritto all'oblio" e il contenuto del diritto stesso.

La Corte ha quindi concluso per la sussistenza nel caso di specie di un obbligo a carico dell'editore di predisporre un sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia, consentendone il rapido accesso. Quasi di passaggio, la Corte ha peraltro rilevato che il fornitore del servizio di motore di ricerca non avesse alcun ruolo o responsabilità nella vicenda, spettanti invece al responsabile del sito sorgente, e rigettando così una delle difese dell'editore, che aveva sostenuto il proprio difetto di legittimazione passiva in favore di Google.

Sulla base della sentenza Cella cassazione, tra il dicembre 2012 e il gennaio 2013 **il Garante ha accolto due ricorsi** prescrivendo all'editore di segnalare con un'annotazione a margine dell'articolo l'esistenza dello "sviluppo" della notizia, in modo da assicurare da un lato, all'interessato, il rispetto della propria attuale identità personale, e dall'altro, ad ogni lettore, un'informazione attendibile e completa. Si noti che si trattava di articoli già precedentemente de-indicizzati.

Ma anche i giudici ordinari si sono adeguati a tale linea (**sentenza 26 giugno 2013, n. 5820** del **Tribunale di Milano)** in relazione a un caso che presenta diverse analogie con quello deciso dalla Cassazione. L'attore qui lamentava la perdurante presenza in Rete – nell'**archivio on-line di un quotidiano** a diffusione nazionale e, a cascata, nei motori di ricerca – di un articolo del 1985 in cui lo si descriveva come **usuraio ed evasore** e lamentava, oltre che la diffamazione, la violazione del proprio diritto all'oblio.

Il giudice milanese ha escluso la diffamazione per prescrizione, ma **ha riconosciuto la lesione del diritto all'oblio**, ritenuto prevalente su ogni altro ipotetico interesse. In particolare, ha osservato che i fatti addebitati all'attore erano risultati essere non tutti veri; che difettava il requisito dell'interesse pubblico alla loro permanente conoscenza, dato il lasso di tempo trascorso dalla vicenda e la carenza di un qualche ruolo di rilevo pubblico dell'attore; e che mancava il perseguimento di un'apprezzabile finalità, tale da giustificare l'identificabilità in Rete dell'attore in relazione al fatto storico, considerato che lo scopo di tenuta dell'archivio può essere soddisfatto con la conservazione di una copia cartacea. Ricordando che la Cassazione aveva ipotizzato come misura estrema di tutela quella della radicale cancellazione dell'articolo dalla Rete, il giudice ha ritenuto che nel caso sottoposto al suo esame fosse proprio questo il rimedio più appropriato, data la carenza nella fattispecie di apprezzabili interessi da contrapporre alla tutela dell'identità personale. Ha dunque ordinato la rimozione dell'articolo dall'archivio telematico del giornale, consentendo solo la tenuta di una copia cartacea, e condannato l'editore al risarcimento del danno morale.

Divieto di profiling

Il Garante della privacy - con un recente ***Provvedimento generale*** (adottato al termine di una consultazione pubblica) pubblicato sulla Gazzetta ufficiale del 3 giugno u.s. - ha previsto che l'installazione di cookie per finalità di profilazione e marketing da parte dei gestori dei siti non può avvenire senza prima aver informato gli utenti e aver ottenuto il loro consenso. Chi naviga in Internet potrà quindi decidere in maniera libera e consapevole se far usare o no le informazioni raccolte sui siti visitati per ricevere pubblicità mirata. Il provvedimento individua modalità semplificate per rendere agli utenti l'informativa on line sull'uso dei cookie e fornisce indicazioni per acquisire il consenso, quando richiesto dalla legge. Ai cookie si riferisce l'art. 122 del Codice della privacy (D.Lgs 196/2003) laddove prevede che "l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalita' semplificate di cui all'art. 13, comma 3, del Codice).

La **procedura semplificata** consentirà agevolmente ai navigatori di manifestare un consenso libero e consapevole".

Per proteggere la privacy degli utenti e consentire loro scelte più consapevoli, il Garante ha dunque stabilito che, d'ora in poi quando si accede alla home page o ad un'altra pagina di un sito web deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente:

1) che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
2) che il sito consente anche l'invio di cookie di "terze parti", ossia di cookie installati da un sito diverso tramite il sito che si sta visitando;
3) un link a una informativa più ampia, con le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti";
4) l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un cookie tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente.

L'utente mantiene, comunque, la possibilità di modificare le proprie scelte sui cookie attraverso l'informativa estesa, che deve essere linkabile da ogni pagina del sito. A mero titolo di esempio, il Garante ha predisposto un modello di banner disponibile sul proprio sito www.garanteprivacy.it

La responsabilità dei prestatori dei servizi on line*: il caso della tutela del diritto d'autore*

Con riferimento al tema della responsabilità dei prestatori di servizi *on line* nei confronti dei contenuti immessi nella Rete, in Italia assume rilievo l'entrata in vigore, il 31 marzo 2014, del regolamento in materia di tutela del diritto d'autore

sulle reti di comunicazioni elettroniche approvato dall'Autorità per le garanzie nelle comunicazioni (Agcom) con la delibera 680/13/Cons.

Il regolamento prevede infatti, tra le altre cose, una procedura, alternativa a quella giurisdizionale, per la rimozione dei contenuti illegali (articoli 6-14). Tale procedura contempla: 1) l'istanza all'Autorità da parte dei soggetti legittimati per ottenere la rimozione di un'opera digitale resa disponibile su Internet ovvero di un contenuto inserito in un palinsesto televisivo in violazione della legge sul diritto d'autore; 2) l'avvio da parte dell'Autorità di un procedimento amministrativo il quale, dopo una fase in cui l'interessato può controdedurre (ordinariamente entro cinque giorni, in situazioni di presunta grave lesione entro tre giorni) rispetto alla contestazione mossa, si può concludere: a) per le pagine Internet con la rimozione spontanea da parte del gestore della pagina dei contenuti illegali, ovvero, in caso di mancata rimozione, con **l'ordine ai prestatori di servizi che svolgono attività di *hosting* di provvedere, di norma, alla rimozione selettiva delle opere digitali, ovvero, in presenza di violazioni massive, alla disabilitazione dell'accesso;** in caso di inottemperanza, si prevede l'applicazione della sanzione amministrativa pecuniaria prevista dall'articolo 1, comma 31, della legge n. 249/1997 (art. 8); b) per i servizi di media audiovisivi, la diffida dal trasmettere i contenuti illegali, ovvero in caso di mancata rimozione, **l'ordine al fornitore di servizi di media lineari (tv generalista) e non lineari (piattaforme tipo Sky) di adottare ogni misura necessaria ad inibire la diffusione di tali programmi o cataloghi al pubblico italiano** (art. 14); in caso di inottemperanza, è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'articolo 1, comma 31, della legge n. 249/1997 (art. 13)

Trattandosi di un provvedimento amministrativo, è possibile contro le decisioni dell'Autorità il ricorso alla giustizia amministrativa (art. 17); è inoltre contemplata la possibilità di ricorrere, in alternativa, all'autorità giudiziaria (art. 6).

