Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche

Commissione di studio per la redazione di principi e linee guida in tema di garanzie, diritti e doveri per l'uso di Internet

Elementi di documentazione

n. 132

25 luglio 2014

Camera dei deputati

XVII LEGISLATURA

Documentazione e ricerche

Commissione di studio per la redazione di principi e linee guida in tema di garanzie, diritti e doveri per l'uso di Internet

Elementi di documentazione

n. 132

25 luglio 2014

Servizio responsabile:

SERVIZIO STUDI – Dipartimento Giustizia

☎ 066760-9559 / 066760-9148 – ✉ *st_giustizia@camera.it*

Hanno partecipato alla redazione del *dossier* i seguenti Servizi e Uffici:

SERVIZIO BIBLIOTECA – Osservatorio della legislazione straniera

☎ 066760-2278 – ✉ *bib_segreteria@camera.it*

SEGRETERIA GENERALE – Ufficio Rapporti con l'Unione europea

☎ 066760-2145 – ✉ *cdrue@camera.it*

***File**: GI0250.doc*

I N D I C E

SCHEDE DI LETTURA

Schede di lettura

LA PROTEZIONE DEI DATI PERSONALI

1. La politica dell'Unione europea

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** del Trattato sul funzionamento dell'Unione europea stabilisce che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.**

La sfera della **riservatezza** delle **informazioni personali** e della **vita privata** dell'individuo trovano particolare tutela negli **articoli 7 e 8** della Carta dei diritti fondamentali la quale ha lo **stesso valore** giuridico dei **Trattati.**

La **riservatezza personale** trova protezione anche nella **Convenzione europea dei diritti dell'uomo (CEDU),** stipulata dagli Stati membri del Consiglio d'Europa, 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 stabilisce altresì 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 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.**

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**.

2. Il pacchetto di riforma

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.

Rispetto alla **direttiva 95/46/CE**, la proposta di **regolamento generale sulla protezione dei dati** ne riorganizza il contenuto, ampliandolo notevolmente. 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.

Consenso esplicito al trattamento

Secondo la riforma, 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 (diritto all'oblio)

Potenziando uno strumento già parzialmente previsto dalla direttiva del 1995, la riforma prevede che **l'interessato avrà diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano o di impedire l'ulteriore diffusione degli stessi.** Va peraltro osservato che dalla previsione di tale diritto non discende l'obbligo generalizzato, per il soggetto che detiene tali dati, di cancellarli. La cancellazione e il divieto di diffusione dei dati possono, infatti, essere richiesti **in presenza di motivi specificatamente individuati** (i dati non sono più necessari rispetto alle finalità per le quali erano stati raccolti; è stato revocato da parte dell'interessato il consenso; è scaduto il periodo di conservazione; la cancellazione o divieto di diffusione discende da una pronuncia di un tribunale o da un'autorità competente; i dati sono stati trattati illecitamente).

Il responsabile del trattamento è tenuto ad **informare i terzi** che stanno trattando tali dati **della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali**. Se ha autorizzato un terzo a

pubblicare dati personali, il responsabile del trattamento è **ritenuto responsabile di tale pubblicazione**.

Sono tuttavia previste **eccezioni** all'obbligo di cancellazione: in particolare, si richiamano motivi di **interesse pubblico, nel settore della sanità pubblica,** per finalità**, statistiche e di ricerca scientifica**.

Diritto alla portabilità dei dati

Al fine di un miglioramento della concorrenza tra i servizi, è previsto il diritto di **trasferire i propri dati da un sistema di trattamento elettronico a un altro**, senza che il responsabile del trattamento possa impedirlo (ad esempio 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).

Divieto di profiling

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. Sono previste deroghe a tale regime, in sintesi, in caso di **conclusione o dell'esecuzione di un contratto**, oppure se consentito da diritto dell'Unione o di uno Stato membro che precisi altresì misure adeguate a salvaguardia dei legittimi interessi dell'interessato, o sulla base del **consenso dell'interessato**.

Il responsabile della protezione dei dati personali

È introdotta 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.

Secondo il Parlamento europeo 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

È riscritta 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** (cosiddetto **sportello unico**).

Il trasferimento dei dati all'estero

Il trasferimento è subordinato alla preventiva adozione, da parte della **Commissione**, di una **decisione** di **adeguatezza** del livello di **protezione** accordato dallo **Stato terzo destinatario** delle informazioni; sono altresì previste fattispecie in deroga alla necessità di tale decisione.

Secondo l'accordo raggiunto dal Consiglio dell'Unione europea Giustizia e affari interni del 6 giugno 2014, oltre ai casi di trasferimenti sulla base di un **accertamento di adeguatezza** rilasciato dalla Commissione o di **garanzie adeguate**, e ai trasferimenti basati su deroghe specificamente indicate nella proposta, sarebbe consentito alle autorità pubbliche nazionali di porre **limiti al flusso di dati personali al di fuori dell'Unione europea** sulla base del diritto dell'Unione o degli Stati membri, in caso di **necessità eccezionale** dettata da **ragioni di interesse pubblico rilevante**.

Lo stato del negoziato

Il pacchetto protezione dati personali è stato approvato in prima lettura da parte della Assemblea plenaria del **Parlamento europeo** nella sessione dell'11-14 marzo 2014.

Rispetto alle proposte originarie, il **Parlamento europeo** ha modificato alcune norme prevedendo che:

a) motori di ricerca social network o fornitori di cloud debbano 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 **non membro;**
b) le società che infrangono le regole incorrano in multe **fino a 100 milioni di euro o fino al 5%** del **fatturato mondiale annuo**.

Quanto all'attività del **Consiglio**, gli Stati membri **non hanno ancora raggiunto un orientamento comune complessivo**.

Tra le questioni più controverse dibattute al Consiglio si segnala il tema dello sportello unico (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), i relativi poteri e il rapporto con le autorità nazionali. Secondo

fonti non ufficiali, durante la riunione informale dei Ministri della giustizia dei Paesi dell'UE del'8 luglio 2014, si sarebbe raggiunto una soluzione di compromesso mediante la previsione di una clausola di flessibilità a favore dei Governi nazionali che desiderano stabilire norme di protezione più elevate.

3. 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.**

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.

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 sè **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

[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.

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 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) **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.**

4. I più recenti sviluppi in Italia

La tutela della privacy

Il più recente intervento del legislatore in materia **di tutela della privacy** costituisce attuazione della delega contenuta nella Legge Comunitaria 2010. Il decreto legislativo n. 69 del 2012, ha infatti modificato il cd. Codice della privacy (D.Lgs. n. 196/2003) in attuazione di normativa comunitaria (*direttiva 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche; direttiva 2009/140/CE in materia di reti e servizi di comunicazione elettronica; regolamento (CE) n. 2006/2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori).*

Tra gli interventi di maggior rilievo introdotti nel citato Codice, si segnalano:

- le modifiche all'art. 4, nel quale viene introdotta la definizione di ***"Violazione dei dati".*** Questa è indicata come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico";
- le modifiche all'art. 32, ora rubricato ***"Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico".*** La disposizione estende ad "altri soggetti", cui il fornitore affida l'erogazione del servizio di comunicazione elettronica, l'obbligo di adottare "misure tecniche e organizzative adeguate al rischio esistente". I soggetti che operano sulle reti di comunicazione elettronica sono tenuti a garantire che i dati siano accessibili soltanto al personale autorizzato nonché la protezione dei dati relativi al traffico, oltre a preservare dalla distruzione, perdita e alterazione quelli trasmessi o archiviati, nell'ottica di una accurata politica di sicurezza;
- l'introduzione dell'art. 32-bis, sugli ***"Adempimenti conseguenti ad una violazione di dati personali"*** e la previsione di un rilevante e nuovo adempimento in capo al fornitore di servizi di comunicazione elettronica accessibili al pubblico. Questi ha oggi l'obbligo di comunicare al Garante l'avvenuta violazione di dati personali, estendendo l'informazione ai contraenti che rimangano pregiudicati nel proprio diritto alla riservatezza. La comunicazione al Garante deve descrivere, altresì, le conseguenze della violazione di dati personali e le misure che il fornitore intende adottare allo scopo di porvi rimedio;
- le modifiche all'art. 122, volte a porre ***un argine all'uso indiscriminato di tecniche pubblicitarie che sfruttano i cookies***. Sino ad oggi era, infatti, radicato nella prassi della Rete un sistema basato sull'opt out, che consentiva ai provider un libero utilizzo dei cookies, fino al momento del dissenso manifesto dell'utente. Dando attuazione alla direttiva 2009/136/CE, il decreto legislativo dispone che l'archiviazione delle informazioni nell'apparecchio terminale di un utente o l'accesso a informazioni già archiviate, sia consentito se l'interessato ha espresso il suo consenso sulla base di un'informativa semplificata, anche tramite specifiche configurazioni di programmi informatici o di dispositivi di facile e chiara utilizzabilità.

Più recentemente, il **DL 93 del 2013** ha modificato (**art. 9)** le norme sul **reato di frode informatica** (art. 640-ter c.p.) prevedendo un incremento di pena

quando il reato sia commesso con ***furto o indebito utilizzo dell'identità digitale*** (comma 1).

Nello specifico, si tratta di circostanza aggravante speciale (perché riguardante il solo delitto di frode informatica) a effetto speciale (perché implica un aumento della pena superiore a un terzo).

Il legislatore, oltre a non prevedere un reato specifico relativo al furto d'identità digitale, in relazione all'aggravante introdotta non ha dato un'esatta definizione al concetto di "identità digitale" né ha chiarito come debba avvenire il furto o l'indebito utilizzo.

L'**art. 10** dello stesso decreto-legge 93/2013 "***liberalizza" l'offerta di accesso alla rete Internet tramite tecnologia WiFi*** sotto tre aspetti:

- non è richiesta l'identificazione personale degli utilizzatori;
- quando l'offerta di accesso ad internet non costituisce l'attività commerciale prevalente del gestore (quali bar, alberghi, altri esercizi commerciali aperti al pubblico, università, etc.), non sono richieste né la licenza del questore, né l'autorizzazione ministeriale;
- si facilita l'installazione delle relative apparecchiature (abrogazione del cd. patentino installatori, cioè dell'obbligo di affidare i lavori di allacciamento dei terminali a imprese abilitate).

Il testo approvato definitivamente è il frutto di interventi modificativi che si sono succeduti nel corso dei lavori parlamentari. L'originaria versione dell'art. 10 presentava invece forti criticità che il Garante della privacy ha segnalato al Parlamento e al Governo. La disposizione originaria obbligava infatti i gestori a "garantire la tracciabilità del collegamento (MAC address)" e stabiliva che la "registrazione della traccia delle sessioni", ove non associata all'identità dell'utilizzatore, non costituiva trattamento di dati personali e non richiedeva adempimenti.

Il diritto alla cancellazione e il 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 della 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.

Il divieto di profiling

Il Garante della privacy - con il ***Provvedimento generale*** (adottato al termine di una consultazione pubblica) pubblicato sulla *Gazzetta ufficiale del 3 giugno 2014* - ha previsto che l'installazione di *cookie*s 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 *cookies* 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

Da ultimo, con il provvedimento del 10 luglio 2014, il Garante ha prescritto a Google Inc. di assicurare maggiore trasparenza nel trattamento dei dati e garanzie per chi utilizza i suoi servizi.

In particolare, il Garante privacy ha stabilito che Google non potrà utilizzare i dati degli utenti a fini di profilazione se non ne avrà prima ottenuto il consenso e dovrà dichiarare esplicitamente di svolgere questa attività a fini commerciali.

L'Autorità ha prescritto a Google l'adozione di un sistema di informativa strutturato su più livelli, in modo da fornire in un primo livello generale le informazioni più rilevanti per l'utenza: l'indicazione dei trattamenti e dei dati oggetto di trattamento (es. localizzazione terminali, indirizzi IP etc.), dell'indirizzo presso il quale rivolgersi in lingua italiana per esercitare i propri diritti etc.; in un secondo livello, più di dettaglio, le specifiche informative relative ai singoli servizi offerti. Ma soprattutto Google dovrà spiegare chiaramente, nell'informativa generale, che i dati personali degli utenti sono monitorati e utilizzati, tra l'altro, a fini di profilazione per pubblicità mirata e che essi vengono raccolti anche con tecniche più sofisticate che non i semplici cookie, come ad esempio il fingerprinting. Quest'ultimo è un sistema che raccoglie informazioni sulle modalità di utilizzo del terminale da parte dell'utente e, a differenza dei cookie che vengono istallati sul pc o nello smartphone, le archivia direttamente presso i server della società.