In base a notizie di stampa, contro il regolamento sono stati avanzati da associazioni di difesa dei consumatori e degli operatori del settore, nonché da parte di soggetti economici operanti nel settore, ricorsi al TAR del Lazio e un ricorso straordinario al Capo dello Stato. Oggetto dei ricorsi sarebbero i seguenti profili:

- viene messo in discussione se i poteri di regolazione in materia di tutela del diritto d'autore riconosciuti all'Agcom dal decreto legislativo n. 44/2010 (c.d. "decreto Romani") possano estendersi fino alla configurazione del procedimento "paragiurisdizionale" previsto dal regolamento e delle sue eventuali conseguenze sanzionatorie, che giungono fino alla rimozione dei contenuti; l'attribuzione di poteri di regolazione in materia all'Agcom potrebbe inoltre costituire, ad avviso di alcuni ricorrenti, un eccesso di delega rispetto a quanto previsto dalla legge comunitaria 2008 (L. n. 88/2009) che contemplava il recepimento della direttiva 2007/65/CE

- con riferimento in generale agli Internet Service Provider, la possibilità di richiedere da parte dell'Agcom, ai sensi dell'articolo 17 del decreto legislativo n. 70/2003, in quanto autorità amministrativa con funzioni di vigilanza, la rimozione del contenuto illegale, appare interpretata estensivamente nel momento in cui si prefigura l'ordine ai fornitori dei servizi di hosting della rimozione dei contenuti[7].

Sulla base del regolamento, l'Agcom ha, alla data del 6 giugno 2014, avviato ventotto provvedimenti. In diciassette casi il provvedimento risulta già concluso. Di questi, in otto casi è stata decisa l'archiviazione; in quattro casi si sono avuti adeguamenti spontanei da parte dei soggetti destinatari del provvedimento, mentre in cinque casi l'Autorità ha ordinato ai prestatori di servizi *on line* la disabilitazione dell'accesso ai siti destinatari del provvedimento.

La net neutrality nell'ordinamento italiano

In Italia il principio delle neutralità della Rete si è affermato principalmente in via "giurisprudenziale", in particolare a seguito della decisione dell'Autorità garante della concorrenza e del mercato di sanzionare come pratica commerciale scorretta ai sensi del Codice del consumo (Decreto legislativo n. 206/2005) l'omessa informazione agli utenti sull'utilizzo di sistemi di filtraggio su linee ADSL che limitano l'accesso ad alcuni siti Internet e programmi *peer to peer* (decisione AGCM 18 dicembre 2008, PS540 *Tele2 – Filtri di utilizzo*). Più recentemente, sul tema della neutralità della Rete meritano di essere segnalate, in Italia, le conclusioni della consultazione pubblica svolta dall'Autorità per le garanzie nelle comunicazioni e terminata nel gennaio 2012.

Le conclusioni registrano, tra le altre cose, un vasto consenso dei soggetti consultati sui seguenti aspetti:

- le politiche di *pricing* e di *traffic management* (vale a dire le politiche che variano i canoni di accesso ad Internet in base alla velocità di connessione) non rappresentano di per sé una violazione dei principi cardine della "neutralità della Rete" individuati nella libertà, equità, efficienza, trasparenza delle offerte e non discriminazione;
- la presenza, nel contesto italiano, di previsioni normative sufficienti ad assicurare un'adeguata protezione degli utenti;

[7] Su questo aspetto vedi anche la recente sentenza della Corte di Giustizia dell'Ue nella causa C-314/12, del 27 marzo 2014, che, da un lato, ha riconosciuto al fornitore di accesso ad Internet la qualifica di intermediario e, dall'altro lato, ha affermato che i diritti fondamentali dell'Unione consentono che possa essere vietato, con un'ingiunzione pronunciata da un giudice (quale quella del caso concreto esaminato dalla Corte, accaduto in Austria), a un fornitore di accesso ad Internet di mettere a disposizione materiali non conformi alle regole sul diritto d'autore, qualora tale ingiunzione non specifichi quali misure il fornitore deve adottare e sia consentito al fornitore di evitare le sanzioni nel caso in cui dimostri di avere adottato tutte le misure disponibili (e purché ciò non si traduca in limitazioni per gli utenti Internet di accesso in modo lecito alle informazioni).

- l'opportunità di verificare la necessità di ulteriori interventi regolamentari per assicurare informazioni accurate agli utenti in materia di *traffic management*
- l'opportunità di un approfondimento in ordine al rapporto tra neutralità della Rete e libertà della Rete.

Francia

Il primo gennaio 2010, dopo un iter durato quasi due anni, è entrata in vigore la legge francese «*Création et Internet*», comunemente denominata legge *Hadopi*, acronimo di *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet*, l'autorità preposta al controllo dei comportamenti degli utenti di Internet lesivi del diritto d'autore. La versione finale della legge (*Loi n. 2009-1311*, del 28 ottobre 2009 - *Hadopi II*) è il risultato di un robusto intervento correttivo svolto dal *Conseil constitutionnel* (*Décision* n. 2009-580 DC, del 10 giugno 2009), che ha depotenziato alcuni principi cardine del primo provvedimento in materia approvato dal Parlamento nazionale (*Loi n. 2009-669*, del 19 giugno 2009 – *Hadopi*). Il Consiglio ha censurato i poteri sanzionatori inizialmente attribuiti all'*Hadopi* e ha negato che la tutela dei diritti di proprietà intellettuale possa giustificare improprie compressioni della libertà di espressione, che vede in Internet uno dei più efficaci strumenti di realizzazione. La sentenza identifica anzi una sorta di "diritto fondamentale" all'accesso ad Internet; contestualmente, essa suggerisce la necessità che qualsiasi sanzione sia proceduta dal vaglio di un'autorità giurisdizionale, introducendo un tema di dibattito la cui risonanza sembra poter oltrepassare i confini francesi. In particolare, il *Conseil constitutionnel* ha affermato che "lo sviluppo generalizzato dei servizi pubblici di comunicazione online e l'importanza di questi ultimi per la partecipazione alla democrazia e l'espressione di idee e opinioni, le libertà di comunicazione dei pensieri e di opinioni sancite dalla Dichiarazione dei Diritti dell'Uomo e del Cittadino del 1789 costituiscono libertà implicite per accedere a tali servizi".