Per utilizzare a fini di profilazione e pubblicità comportamentale personalizzata i dati degli interessati - sia quelli relativi alle mail sia quelli raccolti incrociando le informazioni tra servizi diversi o utilizzando cookie e fingerprinting - Google dovrà acquisire il previo consenso degli utenti e non potrà più limitarsi a considerare il semplice utilizzo del servizio come accettazione incondizionata di regole che non lasciavano, fino ad oggi, alcun potere decisionale agli interessati sul trattamento dei propri dati personali. In proposito, l'Autorità ha anche indicato una modalità innovativa e di facile impiego che, senza gravare eccessivamente sulla navigazione dell'utente, gli consenta di scegliere in modo attivo e consapevole se fornire o meno il proprio consenso alla profilazione, anche con riguardo ai singoli servizi utilizzati.

Google dovrà definire **tempi certi di conservazione dei dati** sulla base delle norme del Codice privacy, sia per quanto riguarda quelli mantenuti sui sistemi cosiddetti "attivi", sia successivamente archiviati su sistemi di "back up". Per quanto riguarda la cancellazione di dati personali, il Garante ha imposto a Google che richieste provenienti dagli utenti che dispongono di un account (e sono quindi facilmente identificabili) siano soddisfatte al massimo entro due mesi se i dati sono conservati sui sistemi "attivi" ed entro sei mesi se i dati sono archiviati sui sistemi di back up.

Google avrà **18 mesi per adeguarsi alle prescrizioni del Garante**.

La responsabilità dei prestatori dei servizi on line

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).

Sulla base delle informazioni attualmente disponibili, risultano due ricorsi pendenti dinanzi al Tribunale Amministrativo Regionale del Lazio ("TAR Lazio") al fine di ottenere l'annullamento del Regolamento, presentati rispettivamente da:

- Associazione nazionale stampa online, Federazione Media digitali indipendenti e Open Media Coalition; e
- Altroconsumo, Movimento Difesa del Cittadino, Assoprovider-Confcommercio e Assintel.

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[2].

Relativamente al ricorso di Altroconsumo, il 9 aprile 2014, si è svolta la **prima udienza dinanzi al TAR Lazio**. Il Giudice amministrativo, non ha adottato alcun provvedimento cautelare.

Risulterebbe, parimenti, pendente un ricorso straordinario al Presidente della Repubblica, rivolto dall'emittente satellitare Sky, per l'eccesso di delega con cui AGCOM avrebbe adottato il Regolamento.

In base ai dati forniti sull'apposita pagina Internet creata dall'AGCOM, dall'entrata in vigore del regolamento, il 31 marzo 2014, risultano giunte all'Autorità 59 istanze, rispetto alle quali sono stati attivati 42 procedimenti, mentre in 17 casi la direzione responsabile ha deliberato l'archiviazione. Per i procedimenti avviati in 12 casi la Direzione responsabile ha disposto l'archiviazione per un adeguamento spontaneo del soggetto interessato. In altri 6 casi la Direzione ha deciso comunque l'archiviazione per ritiro dell'istanza. I 16 casi discussi dal consiglio dell'Autorità si sono invece conclusi in 11 casi con un

[2] 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).

ordine all'operatore di rimuovere il contenuto giudicato illegittimo e in 5 casi con l'archiviazione. Al 10 luglio 2014 risultano pendenti 8 procedimenti.

Ulteriori evoluzioni legislative

Il decreto-legge n. 83/2014 (C. 2426, approvato dalla Camera nella seduta del 9 luglio 2014 e ora all'esame del Senato) prevede, per i profili che qui interessano, che (art. 12, nel testo approvato dalla Camera) siano libere (e, dunque, non necessitino di preventiva autorizzazione) alcune operazioni di riproduzioni di immagini di beni culturali purché attuate senza scopo di lucro per finalità di studio, ricerca, libera manifestazione del pensiero, espressione creativa, promozione della conoscenza del patrimonio culturale. Si tratta de: 1) la riproduzione di beni culturali, ad eccezione dei beni archivistici e bibliografici, attuata in modo che non ci sia alcun contatto fisico con il bene, né l'esposizione dello stesso a fonti luminose, né, all'interno degli istituti di cultura, l'uso di supporti. Si tratterebbe, dunque, di immagini fotografiche acquisite tramite semplici macchine fotografiche o videocamere, smartphone, tablet, purché senza l'uso di flash; 2) la divulgazione con qualsiasi mezzo delle immagini legittimamente acquisite, in modo che le stesse non possano essere ulteriormente riprodotte dall'utente a scopo di lucro neanche indiretto. **Sarà, dunque, possibile pubblicare immagini fotografiche di beni culturali su blog e social network**.

Si ricorda inoltre il recente aggiornamento delle tabelle dell'**equo compenso per la riproduzione privata di fonogrammi e di videogrammi** previsto dalla legge sul diritto d'autore. Il **DM 20 giugno 2014** del Ministero dei beni e delle attività culturali e del turismo prevede un notevole ritocco del compenso (l'ultimo aggiornamento era del 2009) che i produttori devono pagare su smartphone, chiavette Usb, hard-disk esterni, Tv con funzione di registratore e decoder. Di fatto, tutti i dispositivi elettronici che funzionano da archivi digitali. Il DM prevede comunque, con una clausola generale di chiusura, la promozione di protocolli con la Siae per individuare «esenzioni soggettive ed oggettive», per esempio su apparati per videogiochi o per uso professionale di apparecchi. Fuori da questa limitata cerchia, ogni consumatore paga un contributo a sostegno del diritto d'autore.

LA NET NEUTRALITY: PRINCIPI DI LIBERA FRUIZIONE DI SERVIZI E CONTENUTI DELLA RETE

1. La politica dell'Unione europea

Regole comuni per la neutralità della rete[3] **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 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;

[3] 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.

- 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.

2. 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;
- 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.

POLITICHE GENERALI IN MATERIA DI SICUREZZA, EDUCAZIONE E TUTELA DEI DIRITTI

1. Le politiche dell'Unione europea

Nell'ambito delle politiche generali in materia di sicurezza, l'Unione europea ha messo in campo una serie di misure volte a contrastare il cybercrimine, ovverosia quell'ampio spettro di reati specifici a Internet, come ad esempio gli **attacchi** contro i **sistemi di informazione** o il **phishing** (siti bancari fasulli per sollecitare le password che consentono l'accesso ai conti bancari delle vittime), o anche i reati più tradizionali, quali la **frode** e la diffusione di **contenuti illegali**, ad esempio, materiale **pedopornografico** o **incitamenti alla violenza su Internet**, commessi mediante l'uso delle moderne tecnologie di comunicazione.

La Commissione europea, già nel 2007 con la comunicazione "**Verso una politica generale di lotta contro la cibercriminalità**" aveva definito le linee guida di tale politica.

In particolare, gli obiettivi specificamente indicati nella comunicazione consistevano nel: migliorare e facilitare il **coordinamento** e la **cooperazione** fra le **unità** che si occupano di **cibercriminalità**, altre **autorità competenti** e altri **esperti nell'Unione europea**; elaborare un **quadro politico coerente** a livello UE di lotta contro la cibercriminalità; fare opera di **sensibilizzazione sui costi e i pericoli** della cibercriminalità.

La Commissione europea è tornata su tali tematiche il 7 febbraio 2013 con la comunicazione JOIN(2013)1 "**Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro**" (adottata insieme all''Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza), nella quale sono individuati una serie di interventi concernenti, tra l'altro:

- attività di **sensibilizzazione** sul tema della sicurezza;
- sviluppo di un **mercato interno** di prodotti e servizi attinenti alla cibersicurezza;
- promozione di **investimenti**, attività di contrasto alla criminalità informatica;
- elaborazione di una **politica internazionale** dell'UE nel settore.

Si ricorda inoltre che l'aumento dei livelli di sicurezza per i cittadini e le imprese nel ciberspazio costituisce uno degli obiettivi indicati nella **Strategia di sicurezza interna (SSI) 2010-2014**, ideata per permettere all'Unione europea di reagire alle minacce esistenti ed emergenti per la sicurezza della società europea, dei suoi cittadini e delle organizzazioni nell'UE.

Le tre azioni principali riconducibili a tale obiettivo della SSI sono: 1) **potenziare** le capacità delle **autorità di polizia** e delle **autorità giudiziarie**, 2) **collaborare con le imprese** per dare ai cittadini i mezzi per agire e proteggerli e 3) rafforzare la **capacità di far fronte agli attacchi informatici**.

Nell'ambito di tale strategia deve essere inquadrato la costituzione del **Centro europeo per la lotta alla criminalità informatica (EC3),** stabilito presso Europol, e inaugurato agli inizi del 2013. L'EC3 offre **sostegno alle indagini penali** con particolare riferimento alle attività illegali online compiute dalla criminalità organizzata, in particolare gli attacchi diretti contro l'e-banking e altre attività finanziarie online, lo sfruttamento sessuale dei minori online e i reati che colpiscono i sistemi di informazione e delle infrastrutture critiche dell'UE. Il Centro, inoltre, contribuirà a **promuovere la ricerca e lo sviluppo**, ad assicurare lo **sviluppo di capacità** da parte delle autorità incaricate dell'applicazione della legge, dei giudici e dei pubblici ministeri e a effettuare **valutazioni delle minacce**, compresi **analisi delle tendenze, previsioni e allarmi rapidi**. L'EC3 raccoglie e tratta dati relativi alla criminalità informatica e funge da help desk per le unità di contrasto dei paesi dell'UE. Il Centro **offre sostegno operativo** ai paesi dell'UE (ad esempio contro le intrusioni, la frode, l'abuso sessuale di minori online, ecc.) e fornisce **competenze tecniche**, analitiche e forensi di alto livello nelle indagini congiunte dell'UE.

Si ricorda, inoltre, il ruolo **dell'ENISA - Agenzia europea per la sicurezza delle reti e dell'informazione**, che svolge una funzione **consultiva** e di **coordinamento** delle misure adottate dalla Commissione e dai paesi dell'UE per rendere **più sicure le loro reti e i loro sistemi di informazione**. L'ENISA è stata istituita nel 2004, mentre il quadro giuridico ne regola le funzioni è stato recentemente riformato con un regolamento del 2013.

Tra le misure di dettaglio volte a contrastare specifiche forme di cybercrimine messe in campo dall'Unione europea si segnalano, in particolare:

- la Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio. La direttiva contiene, tra l'altro, norme volte a combattere la **pornografia infantile su internet** e il turismo sessuale;

  Tra le fattispecie criminali indicate dalla direttiva sono previsti, tra l'altro:
  - reati di pornografia minorile: possedere, accedere, **distribuire**, **fornire** e produrre **materiale pedopornografico**;
  - reati di **adescamento di minori su internet** per scopi sessuali: **proporre su Internet un incontro con un minore** con l'intento di commettere abusi sessuali o incoraggiarlo, con lo stesso mezzo, a **fornire materiale pornografico che ritragga tale minore**.

  La direttiva obbliga inoltre gli Stati membri a garantire la **tempestiva rimozione** delle pagine web che contengono o diffondono materiale pedopornografico ospitate nel loro territorio e ad adoperarsi per ottenere la **rimozione di pagine ospitate al di fuori del loro territorio**. In determinate condizioni di trasparenza e di informazione degli utenti internet, gli Stati membri hanno altresì facoltà di **bloccare l'accesso a tali siti**.

- la Decisione quadro del Consiglio del 28 maggio 2001 relativa alla lotta contro **le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti** ove, ove sono previste, tra l'altro, disposizioni relative a **illeciti commessi tramite computer**.

- la direttiva 2013/40/UE relativa agli **attacchi contro i sistemi di informazione,** volta ad **armonizzare il diritto penale** degli Stati membri in merito a reati come, ad esempio, l'**accesso** illecito a sistemi di informazione, **l'interferenza illecita** relativamente ai sistemi, l'interferenza illecita relativamente ai dati e l'intercettazione illecita, nonché a **semplificare** la cooperazione tra autorità di contrasto.

Da ultimo, si ricorda che è tuttora all'esame dell'Unione europea una proposta di direttiva COM(2013)48 recante misure volte a garantire un **livello comune elevato di sicurezza delle reti e dell'informazione** nell'Unione. Si tratta in sintesi di: un insieme di obblighi indirizzati agli Stati membri in materia di **prevenzione**, **trattamento** e risposta nei confronti dei **rischi** e degli **incidenti a carico delle reti** e dei **sistemi informativi**; un meccanismo di collaborazione tra gli Stati membri volta ad un'applicazione uniforme della nuova disciplina, che assicuri - se necessario – risposte e trattamenti coordinati ed efficienti dei rischi di incidenti a carico delle reti e dei sistemi informativi; una serie di **obblighi di sicurezza** a carico degli **operatori del mercto** e delle **amministrazioni pubbliche**. Per quanto riguarda quest'ultimo profilo della direttiva, si tratta in particolare di **generalizzare l'obbligo di dichiarazione degli incidenti informatici** (già previsto dalla legislazione Ue per prestatori di servizi di telecomunicazioni tradizionali), estendendone l'applicazione ad **operatori di infrastrutture critiche** (ad esempio nel settore dell'energia e dei trasporti), a **fornitori di servizi dell'informazione** (soggetti che utilizzano piattaforme di commercio informatico, reti sociali, etc.), nonché alle **amministrazione pubbliche**.

Per quanto riguarda il profilo esterno dell'attività Ue si ricordano, in particolare, l'attività della Commissione europea volta a promuovere la Convenzione di Budapest sulla criminalità informatica (nell'ambito del Consiglio d'Europa, firmata nel 2001 ed entrata in vigore nel 2004), in quanto quadro per la cooperazione internazionale nella lotta contro la criminalità informatica, nonché modello per le normative nazionali, nonché la collaborazione con gli Stati Uniti per avviare nel 2012 l'Alleanza mondiale contro l'abuso sessuale di minori online, cui attualmente partecipano 53 paesi, impegnata a migliorare l'individuazione delle vittime, punire i colpevoli, aumentare la sensibilizzazione e ridurre il materiale pedopornografico online.

La sicurezza dei minori on-line è uno degli impegni fondamentali dell'**Agenda digitale europea** ed è parte integrante dei più ampi sforzi della Commissione per garantire la fiducia e la sicurezza on-line.

In tale ambito a maggio 2012 la Commissione ha presentato una **strategia per un internet migliore per i ragazzi** (COM (2012) 196) nella quale è elaborato un piano destinato a garantire ai bambini le competenze e gli strumenti necessari per beneficiare pienamente e in modo sicuro del mondo digitale. La nuova strategia consiste nello sviluppo di un mercato dei contenuti in linea interattivi, creativi ed educativi, in collaborazione fra la Commissione e gli Stati membri, gli operatori di telefonia mobile, i fabbricanti di telefoni cellulari e i prestatori di servizi di socializzazione in rete. Tale strategia si applica anche al cyberbullismo.

La strategia europea per creare un'internet migliore per i ragazzi che definisce un approccio globale nei confronti della sicurezza online dei minori, si applica anche al **cyberbullismo**.

Tra le azioni previste per quanto riguarda la Commissione•

- il finanziamento, a partire dal 2014, di un'infrastruttura di servizio per **sostenere i centri nazionali Safer Internet**[4], i quali forniscono informazioni sulla sicurezza in linea e strumenti di sensibilizzazione dei cittadini al riguardo, nonché piattaforme per la partecipazione giovanile. L'infrastruttura comprenderà anche parametri per lo scambio di buone prassi. Per quanto riguarda l'Italia, nell'ambito del programma Safer Internet la Commissione europea ha co-finanziato il progetto *Generazioni Connesse* avviato nel 2013, che racchiude sotto il coordinamento del Ministero dell'Istruzione, dell'Università e della Ricerca alcune delle principali realtà che si occupano di sensibilizzare i minori ad un utilizzo consapevole di internet e dei new media, quali l'Autorità Garante per l'Infanzia e l'Adolescenza, la Polizia Postale e delle Comunicazioni, Save the Children Italia, Telefono Azzurro, la Cooperativa E.D.I. e il Movimento Difesa del Cittadino. Nel dettaglio Generazioni Connesse promuoverà interventi di sensibilizzazione e formazione in oltre 200 scuole (tra primarie e secondarie di primo grado) su tutto il territorio nazionale, insieme ad attività di peer-education con gli studenti, seminari interattivi con insegnanti e genitori, raggiungendo circa 70.000 persone tra docenti e alunni;
- il sostegno allo sviluppo di pulsanti del browser per le segnalazioni e di link alle linee di emergenza ed il finanziamento di una banca dati per le

[4] Tali centri sono co-finanziati dalla Commissione europea nell'ambito del programma Safer Internet che dal 1999 promuove strategie finalizzate alla promozione e tutela dei diritti online dei più giovani. Per il periodo 2009-2013 Safer internet ha avuto a disposizione un budget di 55 milioni di euro. Per il periodo 2014-2020 il programma Safer Internet è inserito nell'ambito del Meccanismo per collegare l'Europa, che dispone di 1,1 miliardi di euro per le telecomunicazioni

impostazioni sulla privacy per i minori gestita dai centri “Internet più sicuro” (all’interno del citato Meccanismo per collegare l’Europa – CEF);

- il sostegno alla ricerca e allo sviluppo industriali sull’interoperabilità dei sistemi di classificazione dei contenuti (nell’ambito del programma quadro per la competitività e l’innovazione Orizzonte 2020);
- la promozione dello sviluppo di servizi per il riconoscimento dell’età, basati sulle potenzialità tecniche delle carte d’identità riconoscibili a livello UE, come previsto dal progetto legislativo sull’identificazione elettronica (eID);
- investimenti nella ricerca di tecnologie e strumenti per l’identificazione di contenuti pedopornografici (Orizzonte 2020);
- aumento della consapevolezza e del rafforzamento delle capacità, anche attraverso l’insegnamento dell’alfabetizzazione digitale e della sicurezza online in tutte le scuole dell’UE.

2. Il Consiglio d’Europa

Il **Consiglio d'Europa** ha lanciato nel marzo 2014 la ***Campagna di sensibilizzazione per il contrasto del fenomeno dell'incitamento all'odio online***.

L'iniziativa mira a promuovere un monitoraggio partecipativo della rete con lo scopo di individuare e limitare i contenuti di siti, commenti, immagini o video che diffondono messaggi discriminatori.

Il nostro Paese è parte attiva dell'iniziativa ed in particolare il Dipartimento per le politiche della famiglia è partner coinvolto nel Tavolo Tecnico istituito presso il Dipartimento della Gioventù e del Servizio Civile Nazionale.

Obiettivo della campagna è quello di coinvolgere i giovani cittadini europei ed il mondo dell'associazionismo fornendo le competenze per riconoscere e svolgere azioni contro le violazioni dei diritti umani che trovano spazio online. Aumentando la consapevolezza circa il corretto uso dei social network, i giovani tra i 13 e i 30 anni (che costituiscono il target della campagna) sono chiamati a costituire una comunità motivata a discutere e attuare azioni contro l'incitazione all'odio in rete.

La campagna europea è supportata da un sito dedicato, da una campagna online sui social network più diffusi tra i giovani e da materiale di supporto disponibile sia online che offline.

3. Le politiche nazionali

Manca tuttora un inquadramento normativo specifico in materia di bullismo e cyberbullismo.

L'espressione cyberbullismo indica genericamente atti di bullismo e di molestia effettuati tramite mezzi elettronici come l'e-mail, la messaggistica istantanea, i blog, i telefoni cellulari, i cercapersone o i siti web. Il termine "cyberbullying" è stato coniato dall'educatore canadese Bill Belsey nel 2002. I giuristi anglofoni distinguono di solito tra il cyberbullying (cyberbullismo), che avviene tra minorenni, e il cyberharassment (cybermolestia) che avviene tra adulti o tra un adulto e un minorenne.

Anche se il fenomeno appare diffuso in tutto il mondo occidentale sin dalla sua comparsa, la letteratura scientifica sull'argomento non ha ancora raggiunto una definizione condivisa.

Lo studioso Peter Smith e collaboratori (2006) proposero una definizione di cyberbullismo in relazione diretta con le definizioni convenzionali di bullismo. Pertanto il cyberbullismo (cybervullying nella letteratura anglofona) venne definito come un ***atto aggressivo e intenzionale ripetuto nel tempo e compiuto da un individuo o da un gruppo di persone, attraverso l'utilizzo di forme elettroniche di contatto, contro una vittima che non è in grado di difendersi*** (Smith et al., 2006).

Gli stessi autori suddividono il fenomeno in sette categorie:

1) ***sms***: l'invio e la ricezione di messaggi testuali offensivi e diffamatori attraverso il telefono cellulare;

2) ***mms***: l'invio e la ricezione di materiale multimediale (foto/video) recante danno a terze persone;

3) ***calls:*** l'invio e la ricezione di chiamate diffamatorie, in cui l'aggressore intimidisce la vittima con minacce e insulti;

4) ***e-mail:*** l'invio di mail contenenti insulti, minacce, offese e diffamazioni;

5) chatrooms: intimidazioni e offese in chat;

6) ***instant message***: insulti e offese tramite sistemi di comunicazione istantanea (come MSN, Yahoo, Skype etc.);

7) ***websites***: la rivelazione di informazioni personali o la divulgazione di immagini e video compromettenti (per la vittima) attraverso Internet.

Recentemente (Menesini, Nocentini, et al., 2012) è stata indagata l'incidenza del fenomeno "cyberbullismo" in sei diversi paesi europei: Spagna, Germania, Svezia, Estonia, Francia e Italia. ***Per quanto riguarda i dati italiani, tra le pratiche di cyberbullismo più diffuse***, emerge l'invio di messaggi violenti o volgari (flamming), commesso dal 17,8% dei maschi e l'8,7% di femmine; la denigrazione (denigration) coinvolge il 10,2% dei ragazzi e il 6,9% delle ragazze; il furto di identità (impersonification) il 6,2% dei ragazzi e 4,1% delle ragazze;

mentre l'8,4% dei cyberbulli e il 3,8% delle cyberbulle, pratica, invece, l'esclusione della vittima (exclusion) dai gruppi di amici online.

Circa le tecnologie utilizzate, emerge la presenza di diverse modalità (sms, messaggi istantanei, chiamate, chat room, blog) che l'aggressore può utilizzare per compiere atti di bullismo elettronico, il che indica la complessità e le numerose sfaccettature del fenomeno.

Rispetto al bullismo tradizionale nella vita reale, l'uso dei mezzi elettronici conferisce al cyberbullismo alcune caratteristiche proprie quali anonimato del molestatore: in realtà, questo anonimato è illusorio, infatti ogni comunicazione elettronica lascia delle tracce. Per la vittima però è difficile risalire da sola al proprio molestatore; inoltre, a fronte dell'anonimato del cyberbullo, spiacevoli cose sul conto della vittima (spesse volte descritta in modo manifesto, altre in modo solo apparentemente non rintracciabile) possono essere inoltrate a un ampio numero di persone; difficile reperibilità: se il cyberbullismo avviene via sms, e-mail, o in un forum on line privato, ad esempio, è più difficile reperirlo e rimediarvi; indebolimento delle remore etiche: le due caratteristiche precedenti, abbinate con la possibilità di essere «un'altra persona» on line (vedi giochi di ruolo), possono indebolire le remore etiche; spesso la gente fa e dice on line cose che non farebbe o direbbe nella vita reale; assenza di limiti spaziotemporali: mentre il bullismo tradizionale avviene di solito in luoghi e momenti specifici (ad esempio in contesto scolastico), il bullismo informatico investe la vittima ogni volta che si collega al mezzo elettronico utilizzato dal bullo informatico.

Secondo un'***indagine del Censis*** del 2008, il 22,3 per cento delle famiglie denuncia frequenti atti di bullismo nelle classi frequentate dai figli; il 27,6 per cento episodi isolati, mentre il 50,1 per cento non rileva il problema. Nella maggioranza dei casi i genitori segnalano offese ripetute ai danni dell'alunno. I furti di oggetti personali si verificano nel 21,4 per cento delle classi. A questo proposito tra le misure di prevenzione si predispone la realizzazione da parte del Ministero dell'istruzione, dell'università e della ricerca di una ***campagna di informazione da diffondere nelle scuole e uno spot video da trasmettere sui canali RAI*** in fascia di garanzia al fine di raggiungere il maggior numero di ragazzi. All'estero questo primo tipo di intervento ha consentito alle vittime di prendere coscienza del proprio problema e denunciare.

La ricerca più recente sul fenomeno del cyberbullismo (gennaio 2013) è stata realizzata da Ipsos per ***Savethechildren*** (I ragazzi e il cyberbullismo).