Per ciò che riguarda specificamente il delicato tema del "**diritto all'oblio**", nell'ottobre 2010 è stata siglata, da alcuni importanti operatori di siti e motori di ricerca (tra i quali Microsoft), la prima **carta del diritto all'oblio**, elaborata e promossa dall'allora Segretario di Stato francese all'economia digitale Nathalie Kosciusko-Morizet (Governo Fillon II), che si configura come una sorta di codice di condotta il cui contenuto ha valenza prevalentemente programmatica, ma impegna i firmatari ad agire in modo da agevolare il conseguimento di particolari obiettivi, quali il miglioramento della trasparenza nello sfruttamento dei dati e una gestione facilitata dei dati da parte degli utenti. In tale ambito la carta individua una serie di azioni mirate al raggiungimento dei seguenti obiettivi: sensibilizzazione ed educazione degli internauti; protezione dei dati personali dall'indicizzazione automatica da parte dei motori di ricerca; gestione da parte

degli internauti dei dati pubblicati in rete; adozione di misure d'informazioni specifiche a beneficio dei minori; istituzione di un organismo competente a ricevere le richieste di cancellazione o modifica dei dati personali da parte degli utenti e la gestione del trasferimento di dati. Tuttavia, il rifiuto da parte di due colossi Google e Facebook di aderire alla carta riduce di molto l'efficacia di questo tentativo di autoregolamentazione. Alla base del diniego vi è infatti il timore che un controllo più pervasivo sul trattamento dei dati personali potrebbe comportare pesanti ricadute su altri diritti fondamentali, tra i quali *in primis* la libertà di espressione.

Germania

Nell'ordinamento tedesco il diritto relativo ad Internet (c.d. *Internetrecht* o *Onlinerecht*) non costituisce una branca giuridica a sé stante, ma investe diversi ambiti normativi: diritto civile e commerciale, diritto d'autore, disciplina della concorrenza, diritto penale, diritto internazionale privato, protezione dei dati personali, diritto delle telecomunicazioni. Con riferimento a quest'ultimo settore, Internet è stato inizialmente classificato come "servizio telematico" ai sensi della legge federale sui servizi telematici (*Teledienstegesetz - TDG* dell'11 luglio 1997) e come "servizio mediatico" ai sensi dell'Accordo di Stato tra Federazione e *Länder* sui servizi mediatici (*Mediendienste-Staatsvertrag – MDStV* del 31 gennaio 1997). Tale bipartizione, oggi superata dalla nuova disciplina del 2007 che ha abrogato entrambe le normative, si basava sulle diverse competenze legislative attribuite, rispettivamente, alla Federazione per quanto riguarda il settore delle telecomunicazioni e l'aspetto economico, e ai *Länder* per la regolamentazione della stampa e dei servizi radiotelevisivi. Nel 2007, con la riforma sistematica del diritto dei media e di Internet, i due concetti giuridici di servizio telematico e servizio mediatico sono stati fusi in quello di "**mezzo telematico**", oggetto della legge sui media telematici (*Telemediengesetz* del 26 febbraio 2007, da ultimo modificata dall'art. 1 della legge del 31 maggio 2010).

La responsabilità per i contenuti diffusi online è dell'emittente dalla quale tali contenuti sono stati inviati, a meno che essa non riesca a dimostrare che i contenuti di un'altra persona sono stati inoltrati con il suo stesso consenso. Nell'ottica di una rete che supera i confini nazionali devono essere osservate le leggi del paese in cui i dati vengono trasmessi ma, in alcuni casi, il diritto nazionale può essere applicato anche nel paese in cui la legge è stata infranta. Nella maggior parte dei casi, quindi, trova applicazione il diritto vigente nello Stato che trasmette determinati contenuti, sempre che lo Stato del ricevente tolleri l'invio di dati secondo un diritto straniero. Per citare un esempio giurisprudenziale emblematico, si può far riferimento ad una sentenza di principio della Corte di cassazione federale (c.d. *Holocaust-Urteil* del *Bundesgerichtshof*) del 12 dicembre 2000, secondo la quale un cittadino australiano può essere

ritenuto penalmente responsabile in Germania per un sito web negazionista dell'olocausto, ospitato su un server in Australia.

Sul versante della protezione dei dati personali e del diritto alla *privacy* assume particolare rilevanza la sentenza della Corte costituzionale federale del 2 marzo 2010, che ha dichiarato l'**incostituzionalità delle disposizioni attuative della direttiva europea 2006/24/CE** sulla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico. Nello specifico si tratta degli artt. 113a e 113b della *Telekommunikationsgesetz* e dell'art. 100g del codice di procedura penale (*Strafprozessordnung*). Secondo i giudici costituzionali le norme di recepimento della direttiva europea sono incompatibili con l'art. 10, comma 1 della Legge fondamentale (*Grundgesetz*) che sancisce l'inviolabilità del segreto della corrispondenza, postale e delle telecomunicazioni. Tali disposizioni violano quindi un diritto costituzionalmente garantito, consentendo l'archiviazione di dati sensibili in mancanza di parametri di sicurezza per i cittadini e non fornendo informazioni precise in merito alle modalità di utilizzo di tali dati. Pur non mettendo in discussione in linea di principio la validità della norma europea (che sarà poi dichiarata invalida dalla sentenza della Corte di giustizia europea dell'8 aprile 2014), la Corte costituzionale tedesca reputa l'applicabilità delle disposizioni di recepimento di particolare gravità per la segretezza delle telecomunicazioni, ritendo i dati archiviati sufficienti per una **profilazione invasiva degli utenti** riguardo alle loro opinioni politiche, ai loro gusti personali, ai loro comportamenti in fatto di consumi, e ad altro ancora. I giudici hanno inoltre sottolineato il rischio di abuso in quanto l'affidamento ad attori privati di dati di tale importanza non può essere consentito in presenza di deboli garanzie di sicurezza. Non da ultimo la raccolta e conservazione di tali dati senza un preciso motivo rischiano di provocare negli utenti una diffusa sensazione di essere costantemente osservati a scapito della garanzia e tutela dei propri diritti fondamentali.

Per quanto concerne, invece, il diritto di accesso alla rete, connesso al diritto all'informazione, si segnala una più recente pronuncia della Corte di cassazione federale del 24 gennaio 2013 (BGH, Urteil vom 24.01.2013 – III ZR 98/12), che ha riconosciuto il diritto al risarcimento ad un cittadino che, a causa di un adeguamento tariffario, era stato privato della connessione ad internet per due mesi. La Corte ha invece negato il risarcimento per l'impossibilità di utilizzare il fax ed il telefono fisso perché il ricorrente avrebbe potuto ovviare con altri mezzi (fax all'ufficio postale e utilizzo del telefono cellulare). Pur trattandosi di un risarcimento non elevato, va rilevato che la Corte ha ritenuto Internet una componente importante della vita moderna ponendolo sullo stesso piano del diritto alla mobilità (come nel caso dell'impossibilità di utilizzare la propria auto per un certo periodo a causa di un incidente imputabile a terzi). Secondo l'allora Ministro federale della giustizia (Sabine Leutheusser-Schnarrenberger, FDP) la

sentenza è una dimostrazione di quanto la rete sia fondamentale per il diritto all'informazione e configura l'utilizzo di Internet come un vero e proprio diritto del cittadino (*Bürgerrecht*).

Regno Unito

Nel Regno Unito la normativa rilevante per la tutela delle posizioni soggettive concernenti l'accesso ad Internet e la sua utilizzazione ha fonte in una molteplicità di testi legislativi.

La **tutela dei dati personali**, in primo luogo, è disciplinata dal *Data Protection Act 1998*. Adottata in attuazione delle norme comunitarie, la legge ha innovato un ambito disciplinare tradizionalmente caratterizzato dall'elaborazione giurisprudenziale degli istituti tipici della *privacy*. Peraltro, un tratto peculiare delle disposizioni del 1998 è da cogliere nella visione integrata degli aspetti di rilevanza giuridica concernenti la circolazione delle informazioni, che trova espressione nella attribuzione all'autorità indipendente di settore (*Information Commissioner's Office*) di competenze di controllo e di garanzia non limitate al campo della *data protection*, ma concernenti anche il diritto di accesso dei singoli alle informazioni di interesse pubblico (disciplinato dal *Freedom of Information Act 2000*).

Un profilo che ha assunto specifico rilievo, nell'esperienza britannica, si correla con la questione del bilanciamento tra le garanzie concernenti il trattamento di dati personali e le esigenze di tutela dell'ordine pubblico e della sicurezza dello Stato, perseguite attraverso attività di **sorveglianza elettronica** disposte dai poteri pubblici. In quest'ambito, le innovazioni legislative dirette ad adeguare il diritto interno agli aggiornamenti del *corpus* normativo comunitario in materia di *privacy* (con riferimento alle comunicazioni elettroniche e alla *data retention*) si sono intersecate, nel contesto nazionale, con i provvedimenti adottati nell'ambito della lotta al terrorismo.

Principale testo normativo di riferimento, assieme alle norme attuative e ai codici di condotta che ne integrano la disciplina, è a questo riguardo il *Regulation of Investigatory Powers Act 2000* (RIPA), con cui il legislatore ha inteso individuare un punto di equilibrio tra l'azione investigativa dei poteri pubblici – soggetta ad un regime di autorizzazioni - e il rispetto delle garanzie previste dalla CEDU. La necessaria applicazione del principio di proporzionalità, sulla cui sola base possono essere giustificate modalità di controllo certamente invasive della vita privata, discende, in particolare, dalla vigenza dello *Human Rights Act 1998*, con cui il Regno Unito ha incorporato nel proprio ordinamento la Convenzione europea dei diritti dell'uomo, introducendovi garanzie di rango sostanzialmente costituzionale che, nel quadro di più recenti ipotesi politico-istituzionali concernenti l'introduzione di una *written constitution* nel Regno Unito, sono state

considerate il nucleo di una eventuale codificazione dei diritti fondamentali nella forma di un moderno *Bill of Rights*.

Quali che siano i possibili esiti del più generale dibattito circa l'opportunità di una solenne enunciazione dei diritti fondamentali, è il caso di segnalare il rilievo particolare assunto, tra questi, dal diritto alla *privacy*, venuto al centro dell'attenzione sotto il profilo del contemperamento delle relative garanzie con diverse e perlopiù confliggenti finalità di interesse pubblico. Aspetti problematici, a questo riguardo, sono emersi con riguardo all'aggiornamento degli strumenti normativi in materia di intercettazione delle comunicazioni elettroniche (oggetto di un *Communications Data Bill* redatto nel 2012 e tornato al riesame dello *Home Office* dopo i rilievi formulati dagli organi parlamentari in punto di compatibilità con i diritti fondamentali); all'operatività del *National DNA Database*, e alle relative modalità di conservazione (dopo la sentenza di condanna pronunciata nel 2008 nei confronti del Regno Unito dalla Corte europea dei diritti dell'uomo nel caso *Marper*) dei dati genetici e biometrici di persone con precedenti penali; alle previsioni (abrogate nel 2010 dall'attuale Esecutivo pochi mesi dopo il suo insediamento) istitutive di una base centralizzata di dati anagrafici (*Identity Cards Act 2006*). In questo quadro, non è mancata la sollecitazione, espressa in forma di mozione in una delle più recenti sessioni parlamentari, riferita all'opportunità di disciplinare in modo esplicito, quale aspetto sostanziale di una "carta dei diritti di Internet" (*Internet Bill of Rights*), la garanzia della *privacy* dell'utente della Rete.