Secondo la ricerca, i social network sono la modalità d'attacco preferita dal cyber bullo (61%), che di solito colpisce la vittima attraverso la diffusione di foto e immagini denigratorie (59%) o tramite la creazione di gruppi "contro" (57%). Giovani sempre più connessi, sempre più prepotenti: 4 minori su 10 testimoni di atti di bullismo online verso coetanei, percepiti "diversi" per aspetto fisico (67%) per orientamento sessuale (56%) o

perché stranieri (43%). Madri “sentinelle digitali”: 46 su 100 conoscono la password del profilo del figlio, nota al 36% dei papà.

Neologismo che ha faticato poco ad entrare nel linguaggio quotidiano, il “cyber bullismo” è cresciuto nella fertilità di un non-luogo fuori dalla portata e dal controllo dei ragazzi. Azzerate le distanze grazie alla tecnologia, i 2/3 dei minori italiani riconoscono nel cyber bullismo la principale minaccia che aleggia sui banchi di scuola, nella propria cameretta, nel campo di calcio, di giorno come di notte. E percepiscono, soprattutto le ragazze, alcuni degli ultimi tragici fatti di cronaca molto (33%) o abbastanza (48%) connessi al fenomeno. Per tanti di loro, il cyber bullismo arriva a compromettere il rendimento scolastico (38%, che sale al 43% nel nord-ovest) erode la volontà di aggregazione della vittima (65%, con picchi del 70% nelle ragazzine tra i 12 e i 14 anni e al centro), e nei peggiori dei casi può comportare serie conseguenze psicologiche come la depressione (57%, percentuale che sale al 63% nelle ragazze tra i 15 e i 17 anni, mentre si abbassa al 51% nel nord-est). Più pericoloso tra le minacce tangibili della nostra era per il 72% dei ragazzi intervistati (percentuale che sale all’85% per i maschi tra i 12 e i 14 anni e al 77% nel sud e nelle isole,), più della droga (55%), del pericolo di subire una molestia da un adulto (44%) o del rischio di contrarre una malattia sessualmente trasmissibile (24%).

Per il contrasto al bullismo e al cyberbullismo sono messi a disposizione delle **istituzioni scolastiche**, delle famiglie e delle vittime del fenomeno una serie di strumenti, a cominciare dalla direttiva del Ministro dell’istruzione n. 16/2007, contenente le «*Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo*».

Tra le iniziative già intraprese, sono state richiamate le seguenti:

- l'istituzione del numero verde 800.66.96.96 e l'indirizzo *e-mail* «*bullismo@istruzione.it*» riservato a genitori e studenti per segnalazioni di casi, richieste di informazioni e consigli;
- una nuova versione aggiornata del sito *internet* «*smontailbullo.it*» che si occupa di inquadrare il fenomeno da un punto di vista psico-sociologico e culturale fornendo suggerimenti per fronteggiarlo;
- gli Osservatori regionali permanenti sul bullismo attivi presso gli Uffici scolastici regionali.

Rispetto al tema più specifico del ***cyber*bullismo,** il Ministero ha promosso e sostenuto azioni volte al contrasto di tale fenomeno nel Piano nazionale denominato «Più scuola meno mafia», realizzando, a partire dal 2010, una serie di iniziative a livello locale (es. Milano e Caserta) per informare e formare studenti, famiglie e scuole sull'uso e l'abuso della rete informatica e per la gestione dei casi di stalking, cyberbullismo, e, in generale, per il sostegno alle vittime di comportamenti persecutori, per il sostegno psicologico agli studenti e alle le vittime di reati di bullismo e *cyber* bullismo.

Il Ministero ha poi aderito nel 2010 al **progetto europeo** «*Tabby in internet*» (*Threat Assessment of Bullying Behaviour*: Valutazione della minaccia di *cyber* bullismo nei giovani), approvato nel quadro del programma Daphne III (2007-

2013) e finalizzato a promuovere una cultura della rete «sana», ad accrescere la conoscenza delle minacce derivanti dall'uso di *Internet* e/o di altri mezzi di comunicazione informatizzata e ad attivare strategie e interventi mirati alla prevenzione di comportamenti devianti.

Per quanto riguarda le **iniziative** realizzate recentemente, il Ministero ha lanciato il progetto «*Safer Internet*-Generazioni Connesse» per un utilizzo consapevole di *internet* e dei *new media*.. Poiché anche le scuole sono luoghi strategici e deputati a dare risposte adeguate al problema del cyberbullismo, il Ministero ha realizzato sia il portale «*smontailbullo.it*» che il portale «*URP Social*», primo *social* tematico che una pubblica amministrazione realizza, nei quali vengono offerte alle scuole opportunità di approfondimento e di orientamento rispetto a questo fenomeno sociale, sempre più dilagante.

Nell'ottica del processo di rinnovazione della didattica educativa e della formazione segnato dall'interazione fra tecnologia mobile e concetto di rete, il Ministero ha realizzato due *social* tematici: «*www.webimparoweb.eu*» e «*www.ilsocial.eu*», rivolti ai ragazzi *under* 13 e *over* 14, i quali sono espressione di una piazza virtuale dove poter comunicare e socializzare le proprie esperienze, emozioni nel rispetto delle regole sulla sicurezza informatica, della *netiquette* e delle norme sulla *privacy*. Nella fase di prima attivazione (9 settembre 2013-9 ottobre 2013) ha registrato 1.449 visite e 6.038 visualizzazioni di pagina.

Il ***vuoto normativo derivante dalla mancanza di un reato specifico*** sul cyberbullismo ***viene colmato dalla giurisprudenza*** ricorrendo alle fattispecie esistenti. I comportamenti posti in essere possono produrre conseguenze sia sul piano civilistico sia su quello penalistico. I reati che si possono configurare sono: ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), violenza privata (art. 610 c.p.), minaccia (art. 612 c.p.).

Se, come spesso accade, l'autore è un minore di età ricompresa tra i 14 e i 18 anni, si applicheranno le norme del processo penale minorile (D.P.R. n. 448 del 1988). Per il minore che, nel momento in cui ha commesso il fatto, non aveva compiuto i 14 anni, non essendo imputabile, possono essere adottate misure rieducative.

Per colmare il vuoto normativo la **Commissione Giustizia della Camera** ha avviato il 29 maggio 2014 l'esame della ***proposta di legge Campana A.C. 1986*** *(Disposizioni per la prevenzione e il contrasto del bullismo e del bullismo informatico)* che, dopo aver definito le condotte di bullismo e cyberbullismo, punisce con la reclusione da 6 mesi a 4 anni chiunque attraverso tali condotte, «cagiona un perdurante e grave stato di ansia o di paura ovvero ingenera un fondato timore per la propria incolumità».

Le conversazioni sulla rete Internet, nei blog come nei social network - se rappresentano una straordinaria opportunità per lo sviluppo della comunicazione e dello scambio culturale tra persone, spesso a migliaia di km di distanza - sono tuttavia occasione per forme sempre nuove di "hate speech", espressione anglofona tradotta spesso in italiano con la formula ***"incitamento all'odio"***

Lo **hate speech** è una categoria elaborata negli anni dalla giurisprudenza americana per indicare un ***genere di parole e discorsi che non hanno altra funzione a parte quella di esprimere odio e intolleranza verso una persona o un gruppo***, e che rischiano di provocare reazioni violente contro quel gruppo o da parte di quel gruppo. Così in modi impliciti ed espliciti, tra le pieghe della rete o sovraesposti, troviamo forme diverse di hate speech online: da quelli sessisti e omofobici a quelli prodotti contro le religioni diverse e contro diverse affiliazioni, fino a discorsi d'odio prodotti sulla base di etno-nazionalisimi, a sfondo razzista o di discriminazione politica.

E' questo un tema che alimenta un dibattito molto attuale e ancora più controverso in relazione alla ***libertà di espressione su Internet***, dove non esistono specifiche normative internazionali condivise. Le grandi aziende come Google e Facebook affidano la compilazione delle norme di utilizzo dei servizi a un gruppo di lavoro specifico, che chiamano scherzosamente i Deciders, quelli che decidono" (dal nomignolo dato al direttore del settore legale di Twitter, Nicole Wong, quando lavorava per Google).

Il *Community standard* di ***Facebook*** non consente i contenuti che incitano all'odio, ma attua una distinzione tra contenuti seri e meno seri. Se da un lato incoraggia gli utenti a mettere in discussione idee, eventi e linee di condotta, non consente la discriminazione di persone in base a razza, etnia, nazionalità, religione, sesso, orientamento sessuale, disabilità o malattia.

Più rigidamente le Norme della community di ***Youtube*** vietano esplicitamente l'incitamento all'odio (linguaggio che attacchi o umilii un gruppo in base a razza o origine etnica, religione, disabilità/invalidità, sesso, età, condizione sociale o orientamento sessuale/identità di genere).

Twitter è il più "aperto": non vieta esplicitamente lo hate speech e neppure lo cita, eccetto che in una nota sugli annunci pubblicitari (in cui peraltro specifica che la campagne politiche contro un candidato «generalmente non sono considerate hate speech»). Twitter ha però introdotto nel 2013 un bottone all'interno di ogni tweet per indicare l'incitamento all'odio (evitando, tra l'altro, quindi di dover raggiungere il Centro Assistenza dove inoltrare la documentazione delle offese). Inoltre ha aumentato lo staff che gestisce le denunce degli iscritti e ha in cantiere altri progetti contro i discorsi dell'odio.

In tanti social network esistono meccanismi di segnalazione, come ad esempio le bandierine. Ma un collo di bottiglia restano le procedure di controllo degli avvisi che arrivano dagli utenti quando vedono gli hate speech: spesso

sono affidate in outsourcing a personale esterno che non di rado può sottovalutare l'ampiezza di una campagna di odio.

Per quel che riguarda l'Italia, il nostro **ordinamento non prevede una fattispecie di reato** applicabile a tutte le ipotesi di **incitamento all'odio**.

L'organizzazione internazionale non governativa, Human Rights Watch, nel suo Rapporto sulla violenza razzista e xenofoba in Italia, pubblicato il 21 marzo 2011, rileva che, pur esistendo la legge n. 205 del 1993, anche detta "Legge Mancino", diretta a perseguire l'odio razziale, questo stesso strumento soffra della mancanza di qualunque riferimento all'orientamento sessuale, all'identità di genere e alla disabilità, quali motivi scatenanti i crimini d'odio. Un vuoto giuridico che la stessa organizzazione chiede sia prontamente colmato.

La l**egge Mancino**, può considerarsi la principale base normativa nella lotta ai crimini d'odio. Essa incrimina tanto le violenze quanto l'incitamento alla violenza per motivi razziali, etnici, nazionali o religiosi, e coordinandosi con la legge n. 654 del 1975 appronta specifiche e ulteriori sanzioni anche per coloro che partecipano ad associazioni, movimenti o gruppi avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi.

Tuttavia, ***risultano totalmente sconosciuti all'incriminazione gli altri motivi discriminatori, in specie quelli relativi all'orientamento sessuale, all'identità di genere e alle disabilità***, che pur comunemente attengono alle problematiche dei crimini d'odio.

I tentativi di rinfoltire la categoria dei soggetti tutelati dalla Legge Mancino sono stati portati avanti con diversa intensità in diverse legislature e già al tempo dell'approvazione del testo di legge nel 1993. Nessuno di questi è però mai giunto ad una conclusione definitiva.

Nella XVI legislatura la Commissione giustizia della Camera ha - in tre occasioni - avviato l'esame di proposte di legge di iniziativa parlamentare volte a contrastare le discriminazioni fondate su motivi di omofobia e transfobia, svolgendo un'ampia attività istruttoria e conoscitiva. Nei primi due casi è stata l'Assemblea ad approvare pregiudiziali di costituzionalità che hanno bloccato il successivo iter dei provvedimenti; nell'ultimo caso è stata la stessa Commissione giustizia ad approvare un emendamento interamente soppressivo del testo sottopostole.

In questa legislatura è stata **approvato dalla Camera, il 19 settembre 2013, un testo unificato (A.S. 1052)**, attualmente all'esame del Senato, che aggiunge tra le condotte di istigazione, violenza e associazione finalizzata alla discriminazione punite dalla legge Mancino anche quelle ***fondate sull'omofobia o sulla transfobia.*** Il testo non contiene alcun riferimento specifico al mezzo attraverso cui viene diffuso l'incitamento all'odio.

Con riferimento all'**educazione a Internet nelle scuole**, il MIUR promuove il Piano Scuola Digitale diretto a modificare gli ambienti di apprendimento attraverso l'integrazione delle tecnologie nella didattica.