Un profilo non meno rilevante della disciplina cui soggiace l'utilizzazione di Internet, la **libertà di espressione**, non è inciso da previsioni specificamente riferite alla natura del mezzo utilizzato. A parte la prescrizione generale che vieta l'uso "inappropriato" delle reti di comunicazione elettronica (dettata dal *Communications Act 2003*, art. 127), deve infatti farsi capo, per le ipotesi di espressioni discriminatorie e di istigazione all'odio diffuse attraverso la Rete, alla legislazione ordinaria in materia di "*hate speech*". Essa è costituita, principalmente, dal *Public Order Act 1986*, modificato nel 2008 per integrarne le disposizioni con il riferimento alla **discriminazione sessuale e di genere**; e dal *Racial and Religious Hatred Act 2006*, di cui è oggetto la **discriminazione fondata sull'origine etnica e sul credo religioso**. Per quel che concerne le **disabilità**, il termine normativo di riferimento è costituito dall'*Equality Act 2010*, di cui può imputarsi la violazione a chi per mezzo della Rete diffonda contenuti discriminatori riferiti a tale condizione personale, inclusa tra quelle oggetto di tutela (oltre all'età, allo stato civile, all'orientamento sessuale, al mutamento di sesso).

Le disposizioni di questi testi legislativi sono corredate dall'indicazione di criteri che individuano, in relazione ai diversi ambiti della discriminazione, la sussistenza e la gravità del comportamento vietato. La rilevanza di questi criteri, manifestatasi nella loro applicazione in sede giurisdizionale e nell'attività delle *authorities* istituite con compiti di garanzia in taluni settori "sensibili" (come la

Equality and Human Rights Commission), si traduce, sul piano pratico, nella tipizzazione di comportamenti discriminatori e ispirati dall'odio compiuti per mezzo della Rete, per la cui rilevazione e segnalazione è operativo, dal 2011, un apposito servizio *on-line* gestito dalle autorità di polizia (*True Vision*).

Peraltro, un limite alla libertà di espressione, secondo alcune opinioni critiche, sarebbe derivato dal recente intervento rubricato sotto l'espressione "economia digitale", con cui il legislatore ha previsto (con il *Digital Economy Act 2010*) un maggiore coinvolgimento dei *providers* nell'azione di contrasto dei fenomeni di violazione dei diritti di privativa sui contenuti digitali, e delineato strumenti inibitori che possono consistere nel blocco dei siti Internet di cui sia riconosciuta la responsabilità in atti di pirateria concernenti il **diritto d'autore**. Sul piano operativo, le modalità di blocco dei siti Internet, e le relative opzioni tecniche, sono state prese in esame da parte dell'autorità di garanzia delle comunicazioni – OFCOM – in un documento del 2010 espressamente dedicato al "*site blocking*".

Un tema ulteriore, di notevole risonanza presso l'opinione pubblica e posto recentemente anche all'attenzione parlamentare, riguarda la **tutela dei minori *on-line***. Sulla base dei risultati di un'inchiesta indipendente promossa nel 2012 dalla Camera dei Comuni e affidata ad esperti esterni, è stata prospettata, e sottoposta ad una consultazione pubblica, l'opportunità di adottare misure normative per ottenere dai *providers* una preliminare configurazione delle modalità di connessione alla Rete idonea a filtrare e a bloccare preventivamente i contenuti potenzialmente lesivi. Tale soluzione di filtraggio "alla fonte", tuttavia, è stata ritenuta di dubbia efficacia e proporzionalità dal Governo, che nella sua replica alla relazione conclusiva dell'inchiesta ha evidenziato (anche sulla base dei risultati della consultazione pubblica) il ruolo imprescindibile di un'attiva vigilanza dei genitori (attraverso le opzioni tecniche di "*parental control*") sull'uso "sicuro" di Internet da parte dei propri figli.

Il tema dell'adozione di metodiche *opt-in* oppure *opt-out* per la connessione alla Rete e la selezione dei contenuti per suo tramite diffusi è emerso, più di recente, in sede politica e con riferimento particolare alla tutela dei minori rispetto alla diffusione di **contenuti pornografici**. Il Primo Ministro ha annunciato, in un discorso pronunciato nel 2013, l'intento di voler prevedere l'obbligo per i *providers* di predisporre una connessione filtrata ("*family-friendly filters*") per tutti i nuovi utenti salvo loro diversa opzione, e di contattare gli utenti già abbonati per informarli della possibilità di optare per tale modalità "sicura" di configurazione di accesso alla rete ove non preferiscano diversamente. Riguardo alla legislazione vigente, il Primo Ministro ha annunciato modifiche (attraverso il *Criminal Justice and Court Bill* attualmente all'esame del Parlamento) delle norme in materia di pornografia estrema, al fine di reprimerne con maggiore severità la diffusione anche attraverso Internet.

Spagna

La Costituzione spagnola (1978) non contiene riferimenti diretti a Internet. Tuttavia l'art. 18 garantisce il segreto delle comunicazioni e in specie di quelle postali, telegrafiche e telefoniche, salva decisione giudiziale (comma 3), prevedendo inoltre che la legge ponga limiti all'uso dell'informatica per salvaguardare l'onore e l'intimità personale e familiare dei cittadini, nonché il pieno esercizio dei loro diritti (comma 4).

La principale norma in materia di protezione dei dati personali è costituita dalla *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, che ha dato attuazione alla direttiva comunitaria 95/46 del 24 ottobre 1995, "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati". L'aspetto peculiare della legge è costituito dall'enunciazione delle regole che devono presiedere alle operazioni di trattamento di dati personali. In estrema sintesi, si stabilisce che i dati debbano essere trattati in modo leale e legittimo, e in conformità alle condizioni specifiche previste per i dati sensibili (*datos especialmente protegidos*, art. 7); si affermano i princìpi di finalità e di pertinenza, dovendo i dati essere raccolti per uno scopo conforme alla legge, e sottoposti a trattamento solo a questo fine e non per ulteriori utilizzazioni. Essi devono essere conservati per il tempo strettamente necessario al loro trattamento, devono essere accurati e aggiornati, devono essere protetti da misure tecniche di sicurezza, idonee ad impedire la loro perdita, alterazione o distruzione accidentale nonché la loro accessibilità da parte di terzi non autorizzati. Ai soggetti interessati è riconosciuto: il diritto di accesso ai propri dati detenuti da terzi, nonché quello, in casi prestabiliti, di opporsi al relativo trattamento (artt. 6, 14); il diritto di impugnare atti dell'amministrazione o di soggetti privati assunti sulla base di valutazioni sorrette unicamente dal trattamento di dati personali (art. 13); il diritto di accesso al Registro generale di protezione dei dati, in cui sono riportate le finalità dei trattamenti di dati e l'identità dei soggetti responsabili (art. 14); il diritto di ottenere la **rettifica o la cancellazione di dati personali incompleti, inesatti o non pertinenti** (art. 16); il diritto al risarcimento del danno (art. 19). Il legislatore spagnolo ha infine previsto, conformemente alle disposizioni comunitarie, alcune deroghe alla disciplina generale, nel quadro delle garanzie riconosciute ai soggetti interessati: tali deroghe operano con riguardo al trattamento di dati personali compiuti dalle pubbliche autorità a fini di sicurezza nazionale o di assistenza sociale, e da soggetti privati nell'ambito dell'attività giornalistica, della ricerca storica, scientifica e statistica.

Nel 2002 è stata approvata la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, con la quale il legislatore ha accolto un concetto ampio di "servizi della società dell'informazione", comprendente, al di là dell'ambito della contrattazione di beni e servizi per via elettronica, la fornitura di informazioni, l'invio di comunicazioni commerciali, le

attività di intermediazione per l'accesso a Internet, la trasmissione di dati attraverso le reti di telecomunicazioni e l'offerta di strumenti di ricerca, accesso e ricompilazione di dati, purché svolte con finalità economiche. Il principio della libera prestazione dei servizi della società dell'informazione trova il suo limite nel rispetto di alcuni valori fondamentali: la salvaguardia dell'ordine pubblico, delle indagini giudiziarie e della difesa nazionale; la protezione della salute pubblica o delle persone fisiche dei consumatori, degli utenti e degli investitori; il rispetto della dignità della persona e il divieto di discriminazioni in base alla razza, al sesso, alla religione, alle opinioni, alla nazionalità, all'incapacità o a qualsiasi altra circostanza personale o sociale; la protezione della gioventù e dell'infanzia. Le amministrazioni pubbliche devono favorire l'elaborazione e l'applicazione di codici di condotta volontari, redatti con la partecipazione delle associazioni dei consumatori e degli utenti e volti alla protezione dei destinatari dei servizi, in particolare dei minori. Per quanto concerne l'informazione e il controllo, sia i destinatari sia i fornitori dei servizi possono, indirizzandosi ai Ministeri competenti e agli organi corrispondenti presso le Comunità autonome, ottenere informazioni relative ai propri diritti, alle obbligazioni contrattuali, ai procedimenti di risoluzione dei conflitti, nonché indicazioni concernenti le autorità, le associazioni e le organizzazioni che possono fornire informazioni ulteriori o assistenza pratica.

Nel 2009 è stato adottato il *Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas*. La **Carta dei diritti dell'utente dei servizi di comunicazione elettronica** ha raccolto le disposizioni relative ad alcuni diritti già riconosciuti, aggiungendone degli altri. In particolare l'art. 3 del decreto riconosce, tra gli altri, il diritto a ottenere una connessione alla rete telefonica pubblica da un'ubicazione fissa, che faciliti l'accesso funzionale a Internet e di accedere alla prestazione del servizio telefonico, così come al resto delle prestazioni comprese nel servizio universale, il diritto a ricevere servizi di comunicazioni elettroniche con garanzia di qualità ed un'informazione comparabile, pertinente e aggiornata sulla qualità dei servizi di comunicazioni elettroniche disponibili, e infine il diritto alla protezione dei dati di carattere personale[8]. L'art. 5 prevede che, in relazione al servizio di banda larga per l'accesso a Internet, l'operatore non può applicare all'utente finale un'offerta la cui velocità pubblicizzata sia superiore alla velocità massima permessa dalla tecnologia utilizzata. L'art. 16 prevede inoltre il diritto a un indennizzo per l'interruzione temporanea del servizio di accesso a Internet.

La *Ley 2/2011, de 4 de marzo, de Economía Sostenible*, all'interno della Strategia di recupero dell'economia spagnola, ha previsto un ampio programma di riforme volte a una nuova crescita equilibrata e duratura, che sia sostenibile dal punto di vista economico, ambientale e sociale. In particolare l'art. 52 ha

[8] Sul sito del Governo spagnolo è disponibile una scheda sul contenuto della Carta dei diritti dell'utente delle telecomunicazioni.

previsto l'inclusione, come parte integrante del servizio universale di telecomunicazioni, di una **connessione che consenta comunicazioni di dati di banda larga a una velocità di downstream di 1 Mbit al secondo**, mediante qualsiasi tecnologia. La Commissione delegata del Governo per gli affari economici può fissare un costo massimo per le connessioni che permettono comunicazioni in banda larga incluse nel servizio universale. La quarantatreesima disposizione finale disciplina inoltre l'attività di download da Internet, prevedendo la possibilità, da parte della Commissione sulla proprietà intellettuale, di privazione dell'accesso a Internet per i soggetti che violano i contenuti protetti dalle norme sul diritto d'autore.

Infine, nel 2014 è stata approvata la nuova legge sulle comunicazioni: la *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*. L'art. 3 della legge pone tra gli obiettivi della legge la difesa degli interessi degli utenti, assicurando il loro diritto di accesso ai servizi di comunicazioni elettroniche in condizioni adeguate di prezzo e qualità, promuovendo la capacità degli utenti finali ad accedere e distribuire l'informazione o utilizzare le applicazioni e i servizi, in particolare attraverso un accesso a Internet. Tutti gli utenti finali del servizio universale possono ottenere una connessione alla rete pubblica di comunicazioni elettroniche da un'ubicazione fissa, che consenta di realizzare comunicazioni tramite voce, fax e dati, a velocità sufficiente per accedere in maniera funzionale ad Internet. Tale connessione deve permettere comunicazioni di dati in banda larga a una velocità di downstream di 1 Mbit al secondo (art. 25). La Strategia nazionale di reti ultrarapide deve adottare le misure per raggiungere gli obiettivi stabiliti dall'Agenda digitale per l'Europa e incorporati nell'Agenda digitale per la Spagna e, in particolare, per assicurare l'universalizzazione di una connessione che permetta comunicazioni di dati di banda larga che si estenda progressivamente, in modo da raggiungere nel 2017 una velocità minima di Internet di 10 Mbit al secondo e, entro il 2020, di consentire a tutti gli utenti una velocità minima di Internet di 30 Mbit al secondo, e ad almeno il 50% delle famiglie l'accesso a servizi di velocità superiore a 100 Mbit al secondo (diciottesima disposizione aggiuntiva).