Le azioni del piano riguardano, in particolare:

- l'editoria digitale scolastica, inserita nel piano delle attività dell'Agenda digitale europea e nazionale per migliorare l'alfabetizzazione, le competenze e l'inclusione nel mondo digitale;
- le iniziative CI@ssi 2.0 e lavagna interattiva multimediale (LIM) finalizzate a modificare gli ambienti di apprendimento con un utilizzo costante e diffuso delle tecnologie a supporto della didattica;
- le iniziative @urora e Oltre l'@urora, per agevolare il reinserimento di minori in situazioni di svantaggio attraverso l'acquisizione di competenze certificate mediante strumenti di comunicazione multimediale;
- l'HSH@Network (Hospital School Home Network), per il supporto dell'apprendimento di studenti ospedalizzati o in terapia domiciliare mediante le nuove tecnologie.

Si segnala peraltro che l'**articolo 11** del DL. 104/2013 (L. 128/2013) ha autorizzato la spesa per gli anni 2013 e 2014, rispettivamente di **5 milioni di euro** e di **10 milioni di euro**, per assicurare alle istituzioni scolastiche statali secondarie, prioritariamente a quelle di secondo grado, la realizzazione e la fruizione della **connettività *wireless***, in modo da consentire agli studenti l'accesso ai materiali didattici ed ai contenuti digitali. L'assegnazione delle risorse alle istituzioni scolastiche è effettuata in proporzione al numero di edifici scolastici.

Con riferimento invece ai **contenuti didattici**, si segnala quanto contenuto, per quanto riguarda la **scuola dell'infanzia e del I Ciclo di Istruzione**, nelle Indicazioni nazionali per il curricolo che fanno rientrare nel profilo delle competenze al termine del Primo ciclo di istruzione (v. p. 10) le buone competenze digitali, la consapevolezza nell'uso delle tecnologie della comunicazione per ricercare e analizzare dati e informazioni, per distinguere tra informazioni attendibili e quelle che necessitano di approfondimento, controllo e verifica e per interagire con soggetti diversi nel mondo. Le predette Indicazioni fanno peraltro riferimento alla definizione ufficiale delle otto competenze-chiave (Raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006 (2006/962/CE)), tra cui la "competenza digitale" che consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (ICT): l'uso del computer per reperire, valutare, conservare, produrre, presentare e

scambiare informazioni nonchè per comunicare e partecipare a reti collaborative tramite Internet.

Con riferimento ai **Licei**, le Indicazioni nazionali riportano obiettivi specifici di apprendimento per quanto riguarda più strettamente l'Informatica. Per il primo biennio l'obiettivo è saper usare gli strumenti di lavoro più comuni del computer insieme ai concetti di base ad essi connessi e conoscere, tra l'altro, la struttura e i servizi di Internet, per condurre gli studenti a un uso efficace della comunicazione e della ricerca di informazioni e alla consapevolezza delle problematiche e delle regole di tale uso.

Con riferimento agli **istituti tecnici e professionali**, infine, le linee guida per il passaggio al nuovo ordinamento, in particolare per il Primo biennio (Istituti tecnici e Istituti professionali) prevedono l'insegnamento dell'informatica e delle tecnologie dell'informazione e della comunicazione.

PRECEDENTI INIZIATIVE PER LA REGOLAZIONE DI INTERNET

Negli ultimi anni tra le iniziative volte a individuare principi e linee guida in tema di garanzie, diritti e doveri per l'uso di internet, si segnala in particolare il documento predisposto dal Ministro dell'Istruzione del Governo Monti (Profumo), nel settembre 2012, dal titolo "*Principi fondamentali di internet*".

Il documento, sul quale il Governo ha aperto una consultazione pubblica, individuava in primo luogo alcuni principi fondamentali di internet nei principi generali che definiscono l'infrastruttura, nella cittadinanza in rete, negli utenti in quanto consumatori di servizi in Internet, nella produzione e circolazione dei contenuti e nella sicurezza della rete.

Tra i principi generali che definiscono Internet, il documento governativo sottolineava come la rete rappresenti un bene comune e uno strumento cruciale per lo sviluppo e l'esercizio dei diritti umani; riaffermava la neutralità della rete e la sua architettura aperta e sottolineava i benefici della tecnologia e della rete nonché del modello decisionale trasparente, con il coinvolgimento di tutti i portatori di interesse.

La cittadinanza in rete veniva dunque sviluppata in relazione ai seguenti principi:

- Accesso all'infrastruttura indipendentemente dal luogo di residenza
- Punti di accesso ad Internet
- Accesso e riutilizzo dei dati del settore pubblico
- Accessibilità come strumento di inclusione
- Diritti umani e libertà fondamentali in rete e per mezzo della rete
- Auto-organizzazione e autonomia degli individui in rete

Il profilo degli utenti veniva poi affrontato attraverso il tema delle competenze e dell'identità digitale, della riservatezza e della necessaria archiviazione e poi cancellazione dei dati personali.

Riconoscendo come la Rete sia un luogo di produzione e scambio di conoscenza e, in quanto tale, rappresenti un'inestimabile risorsa per l'educazione, l'informazione, la ricerca, e lo sviluppo dei popoli, il documento sottolinea l'esigenza che la *governance* di Internet scaturisca dall'apporto e dalla partecipazione attiva dei cittadini, ossia di coloro che quotidianamente usano e costruiscono la rete e le sue applicazioni.

PROFILI INTERNAZIONALI

Internet Governance Forum - IGF

L'evoluzione di Internet, penetrato nel corso di mezzo secolo in tutti i settori della vita politica, economica, culturale e sociale e divenuto l'ambiente dell'interazione a tutto campo di una massa via via crescente di individui ed istituzioni, ha prodotto la definizione, accolta anche in ambito accademico, di ***Internet Eco System***.

Il complesso tema della *governance* di Internet è stato affrontato, in sede Onu, con l'**Internet Governance Forum (IGF)** creato nel 2006 dal Segretario Generale.

L'iniziativa venne intrapresa a seguito dei ***World Summit on Information Society*** **(WSIS)** di Ginevra (2003) e Tunisi (2005), in particolare par. 72 dell'Agenda di Tunisi.

L'**IGF** è divenuto il principale **forum multilaterale** su questioni di politica pubblica relative alla *governance* di Internet; si tratta, infatti, della sede internazionale dedicata alla rete che, con **approccio multistakeholder** facilita il confronto, su un piede di parità, tra tutti i portatori di interesse internazionali: governi, società civile, mondo accademico, comunità tecniche, settore privato.

Sebbene istituito in ambito Onu, l'**IGF** è un **forum aperto** che non contempla né *membership* né la ricerca di soluzioni negoziali.

Si tratta, invece, di un luogo di discussione delle questioni di politica pubblica sugli elementi chiave della *governance* di Internet al fine di promuoverne sostenibilità, sicurezza, stabilità e sviluppo.

La *mission* di IGF consiste, tra l'altro, nell'agevolare il dialogo tra gli enti che si occupano di politiche pubbliche trasversali relative a Internet, nell'interfacciare con le organizzazioni governative sulle questioni di loro competenza, nel facilitare lo scambio di informazioni e di *best practices*, facendo pieno uso delle competenze delle comunità accademiche, scientifiche e tecniche; nel migliorare il coinvolgimento delle parti interessate nei meccanismi di *governance* di Internet esistenti e/o futuri; nell'individuare e far emergere le criticità portandole all'attenzione degli organi competenti e del pubblico in generale, formulando, se del caso, raccomandazioni; nel contribuire allo sviluppo delle capacità di

governance di Internet nei paesi in via di sviluppo, attingendo pienamente alle risorse locali di conoscenze e competenze.

L'IGF, che vuole costituire una sede di informazioni ed ispirazione per i *policy makers* del settore pubblico e privato, pubblica i propri lavori e dà conto delle attività organizzate nel proprio ambito sul sito http://www.intgovforum.org/cms/

L'IGF vuole essere uno spazio neutro che pone tutti gli attori su un piano di parità ed è, pertanto, dotato di *power of recognition*, ossia il potere di individuare le questioni chiave; tra le più in evidenza quelle derivanti dal *cloud computing*, dal così detto *"Internet delle cose"* , e dalle minacce ai diritti umani ed alla sicurezza nel cyberspazio.

Dal punto di vista organizzativo, l'IGF è assistito da un segretariato ubicato a Ginevra, ed è convocato dal Segretario Generale dell'Onu, che si avvale di un gruppo di 55 consulenti *(Multistakeholder Advisory Group – MAG*) da lui stesso nominati in rappresentanza di governi, settore privato società civile, comunità accademiche e tecniche, che lo assistono sul programma e sul calendario degli incontri del Forum.

Quanto alle risorse finanziarie (http://www.intgovforum.org/cms/funding), le attività del Segretariato dell'IGF sono finanziate con contributi fuori bilancio versati in un fondo fiduciario gestito dall' UNDESA (Dipartimento delle Nazioni Unite per gli Affari Economici e Sociali) cui contribuisce anche la Commissione europea; l'IGF è finanziato, inoltre, da donazioni da parte di gruppi di interesse mentre la maggior parte dei costi connessi alla riunione annuale è sostenuta dai paesi ospitanti.

Il mandato dell'IGF, che scadrà nel dicembre 2015 (l'ultima proroga quinquennale risale al dicembre 2010), dovrebbe essere rinnovato dall'Assemblea Generale dell'Onu (69ª sessione).

Il Forum si articola in una varietà di iniziative, regionali, nazionali e tematiche. Queste ultime, denominate ***Dynamic coalitions,*** sono raggruppamenti informali costituiti da rappresentanti di almeno tre gruppi di *stakeholders* che si aggregano intorno a temi specifici, rispetto ai quali si pongono come piattaforme aperte di discussione; chiunque, registrandosi sul sito, se ne può fare promotore e l'iniziativa è sottoposta al vaglio del segretariato IGF. Attualmente sono attive 12 *Dynamic coalitions*, incentrate su una gamma di tematiche della governance di Internet che spazia dalla neutralità del network, all'ottica di genere nell'Internet governance, alla *child on line safety.*

Ma è attraverso l'**Annual IGF meeting** che vengono propiziate visioni comuni su più ampia scala sia sul lato dell'ottimizzazione delle opportunità offerte da Internet, sia su quello della reazione ai rischi ed alle sfide dell'interconnessione globale.

La **nona edizione** dell'**Annual IGF Meeting,** che avrà luogo ad Istanbul il prossimo 2-5 settembre 2014, si incentrerà su *"Connecting Continents for Enhanced Multistakeholder Internet Governance"* nonché su una serie di sottotemi tra i quali accesso ad Internet, creazione, diffusione ed uso di contenuti, Internet e sviluppo, risorse critiche, Internet e diritti umani, ruolo di IGF nel futuro dell'*Internet ecosystem.*

Carta dei diritti per la Rete

Dopo che già al WSIS di Tunisi era emersa la necessità di una **Carta dei diritti per la Rete** che *"parta proprio dalla constatazione che Internet sta realizzando una nuova, grande redistribuzione del potere"*[5]*,* in vista del **2° meeting annuale** IGF (Rio de Janeiro, novembre 2007) l'Italia aveva dato vita, insieme al Brasile, alla città di Parigi, alle ONG italiane e ad altri, ad una *Dynamic Coalition* finalizzata alla definizione ed all'adozione internazionale di una Carta dei Diritti di Internet, ***l'Internet Bill of Rights***, organizzando un forum di discussione a Roma sul tema. Nonostante gli autorevoli *endorsement* al progetto, emersi anche in chiusura del forum di Rio, l'*Internet bill of rights* non ha ancora visto la luce.

La **Charter of Human Rights and Principles for the Internet (IRPC Charter)** (http://internetrightsandprinciples.org/site/) costituisce uno dei più recenti esiti dell'attività di networking basata sull'IGF ed è il risultato dell'azione della *Dynamic Coalition* denominata *Internet Rights and Principles Coalition* costituita da persone ed organizzazioni che lavorano per la difesa dei diritti umani nell'ambiente Internet. L'Italia vi partecipa anche a livello governativo.

Il documento, presentato come contributo al NET Mundial *(Multistakeholder Meeting on the Future of Internet Governance)* di San Paolo del Brasile (23-24 aprile 2014) condensa in **10 principi generali**, senza alterarne complessivamente il contenuto, le 21 clausole della carta risalente al 2011 e già riconosciuta come uno degli esempi di maggior successo del modello *multistakeholder* dell'Internet governance.