Altri paesi europei

La **Grecia** è tra i Paesi i cui ordinamenti contemplano previsioni di rango costituzionale, rilevanti per la ricostruzione di una sfera di diritti fondamentali espressamente riconducibili all'accesso e all'utilizzazione di Internet. La costituzione ellenica, a seguito della revisione costituzionale del 2001, prevede all'art. 5A), comma 2, che «ciascuno ha il diritto di partecipare alla Società dell'Informazione. La facilitazione dell'accesso alle informazioni trattate in forma elettronica, come anche la produzione, lo scambio e la diffusione di esse, è

materia di obblighi per lo Stato, in conformità alle garanzie di cui agli articoli 9, 9A e 19» (traduzione non ufficiale).

All'esplicita previsione costituzionale di un diritto di accesso alla rete, fonte del corrispondente obbligo a carico dei pubblici poteri di garantirne l'effettiva realizzazione, non risulta però che abbiano fatto seguito provvedimenti attuativi da parte del legislatore ordinario, la cui adozione non costituisce, presumibilmente, una priorità attuale, considerata la dura crisi economica che ha colpito il Paese.

Sempre in ambito europeo, una delle esperienze più significative è quella dell'**Estonia**, il cui *Telecommunications Act* del febbraio 2000 ha inserito l'accesso alla rete nel novero degli obblighi di servizio universale, prefiggendosi, all'art. 5, di rendere Internet *"(…) universally available to all subscribers regardless of their geographical location, at a uniform price".* In più, la Legge specifica l'intenzione di abbattere ogni discriminazione nei confronti degli utenti residenti in zone geograficamente disagiate del Pese, e ciò sia dal punto di vista del diniego dell'accesso alla rete, sia sotto il profilo dell'adeguamento tariffario nei confronti di tali soggetti. Inoltre, in ragione di una forte promozione delle nuove tecnologie al servizio della partecipazione democratica, l'Estonia ha introdotto, sin dalle elezioni amministrative del 2005, un sistema di votazione elettronica da sfruttare, su massima scala, anche per le elezioni politiche. Il voto elettronico è così divenuto una realtà consolidata, ripetutasi da ultimo in occasione delle elezioni politiche del 2011, quando il 24,3% delle preferenze è stato espresso con questa modalità.

Il meccanismo è stato sottoposto a critiche, successivamente diradate da una pronunzia della *Riigikohus*, la Corte suprema estone, che ha ricondotto l'introduzione dell'*e-vote* al tentativo di favorire la massima partecipazione possibile dei cittadini nei procedimenti elettorali.

La rilevanza di Internet è dunque saldata al principio partecipativo, tanto da porre la salvaguardia della partecipazione informatica su un piano sovraordinato rispetto ai dubbi espressi in relazione alla garanzia del rispetto di numerose caratteristiche del voto, tra cui segretezza, personalità e libertà.

Infine, anche la **Finlandia** ha intrapreso un percorso normativo iniziato con l'approvazione del *Communications Market Act (393/2003)*, e culminato sei anni dopo con l'introduzione della banda larga tra gli obblighi di servizio universale.

La Sezione 60c) della legge finnica contiene la regolamentazione degli obblighi di servizio universale delle telecomunicazioni. La FI.CO.R.A. (*Finnish Communications Regulatory Authority*) individua un *provider* cui viene attribuito il ruolo di gestore del servizio universale delle telecomunicazioni, che ha il dovere di erogare il servizio alla totalità degli utenti ad un prezzo ragionevole ed indipendentemente dalla collocazione geografica. Tra gli obblighi di servizio universale, la legge individua anche una "*appropriata connessione Internet per tutti gli utenti"*. Il legislatore si cura altresì di stabilire dei parametri di riferimento

per valutare quando un servizio abbia un prezzo “ragionevole” e quando una connessione possa ritenersi “appropriata”. Dal primo punto di vista dovranno essere valutati i prezzi medi, nonché il coefficiente di difficoltà ed i costi da sostenere per la realizzazione dell’infrastruttura. Dal secondo punto di vista, la legge attribuisce al Ministero dei Trasporti e delle Comunicazioni il compito di fissare, con decreto, la funzionalità minima di una connessione alla Rete affinché la stessa possa considerarsi “appropriata”. Ad oggi il governo finnico, con l’emanazione del Decreto 732/2009 sulle tariffe minime di un accesso funzionale ad Internet come servizio universale (traduzione inglese), ha fissato tale misura in almeno 1 Mbit per secondo in downstream.

Focus: Le esperienze di alcuni Paesi dell'America latina

In alcune Costituzioni dei Paesi dell'America latina è possibile rinvenire precisi riferimenti relativi a Internet e alle reti informatiche.

In **Venezuela** la Costituzione (1999-2000), all'art. 28, sancisce il diritto di ogni persona ad accedere all'informazione e ai dati contenuti in registri ufficiali o privati sulla persona medesima o sui suoi beni, con le eccezioni stabilite dalla legge, così come di conoscere l'uso che viene fatto dei dati e di richiedere al tribunale competente l'aggiornamento, la rettifica o la distruzione degli stessi, nel caso siano erronei o ledano illegittimamente i propri diritti. Allo stesso modo si può accedere a documenti di qualsiasi natura che contengano informazioni la cui conoscenza sia di interesse per comunità o gruppi di persone, fatto salvo il segreto delle fonti di informazione giornalistica o di altre professioni determinate dalla legge. L'art. 108 prevede che i mezzi di comunicazione, pubblici e privati, debbano contribuire alla formazione dei cittadini. Lo Stato deve altresì garantire servizi pubblici di radio, televisione e reti di biblioteca e informatiche, al fine di permettere l'accesso universale all'informazione. I centri di istruzione devono incorporare la conoscenza e l'applicazione delle nuove tecnologie e delle sue innovazioni, secondo requisiti stabiliti dalla legge.