---

[5] Stefano Rodotà, *Una Costituzione per Internet,* in *Notizie di Politeia, XXII, 82, pp. 177-182.*

I dieci principi, radicati nelle norme internazionali sui diritti umani e posti a costituire la base della *governance* di Internet sono:

1. **Universalità e uguaglianza**. Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti, che devono essere rispettati e protetti nella rete Internet;
2. **Diritti e Giustizia Sociale.** Internet è uno spazio per la promozione, la protezione, il rispetto dei diritti umani e la promozione della giustizia sociale. Ognuno ha il dovere a rispettare i diritti umani di tutti gli altri nella rete Internet;
3. **Accessibilità.** Tutti hanno pari diritto di accesso e di utilizzo di un Internet sicuro e aperto;
4. **Espressione e associazione.** Ogni individuo ha il diritto di cercare, ricevere e comunicare informazioni liberamente su Internet senza censure o altre interferenze. Ognuno ha anche il diritto di libera associazione attraverso Internet, per motivi e fini sociali, politici, culturali o altri;
5. **Privacy e protezione dei dati.** Ogni individuo ha diritto alla privacy online. Questo include la libertà dalla sorveglianza, il diritto di utilizzare la crittografia, e il diritto di anonimato in Internet. Ogni individuo ha diritto alla protezione dei dati, incluso il controllo sulla raccolta di dati personali, la loro conservazione e trasformazione, la cessione e la divulgazione;
6. **Vita, libertà e sicurezza**. Il diritto alla vita, alla libertà e alla sicurezza devono essere rispettati, protetti e realizzati su Internet. Questi diritti non devono essere violati o utilizzati per violare altri diritti nella rete digitale;
7. **Diversità.** La diversità culturale e linguistica su Internet deve essere promossa, l'innovazione tecnica e politica dovrebbero essere incoraggiate a facilitare la pluralità di espressione;
8. **Uguaglianza**. Ciascuno deve avere un accesso universale e aperto ai contenuti di Internet, liberi da priorità discriminatorie, filtraggi o controlli del traffico per ragioni commerciali, politiche o altre ragioni;
9. **Norme e regolamento.** L'architettura di Internet, i sistemi di comunicazione ed i formati dei documenti e dei dati si basano su standard aperti per garantire la completa interoperabilità, l'inclusione e le pari opportunità per tutti;
10. **Governance.** I diritti umani e la giustizia sociale devono costituire il quadro giuridico e normativo fondamentale su cui Internet funziona ed è governato. Questo deve avvenire in modo trasparente e multilaterale, basato su principi di apertura, di partecipazione inclusiva e di responsabilità.

Recenti iniziative nell'ambito del Consiglio d'Europa

Il **Comitato dei Ministri del Consiglio d'Europa** in occasione della 1197ª riunione dei Delegati dei Ministri del **16 aprile 2014** ha adottato la **Raccomandazione CM/Rec(2014)6** relativa a una **Guida dei diritti umani per gli utenti di Internet.**

La **Raccomandazione** prevede che:

1. gli Stati membri garantiscano ad ogni persona soggetta alla propria giurisdizione i **diritti umani e le libertà fondamentali** sanciti dalla Convenzione europea dei diritti dell'uomo, **obbligo ugualmente valido nel contesto dell'utilizzo di Internet**, nel cui ambito si applicano altresì le altre convenzioni e gli altri strumenti del Consiglio d'Europa riguardanti la protezione del diritto alla libertà di espressione, all'accesso all'informazione, alla libertà di riunione, la protezione contro la criminalità informatica e il diritto alla vita privata e alla protezione dei dati a carattere personale;
2. gli obblighi relativi alla protezione ed alla promozione dei diritti umani comprendono anche la **vigilanza in tal senso sulle imprese private**;
3. sia riconosciuto il **valore di servizio pubblico di Internet**;
4. gli **utenti** di Internet siano **consapevoli dei diritti umani di cui godono online** e li sappiano esercitare qualora siano imposte restrizioni o si verifichino ingerenze;
5. al fine di garantire che i diritti umani e le libertà fondamentali si applichino in **ugual misura online e offline**, il Comitato dei Ministri, conformemente all'Articolo 15.*b* dello Statuto del Consiglio d'Europa, raccomanda agli Stati membri di:

   5.1. **promuovere attivamente la Guida dei diritti umani per gli utenti di Internet**, allegata alla raccomandazione, **presso i cittadini, le istituzioni pubbliche e gli operatori del settore privato e adottare misure specifiche in vista della sua applicazione**;

   5.2. valutare, esaminare regolarmente e ove necessario eliminare le restrizioni all'esercizio dei diritti e delle libertà su Internet, in particolare quando quest'ultime non siano in conformità con la Convenzione, alla luce della pertinente giurisprudenza della Corte europea dei diritti dell'uomo;

   5.3. garantire che gli utenti di Internet abbiano **accesso a ricorsi effettivi**, nel caso in cui i loro diritti e le loro libertà abbiano subito restrizioni o se ritengono che siano stati lesi.

   5.4. promuovere il coordinamento con altri attori statali e non statali, all'interno e all'esterno del Consiglio d'Europa, per quanto concerne le norme e le procedure che incidono sulla protezione dei diritti umani e delle libertà fondamentali su Internet;

5.5. incoraggiare il **settore privato**, che dovrebbe essere incoraggiato a **contribuire alla diffusione della Guida**, ad avviare un vero dialogo con le autorità pubbliche competenti e con la società civile sul tema della responsabilità sociale delle imprese;

5.6. incoraggiare la **società civile** a sostenere la diffusione e l'applicazione della Guida, affinché possa costituire uno strumento efficace al servizio degli utenti di Internet.

La **Guida dei diritti umani per gli utenti di Internet** costituisce la concretizzazione di un progetto annunciato al **6º Annual Forum IGF** (Nairobi, settembre 2011).

La guida, elaborata nell'ambito della strategia di lungo termine del Consiglio d'Europa ed adottata dal Comitato dei Ministri in rappresentanza degli Stati membri, è **basata sui diritti e libertà sanciti dalla Convenzione europea dei diritti dell'uomo** e sull'interpretazione di tali diritti da parte della Corte europea dei diritti dell'uomo. Essa è finalizzata a consentire agli utenti **l'esercizio online dei diritti umani**, concentrandosi su quelli di maggiore impatto per il web: il diritto di accesso e di non discriminazione, la libertà di espressione e di informazione, libertà di riunione, di associazione e di partecipazione, la protezione della vita privata e dei dati personali, il diritto all'istruzione ed alle conoscenze generali, la protezione dei bambini e dei giovani, il diritto a un ricorso effettivo in caso di violazione dei diritti umani online.

La guida[6] è il prodotto di una vasta consultazione multipartenariale avviata presso governi, imprese private (in particolare fornitori di servizi online e di telecomunicazioni), esponenti della società civile e del mondo tecnico ed accademico.

Al Forum IGF di Nairobi il Consiglio d'Europa aveva presentato i **10 principi della *governance* di Internet** adottati dal suo Comitato dei Ministri, che dovrebbero essere accolti dai 47 paesi membri nello sviluppo di politiche nazionali ed internazionali legate a Internet (https://wcd.coe.int/ViewDoc.jsp?id=1835773).

I principi sono:

1. Human rights, democracy and rule of law;
2. Multi-stakeholder governance;
3. Responsibilities of states;
4. Empowerment of Internet users;
5. Universality of the Internet;

[6] Guida in breve, in lingua italiana https://wcd.coe.int/ViewDoc.jsp?Ref=DC-PR049%282014%29&Language=lanItalian&Ver=original&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE

6. Integrity of the Internet;
7. Decentralised management;
8. Architectural principles;
9. Open network;
10. Cultural and linguistic diversity

La **Guida,** allegata alla Raccomandazione del 16 aprile 2014 è articolata in un'introduzione e 6 paragrafi e si rivolge direttamente agli utenti ai quali rammenta i propri diritti. La Guida presenta in sintesi i seguenti contenuti:

Introduzione: esplicita i **destinatari della Guida** (tutti gli utenti di Internet), le **finalità** (la tutela dei diritti nel contesto di Internet) ed i **fondamenti giuridici** (la Convenzione europea dei diritti dell'uomo e le altre convenzioni o strumenti del Consiglio d'Europa relative alla tutela dei diritti umani, vincolanti per gli Stati membri). Nella guida si precisa che non vengono così creati nuovi diritti, bensì sono estesi al web gli stessi diritti dell'*off-line*.

Libertà di espressione e di informazione: vi si richiama il diritto di cercare, ricevere e comunicare informazioni ed idee senza ingerenze da parte delle autorità pubbliche e senza limiti di frontiera.

Riunione, associazione e partecipazione: riguarda il diritto di riunione ed associazione in modo pacifico attraverso Internet.

Protezione della vita privata e dei dati personali: rammenta il diritto al rispetto della vita privata e familiare su Internet, comprensivo della protezione dei dati personali e del rispetto della segretezza della corrispondenza e delle comunicazioni.

Istruzione e conoscenze generali: riguarda il diritto all'istruzione, compreso l'accesso alle conoscenze.

Bambini e giovani: viene loro rammentato il diritto a godere di tutti i diritti e di tutte le libertà indicate nella Guida, con particolare riguardo, in relazione all'età, al diritto a una protezione particolare e ad un affiancamento specifico durante l'utilizzo di Internet.

Ricorsi effettivi: si diffonde sulle modalità di esercizio del diritto al ricorso precisando che le vie per adirlo dovrebbero essere disponibili, note, accessibili,

economicamente abbordabili ed appropriate ad ottenere una riparazione adeguata.

Si segnala altresì che, sul **diritto di accesso ad Internet,** è intervenuta, da ultimo, l'Assemblea parlamentare del Consiglio d'Europa che, il 9 aprile 2014, ha approvato la **raccomandazione n. 1987 sul diritto di accesso a Internet**, sottolineando che esso deve essere ispirato al principio di neutralità della rete. La risoluzione evidenzia che, poiché la libertà di espressione passa anche attraverso il web, gli Stati del Consiglio d'Europa devono prevedere un diritto di accesso per ciascuno, tanto più che Internet serve anche a garantire un contatto tra cittadini ed autorità pubbliche. Il diritto di accesso a Internet, sottolinea l'Assemblea parlamentare, è un requisito essenziale per l'esercizio dei diritti in base alla Convenzione ed è pertanto essenziale a garantire la democrazia. Indispensabili, inoltre, interventi di carattere tecnico da parte degli Stati e meccanismi che consentano l'utilizzo della rete da punti di accesso pubblici.

PROFILI COMPARATI

Francia

L'ordinamento francese riconduce la **tutela della privacy su internet** al **diritto al *respect de la vie privée*** sancito dal *Code civil* francese secondo il quale "ciascuno ha diritto al rispetto della vita privata" (art.9) e derivante, secondo il Consiglio costituzionale, dal più generale diritto alla libertà proclamato dalla *Déclaration des droits de l'homme et du citoyen de 1789* (art. 2). Pur mancando una definizione legale di "vita privata", la giurisprudenza ha nel tempo ampliato gli ambiti suscettibili di tutela in base a tale diritto quali, tra gli altri, il domicilio, l'immagine, la voce, lo stato di gravidanza, lo stato di salute, la vita sentimentale e la corrispondenza. Il *Code pénal* (artt. 226-1 e ss.) ne sanziona le violazioni e dedica, in particolare, disposizioni specifiche agli attentati ai diritti della persona risultanti da banche dati o da trattamenti informatici di dati personali (articoli da 226-16 a 226-24).

Lo sviluppo delle tecnologie dell'informazione e della comunicazione su Internet (messaggerie elettroniche, social network, blog, etc.), hanno richiesto esigenze specifiche per garantire il diritto alla tutela e al rispetto della *privacy*, sia a livello europeo che nazionale. Il ***Code des Postes et des Communications électroniques***, in conformità con la normativa UE in materia, dedica una sezione alla ***Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques*** (articoli da L34-1 a L34-6). Le disposizioni del Codice riguardano, soprattutto, il trattamento di dati personali nell'ambito della fornitura al pubblico di servizi di comunicazioni elettroniche, con particolare riferimento alle reti che gestiscono dispositivi di raccolta di dati e di identificazione di dati personali, ma prevedono anche una tutela degli utenti "consumatori" della rete, quali le norme relative al divieto di *spamming* che assicurano il principio dell'accordo preventivo dell'utente (*opt in*) sull'arrivo di messaggi pubblicitari e sull'installazione di *cookies* (art. L34-5).

Anche il fatto che lo stesso soggetto abbia rivelato fatti e informazioni relativi alla sua vita privata non autorizza automaticamente la "redivulgazione" di alcuni di tali fatti senza un'apposita autorizzazione (diritto all'oblio), se non quando la pubblicazione di tali fatti non abbia la finalità di nuocere e obbedisca ad un interesse legittimo. A proposito del delicato tema del "**diritto all'oblio**", si segnala che nell'ottobre 2010 sono state siglate, da alcuni importanti operatori di siti e motori di ricerca (tra i quali Microsoft) due specifiche **Carte del diritto all'oblio digitale** elaborate e promosse dall'allora Segretario di Stato francese all'economia digitale Nathalie Kosciusko-Morizet:

- la *Charte du Droit à l'oubli numérique* nella **pubblicità "mirata"**, che riguarda i dati personali raccolti passivamente, senza che l'utente della rete ne sia veramente a conoscenza e utilizzati per veicolare messaggi pubblicitari online (ad es. spam);
- la *Charte du Droit à l'oubli numérique* nei **siti collaborativi e nei motori di ricerca**, che riguarda i dati personali pubblicati intenzionalmente sulla rete dall'internauta.

Le due Carte, che si configurano come una sorta di codice di condotta il cui contenuto ha valenza prevalentemente programmatica, hanno l'obiettivo, tra gli altri, di proteggere la vita privata su internet e di semplificare e facilitare la soppressione e la de-indicizzazione di dati personali pubblicati su internet.

In particolare la seconda Carta, relativa ai social network e ai motori di ricerca, 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. I rappresentanti di siti collaborativi e di motori di ricerca si sono impegnati a mettere a punto nuovi dispositivi al fine di garantire la protezione dei dati privati degli utenti di Internet.

In tale ambito sono previste una serie di azioni finalizzate alla sensibilizzazione ed educazione degli internauti, alla protezione dei dati personali dall'indicizzazione automatica da parte dei motori di ricerca; alla gestione da parte degli internauti dei dati pubblicati in rete; all'adozione di misure d'informazioni specifiche a beneficio dei minori; all'istituzione di un organismo competente a ricevere le richieste di cancellazione o modifica dei dati personali da parte degli utenti e alla gestione del trasferimento di dati. Per quanto riguarda i *social network*, si tratta in special modo di creare un "ufficio dei reclami" virtuale che permetta di centralizzare le richieste di modifica dei dati o di soppressione di un account. I motori di ricerca, dal canto loro, dovrebbero impegnarsi a sopprimere più rapidamente la maschera di collegamento (*cache*) delle pagine web quando il loro contenuto indesiderato figuri sui social network, in modo da far sparire i risultati dei motori di ricerca potenzialmente nocivi per la reputazione sulla rete dell'internauta. Tuttavia il **rifiuto di** due colossi come **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.

Il *Code des Postes et des communications éléctroniques* (cfr. in particolare art. 32-1) riconosce e assicura anche l'attuazione del **principio della neutralità delle reti** secondo il quale una "rete pubblica di massima utilità" aspira a trattare tutti i suoi contenuti, siti e piattaforme nella stessa maniera; neutralità che consente alla rete (internet o altre reti, come i servizi di rete mobile) di "trasportare" ogni forma di informazione e di accettare qualsiasi tipo di applicazione. Il codice sancisce il principio di neutralità nella sua dimensione

economica attraverso obblighi di trasparenza agli operatori in materia di gestione del traffico in rete e di restrizione all'accesso alla rete per assicurare una concorrenza effettiva tra le reti e tra i fornitori di servizi di comunicazione online, ma garantisce la neutralità delle reti anche nella sua dimensione sociale, attraverso misure volte a favorire il libero accesso generalizzato degli utenti finali all'informazione. L'*Autorité de régulation des communications électroniques et des postes (ARCEP)*, autorità amministrativa indipendente regolatrice, esercita poteri particolari per impedire la violazione del principio di neutralità, quali il potere di stabilire esigenze minime in termini di qualità del servizio (esercitabile non solo per internet, ma potenzialmente per tutte le reti) (*Code des Postes et des communications éléctroniques*, articoli da L36-1 a L36-13).

Per quanto riguarda la **libertà di espressione su internet** e la **tutela dei diritti d'autore dalla c.d. pirateria digitale**, la *Loi n. 2009-1311* del 28 ottobre 2009 su *Creation et internet*, entrata in vigore il primo gennaio 2010, ha dettato la disciplina della *Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet* ***(HADOPI)***, l'autorità preposta al **controllo dei comportamenti** degli utenti di Internet **lesivi del diritto d'autore**. La versione finale della legge è il risultato di un profondo intervento correttivo svolto dal *Conseil constitutionnel* sulla Legge istitutiva dell'Alta Autorità (*Loi n. 2009-669*, del 19 giugno 2009). Con la decisione del 10 giugno 2009 (*Décision* n. 2009-580 DC,) il Consiglio costituzionale ha depotenziato alcuni dei 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. Il Consiglio costituzionale ha anzi sancito una sorta di **"diritto fondamentale" all'accesso ad Internet**; contestualmente, la decisione del 2009 ha suggerito la necessità che qualsiasi sanzione sia proceduta dal vaglio di un'autorità giurisdizionale. 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".

La libertà di espressione su internet trova un limite in Francia anche nelle norme che definiscono i reati di **diffamazione** e di **ingiuria** o di **incitamento all'odio razziale o alla discriminazione** espressi mediante mezzi di comunicazione pubblica, contenute nella **Legge sulla libertà di stampa del 1881**, più volte modificata (*Loi du 29 juillet 1881 sur la liberté de la presse*). Il testo legislativo prevede un regime speciale per la sanzione dei reati commessi a mezzo stampa o mediante altri mezzi di comunicazione, tra i quali è **compreso anche "ogni mezzo di comunicazione al pubblico per via elettronica"** (art. 23).

Il diritto francese oltre a prevedere i reati di diffamazione e ingiuria (art. 29, commi 1 e 2) e di incitamento all'odio razziale o alla discriminazione (art. 24, comma 5), dà anche diverso rilievo al fatto che le dichiarazioni diffamatorie, ingiuriose o oltraggiose siano state espresse in **forma pubblica** o **privata**.

La legge sulla libertà di stampa definisce come *délits* (**reati**) la **diffamazione** e l'**ingiuria espresse in forma pubblica** e ne prevede le sanzioni penali (artt. 30-33). Qualora invece la diffamazione o l'ingiuria siano espresse in forma privata, il Codice penale le qualifica come infrazioni definite "contravvenzioni" (*contraventions*) di I classe (*Code Pénal*, art. R621-1 e art. R.621-2), punibili con un'ammenda fino a 38 euro (*Code Pénal*, art. 131-13).

L'**incitamento all'odio (per razza, genere, orientamento sessuale, handicap, etc) o alla discriminazione** (Legge sulla libertà di stampa, art. 24, comma 5) comporta pene fino ad un anno di detenzione e/o un'ammenda fino a 45.000 euro, oltre ad eventuali pene accessorie.

Le **pene** relative alla diffamazione e all'ingiuria pubblica e all'incitamento variano anche in base alla **vittima del reato** e/o alle **motivazioni** che ne sono alla base.

L'imputazione di **responsabilità penali** per gli illeciti previsti dalla legge sulla libertà di stampa commessi attraverso internet è inoltre regolata dalla **legge del 1982 sulla comunicazione audiovisiva**, da ultimo modificata nel 2009 (*Loi n. 82-652 du 29 juillet 1982 sur la communication audiovisuelle - testo in vigore*). Il provvedimento prevede una responsabilità penale principale del direttore o co-direttore di una pubblicazione elettronica se la messa online del messaggio incriminato è stata preventivamente determinata; in questo caso l'autore materiale del messaggio diffamatorio o ingiurioso sarà perseguito solo come "complice". Nel caso in cui invece la pubblicazione del messaggio incriminato non sia stata preventivamente determinata dal direttore, risulterà come "autore principale" del messaggio, e dunque perseguibile, l'autore materiale dello stesso, o in caso di sua impossibile identificazione, il produttore (*producteur*) della pubblicazione (art. 93-3).

La responsabilità del direttore (o del co-direttore) è poi esclusa "se l'illecito risulta dal contenuto di un messaggio indirizzato da un internauta ad un servizio di comunicazione online e messo a disposizione del pubblico da tale servizio in uno spazio di contributi personali identificato come tale". In tal caso deve inoltre risultare che il direttore (o il co-direttore) non era effettivamente a conoscenza del messaggio prima della sua messa online o che, appena avutane notizia, abbia provveduto prontamente a ritirarlo dalla rete.

Sempre con riferimento alle **responsabilità penali** per le dichiarazioni diffamatorie e ingiuriose pubblicate online, rileva anche la normativa riguardante in modo specifico i supporti della comunicazione via internet. A tal proposito sono da considerare in particolare gli obblighi sanciti dalla **legge sull'economia digitale del 2004** (*Loi n. 2004-575 du 21 juin 2004 sur l'économie numerique*).

La legge del 2004 stabilisce, in modo specifico, che i **gestori di piattaforme digitali** che assicurano lo stoccaggio di messaggi scritti, immagini, ecc. online, su richiesta degli utenti dei servizi di stoccaggio, in linea di principio **non** siano **responsabili** per le attività o le informazioni di carattere illecito immesse sui siti internet, nel caso in cui non siano a conoscenza del loro contenuto illecito o se, dal momento in cui essi ne abbiano avuto conoscenza, abbiano provveduto prontamente a ritirare i messaggi incriminati o a renderne impossibile l'accesso (art. 6, I, 3).

Il provvedimento dispone inoltre che i **soggetti che offrono servizi per l'accesso alla rete** e i gestori di piattaforme digitali che assicurano **lo stoccaggio di messaggi**, ecc. online "**non sono sottoposti ad un obbligo generale di controllare le informazioni** che trasmettono o memorizzano, né ad un obbligo generale di ricercare fatti o circostanze che rivelano attività illecite" (art. 6, I, 7).

Tuttavia, con riguardo ad alcune informazioni è invece loro richiesto un particolare **controllo sui messaggi** che gli internauti possono diffondere. Si tratta di comunicazioni sui seguenti temi: **apologia dei crimini contro l'umanità**, **incitamento all'odio razziale**, così come alla **pornografia infantile**, incitamento alla **violenza,** in particolare **contro le donne, offese alla dignità umana** (art. 6, I, 7).

Ai fini di un contrasto alla diffusione di tali contenuti illeciti, gli **internet host provider** e i gestori di piattaforme digitali di stoccaggio di messaggi online sono obbligati a mettere a punto un **dispositivo per la segnalazione di messaggi illeciti facilmente accessibile e visibile**. Essi hanno inoltre l'obbligo di informare le autorità competenti di ogni attività illecita di diffusione dei temi sopra richiamati da parte degli utenti dei loro servizi, che sia stata loro segnalata e di rendere pubblici i mezzi che essi dedicano alla lotta contro queste attività illegali (art. 6, I, 7). L'inosservanza di tali obblighi generali è penalmente sanzionata.

Ogni vittima di dichiarazioni diffamatorie o ingiuriose, secondo la legge sulla libertà di stampa, ha inoltre "**diritto di replica"** (*droit de réponse*)**.**

La legge del 2004 ha istituito anche uno specifico **diritto di replica applicato a internet** in base al quale ogni persona nominata o designata in un servizio di comunicazione al pubblico online dispone di un diritto di replica, con possibilità di richiedere anche la correzione della pubblicazione o del messaggio che possa indirizzare al servizio online (art. 6, IV). La richiesta di esercizio del diritto di replica è indirizzata al direttore della pubblicazione online, o in caso di persona che editi a titolo non professionale o mantenga l'anonimato, al *provider* o al *web host provider*. La richiesta di replica, che è gratuita, deve essere presentata entro il termine di 3 mesi dalla data di diffusione al pubblico del messaggio in causa. Il direttore della pubblicazione è tenuto a inserire le repliche nel servizio di comunicazione al pubblico online entro i tre giorni successivi alla ricezione di tali repliche, pena l'obbligo del pagamento di un'ammenda di 3750 euro, che non

esclude anche eventuali altre sanzioni e risarcimento dei danni ai quali il messaggio online in causa possa dare luogo (cfr. inoltre *Décret d'application* du 24 octobre 2007).

Altro limite alla libertà di espressione su internet è dato dalle misure contro il fenomeno del **"cyberbullismo"**, consistente in molestie e in intimidazioni che si manifestano per ***e-mail*** o attraverso i ***blog*** sui quali gli aggressori, spesso giovani internauti che si nascondono sotto una falsa identità, possono in particolare inviare insulti o minacce alla vittima, far circolare commenti odiosi o diffondere immagini truccate che mostrino la "vittima" in situazioni imbarazzanti i degradanti, etc.