In **Honduras** la Costituzione (1982), all'art. 182 (riformato nel 2006), riconosce, accanto all'*hábeas corpus*, un *hábeas data*. Quest'ultimo può essere promosso dalla persona i cui dati personali o familiari figurano in archivi, registri pubblici o privati, al fine di ottenere accesso all'informazione, impedire la sua trasmissione o divulgazione, rettificare dati inesatti o erronei, aggiornare l'informazione, esigere confidenzialità e l'eliminazione di false informazioni, rispetto a qualsiasi archivio o registro, pubblico o privato, contenuto in mezzi convenzionali, elettronici o informatici, che producano danno all'onore, all'intimità personale, familiare e alla propria immagine. Tale garanzia non riguarda il segreto delle fonti di informazione giornalistica.

In **Brasile** la Costituzione (1988), all'art. 5 (2014), prevede che

"Tutti sono uguali davanti alla legge, senza distinzione alcuna; è garantita, tanto ai brasiliani quanto agli stranieri residenti nel Paese, l'inviolabilità del diritto alla vita, alla libertà, all'uguaglianza, alla sicurezza e alla proprietà, nei seguenti termini:

(…)

LXXII. L'*habeas data* verrà concesso:

a) per assicurare la conoscenza di informazioni relative alla persona del richiedente, come risultano nei registri o nelle banche dati di enti governativi o di

carattere pubblico;
b) per la rettifica di dati, qualora non si preferisca farlo con processo segreto, giudiziale o amministrativo"[9].
(…)"
Il Brasile ha quindi introdotto nel 2014 una disciplina organica relativa ai principi, alle garanzie, ai diritti e ai doveri per l'uso di Internet (*Lei n. 12.965*, del 23 aprile 2014, cosiddetto "*Marco Civil da Internet*"). Essa si fonda sul rispetto della libertà di espressione, come pure sul riconoscimento della dimensione globale della rete; sui diritti umani, lo sviluppo della personalità e l'esercizio della cittadinanza nell'ambito dei media digitali; sul pluralismo e la diversità; sull'apertura e la collaborazione; sulla libera iniziativa, la libera concorrenza e la tutela dei consumatori; sulla finalità sociale della rete (art. 2). La disciplina dell'uso di Internet deve attenersi ai seguenti principi: garanzia della libertà di espressione, comunicazione e manifestazione del pensiero, ai sensi della Costituzione; tutela della vita privata; protezione dei dati personali, secondo quanto previsto dalla legge; mantenimento e garanzia della neutralità della rete; mantenimento della stabilità, sicurezza e funzionalità della rete, mediante misure tecniche compatibili con gli standard internazionali e incoraggiando l'uso delle migliori pratiche; responsabilizzazione degli agenti in base alle loro attività, conformemente alla legge; mantenimento della natura partecipativa della rete; libertà quanto ai modelli di attività economica perseguiti su Internet, purché non in contrasto con gli altri principi stabiliti dalla legge (art. 3). La nuova normativa si prefigge, infine, i seguenti obiettivi: promuovere il diritto di tutti all'accesso a Internet; favorire l'accesso all'informazione, la conoscenza e la partecipazione alla vita culturale e alla gestione della cosa pubblica; promuovere l'innovazione e stimolare l'ampia diffusione delle nuove tecnologie e dei nuovi modelli di utilizzo e di accesso; promuovere l'adesione a standard tecnologici aperti che consentano la comunicazione, l'accessibilità e l'interoperabilità tra applicazioni e basi di dati (art. 4).
In **Ecuador** la Costituzione (2008), all'art. 16, sancisce che tutte le persone, in forma individuale o collettiva, hanno diritto a: una comunicazione libera, interculturale, includente, diversa e partecipativa, in tutti gli ambiti dell'interazione sociale, in qualsiasi mezzo e forma, nella loro propria lingua e con i propri simboli; all'accesso universale alle tecnologie di informazione e comunicazione; alla creazione di mezzi di comunicazione sociale e all'accesso in eguaglianza di condizioni all'uso delle frequenze dello spettro radioelettrico per la gestione di stazioni di radio e televisione pubbliche, private e comunitarie, e a bande libere per lo sfruttamento di reti senza fili; all'accesso e all'uso di tutte le forme di comunicazione visiva, uditiva, sensoriale e ad altre che permettano

[9] Una traduzione in italiano della Costituzione brasiliana, aggiornata al 2003, è disponibile sul sito del Consiglio regionale del Veneto.

l'inclusione delle persone con disabilità; ad integrare gli spazi di partecipazione previsti nella Costituzione nel campo della comunicazione.
In ultimo va segnalata un'importante sentenza della *Sala Constitucional* (Corte Costituzionale) della **Costa Rica**, che, con la pronuncia n. 12790 del 30 luglio del 2010, ha affermato che "il ritardo del governo ad aprire il mercato delle comunicazioni alla concorrenza equivale ad una violazione delle libertà fondamentali, arrecando un grave pregiudizio alla libertà di scelta dei consumatori e all'eliminazione del *digital divide*". Secondo le argomentazioni della Corte, "l'evoluzione negli ultimi venti anni in materia di tecnologia dell'informazione e della comunicazione […] ha rivoluzionato l'ambiente sociale dell'essere umano […], con la conseguenza che può affermarsi che questa tecnologia ha avuto un impatto significativo sul modo nel quale l'essere umano comunica, facilitando la relazione tra persone ed istituzioni a livello mondiale e eliminando la barriera di spazio e tempo. Ne discende che l'accesso a queste tecnologie si converte in uno strumento primario per agevolare l'esercizio dei diritti fondamentali, come, tra gli altri, la partecipazione democratica (democrazia elettronica) e il controllo dei cittadini, la formazione, la libertà di espressione e di pensiero, l'accesso all'informazione ed ai servizi pubblici online, il diritto a rapportarsi con i pubblici poteri attraverso strumenti elettronici e la trasparenza amministrativa". In questo modo, la *Sala Constitucional* ha riconosciuto il ruolo di Internet come strumento fondamentale della comunicazione interpersonale, agevolando il rapporto tra i cittadini privati e i pubblici poteri, mediante il superamento di barriere tecniche che gli strumenti tradizionali non erano in grado di eliminare.