Anche se attualmente il diritto francese **non** prevede espressamente il **reato di cyberbullismo**, l'autore di atti compiuti a tal fine è suscettibile di essere perseguito sulla base di norme del Codice Civile, del Codice penale o del Diritto di Stampa previste per reati e atti illeciti quali, ad esempio: l'ingiuria o la diffamazione pubblica (citata Legge del 29 luglio 1881, art. 32); l'incitamento all'odio o alla discriminazione per motivazioni legate alla razza, al sesso, all'orientamento sessuale o all'handicap (citata Legge del 29 luglio 1881, art. 24); la violazione del diritto all'immagine in caso di diffusione di foto o video oltraggiosi (*Code Pénal*, art. 226-1 e art. 226-2); l'usurpazione d'identità (*Code Pénal*, art. 226-4-1); la diffusione di contenuti a carattere pornografico di un minore (*Code Pénal*, art. 227-13).

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.

Con la **legge del 22 luglio 1997** (rimasta in vigore fino al 2007) recante la disciplina delle condizioni generali per i servizi di informazione e comunicazione (*Gesetz zur Regelung der Rahmenbedingungen für Informations-und Kommunikationsdienste – IuKD)* sono state introdotte nell'ordinamento tedesco alcune norme che riguardano specificamente la **responsabilità dei *provider* e degli operatori in internet**. Tali disposizioni, contenute precisamente nel **§ 5 della legge sull'utilizzo dei servizi telematici** (*Gesetz über die Nutzung von Telediensten, Teledienstegesetz - TDG*) che costituiva l'art. 1 della *IuKD*, distinguono due figure di *provider*: il fornitore di servizi e il fornitore di un accesso alla rete. Il primo, oltre a predisporre un accesso alla rete per i propri utenti, è un fornitore di informazioni – in modo diretto o tramite terzi – sulla rete stessa. Qualsiasi *provider* che predisponga pagine *web* a cui gli utenti possono accedere rientra in questa categoria e deve considerarsi responsabile sia per il materiale illecito da lui stesso creato o riprodotto e messo a disposizione per i propri utenti, sia per il materiale prodotto da altri e messo a disposizione sul suo *server*. In quest'ultimo caso, però, occorre che il *provider* sia a conoscenza della pubblicazione di materiale illecito sul suo *server*, che disponga degli strumenti tecnici per evitare l'ulteriore diffusione in rete di tale materiale e che si possa ragionevolmente attendere un suo intervento affinché la diffusione di tale materiale venga impedita. Diversa è invece la posizione della seconda figura di *provider*, che è escluso da qualsiasi forma di responsabilità per il materiale inviato da terzi, poiché è solo un fornitore di accesso alla rete al pari di un operatore telefonico.

Prima dell'approvazione della legge federale del 1997, la giurisprudenza tedesca era orientata ad applicare la disciplina della responsabilità editoriale di una testata giornalistica anche all'*internet provider*. In materia di diffamazione, ad

esempio, l'orientamento dei giudici era quello di limitare la responsabilità dell'editore, e quindi per analogia anche quella del *provider*, alle sole affermazioni dichiaratamente offensive. Nell'affrontare un caso di diffamazione online, il Tribunale distrettuale di Stoccarda sostenne l'impossibilità di riconoscere in capo al provider responsabile un obbligo di controllo di tutto il materiale inviato dai propri utenti. Secondo i giudici di Stoccarda, tale responsabilità poteva essere ammessa soltanto nel caso in cui il *provider* fosse stato a conoscenza o avesse potuto conoscere l'esistenza del materiale offensivo.

Le disposizioni contenute nella legge del 1997 riprendono in parte le affermazioni dei giudici di Stoccarda stabilendo le tre condizioni già menzionate perché possa attribuirsi una qualche responsabilità al fornitore di servizi in rete e cioè, riepilogando: che questi sia effettivamente a conoscenza (non basta quindi la mera conoscibilità) del materiale illecito; che abbia i mezzi tecnici idonei ad impedire l'ulteriore uso di tale materiale e che ci si possa ragionevolmente aspettare che tale impedimento venga messo in atto.

Dopo la sua entrata in vigore (1° agosto 1997), la legge sui servizi telematici (*Teledienstegesetz*) è stata modificata tre volte (nel 2000, nel 2001 e nel 2006) ed è stata infine abrogata e incorporata nella **nuova legge sui media telematici** (*Telemediengesetz – TMG*), contenuta nell'art. 1 della legge di unificazione di norme su determinati servzi elettronici di informazione e comunicazione (*Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste, Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz - ElGVG*) del 26 febbraio 2007, con la quale è stata recepita in Germania la **direttiva comunitaria 2000/31/CE dell'8 giugno 2000** relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno. La nuova legge, in vigore dal 1° marzo 2007 e da ultimo modificata nel maggio 2010, si applica ai c.d. *Telemedia*, definiti in senso ampio come qualsiasi servizio di informazione o di comunicazione elettronico, che non sia, da un lato, una trasmissione radiofonica o televisiva (*Rundfunk*) e, dall'altro, un servizio di telecomunicazioni (*Telekommunikationsdienst*). Nel campo di applicazione della TMG non rientrano, ad esempio, né l'*Internet Protocol TV* (IPTV), né il *Voice Over Internet Protocol* (VOIP), ma le nuove disposizioni si applicano pienamente ai siti *web*, alla posta elettronica, ai motori di ricerca, alle piattaforme di scarico della musica, ai *webshop*, ai *blog*, ai *newsgroup*, ai portali, alle *chatroom* e ai video *on demand*. Sono soggetti alla nuova disciplina tutti i prestatori di servizi telematici, compresi quelli di natura pubblica, a prescindere dal fatto che sia percepito o meno un compenso per l'utilizzo del servizio stesso.

Sostanzialmente le disposizioni contenute nella *Telemediengesetz* (§§ 7-10), pur essendo più ampie e dettagliate rispetto alla legge precedente, non mutano la **responsabilità dei *provider* dei media telematici per i contenuti di terzi**

ospitati sui propri *server* (aste online, mercati virtuali, *forum* di discussione, siti *web*, ecc.). Tale responsabilità è infatti disciplinata anche dalla normativa comunitaria in materia di commercio elettronico, che non prevede un obbligo generale di monitorare in via preventiva i contenuti pubblicati, ma solo quello di intervenire a posteriori una volta accertato il contenuto illecito. Il **§ 7, comma 1** della TMG, analogamente al § 5, comma 1 della vecchia normativa, stabilisce infatti che i fornitori di servizi (*Diensteanbieter*) sono **responsabili per le proprie informazioni da essi rese disponibili in rete secondo le leggi generali**, ovvero le norme di diritto civile e penale (ivi comprese quelle relative al reato di ingiuria e diffamazione), di diritto pubblico e, in particolare, sul diritto d'autore. In tal caso la disciplina applicabile è assimilabile a quella prevista per le pubblicazioni *off-line*. Il comma 2 dello stesso articolo precisa però che gli stessi fornitori di servizi non hanno alcun obbligo di vigilanza sulle informazioni da essi trasmesse o memorizzate, né quello di indagare sulle circostanze che indichino un'attività illecita. Resta tuttavia invariato l'obbligo di rimuovere o di bloccare l'utilizzo delle informazioni così come previsto dalle leggi generali anche nel caso di irresponsabilità dello stesso fornitore di servizi.

Rispetto alla vecchia disciplina, la legge del 2007 distingue, ai fini della responsabilità imputabile al *provider* per i materiali altrui, la fattispecie della trasmissione (*Durchleitung*) di informazioni e quella della memorizzazione (*Speicherung*) di tali informazioni sul proprio *server*. In merito al primo profilo, il § 8 stabilisce che il fornitore di servizi non è responsabile per le informazioni altrui, che egli trasmette in una rete di comunicazione o a cui dà accesso per l'utilizzo, a meno che egli stesso non abbia indotto la trasmissione, non abbia selezionato il destinatario delle informazioni trasmesse e non abbia selezionato o modificato le informazioni trasmesse. L'irresponsabilità del *provider* è espressamente esclusa qualora egli collabori intenzionalmente con l'utente del suo *server* al fine di commettere un'azione illecita. Parimenti, il § 10 dispone che il *provider* non sia responsabile per le informazioni altrui che memorizza sul suo *server*, a meno che non sia a conoscenza dell'azione o dell'informazione illecita e non agisca prontamente per rimuovere l'informazione o bloccare l'accesso ad essa non appena acquisito tale conoscenza.

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*).

Nella seduta plenaria del 18 aprile 2013 è stata presentata al *Bundestag* la **relazione finale della Commissione d'indagine su internet e la società digitale** (*Enquete-Kommission Internet und die digitale Gesellschaft*), che per tre anni, a partire dal maggio 2010, ha approfondito le problematiche connesse all'utilizzo della rete in ambito politico, economico e sociale. Il lavoro della Commissione, **costituita da 17 deputati e 17 esperti** nominati dai Gruppi parlamentari, è stato organizzato in **12 gruppi tematici** (*Projektgruppen*), ciascuno dedicato ad un aspetto particolare di internet che è stato poi oggetto di una specifica relazione: **diritto d'autore** (stampato BT n. 17/7899); **neutralità**

della rete (stampato BT n. 17/8536); **protezione dei dati e diritti della persona** (stampato BT n. 17/8999); **formazione e ricerca** (stampato BT n. 17/12029); **democrazia e Stato** (stampato BT n. 17/12290); **economia, lavoro e impatto ambientale** (stampato BT n. 17/12505); **accesso, struttura e sicurezza in rete** (stampato BT n. 17/12541); **interoperabilità, standard e software libero** (stampato BT n. 17/12495); **internet *governance* a livello nazionale e internazionale** (stampato Bt n. 17/12480); **tutela del consumatore** (stampato BT n. 17/12540); **cultura, media e pubblico** (stampato BT n. 17/12542). Complessivamente sono state svolte oltre 200 sedute che hanno coinvolto nel dialogo anche i cittadini registrati sull'apposita piattaforma di partecipazione (in totale 3.200), definiti il 18° esperto della Commissione. Negli interventi finali in Assemblea sono stati sottolineati in particolare tre ambiti nei quali il ruolo di internet è stato ritenuto fondamentale: **la politica della formazione, l'economia digitale e lo sviluppo della democrazia digitale** cui sono strettamente connessi la libertà dell'informazione e la trasparenza nei procedimenti politici. Rispetto a quest'ultimo aspetto, va evidenziata la **massima trasparenza** che è stata data ai lavori della Commissione di indagine garantendo l'accesso ad internet, la pubblicazione di tutti i documenti e la diretta delle sedute. Tra le raccomandazioni contenute nella relazione finale vi era anche la proposta di insediare una commissione parlamentare permanente sulla c.d. politica della rete (*Netzpolitik*). La proposta è stata infine accolta ed attuata nella nuova legislatura, iniziata ad ottobre 2013, con l'approvazione della **mozione** presentata da tutti i Gruppi parlamentari (CDU/CSU, SPD, Sinistra e Verdi) l'11 febbraio 2014 (stampato BT n. 18/482) per l'**istituzione della Commissione per l'Agenda digitale** (*Ausschuss Digitale Agenda*), composta da 16 deputati. A partire dalla prima seduta costitutiva del 19 febbraio 2014, la Commissione ha finora svolto 13 sedute, alcune delle quali anche pubbliche. Basandosi sugli esiti della Commissione di indagine della 17a legislatura e sui lavori svolti dalla Sottocommissione sui nuovi media istituita presso la Commissione parlamentare per la cultura, la nuova Commissione, la cui attività sarà principalmente di tipo consultivo, dovrà affrontare nell'arco della legislatura, in particolare, alcuni temi chiave come l'espansione della banda larga e la sicurezza in internet.

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 nell'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* (come recentemente modificato dal *Data Retention and Investigatory Powers Act 2014*, approvato dopo la sentenza della Corte di Giustizia UE resa nell'aprile 2014 sulla direttiva 2006/24/CE), 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*".

Per quel che concerne il profilo della cosiddetta "***net neutrality***", l'OFCOM ha recentemente riaffermato nel suo ultimo piano annuale (*OFCOM Annual Plan for 2013/14*, 28 marzo 2013, parr. 5.13-5.15, pp. 37-38) di **non rilevare particolari problematiche** in relazione alla gestione del traffico in rete degli *Internet Service Provider* (ISP). Il punto di vista dell'OFCOM sul tema della neutralità della rete era stato peraltro esposto più in dettaglio dall'Autorità medesima nel documento del 24 novembre 2011, dal titolo *Ofcom's approach to net neutrality*[7].

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.

Il particolare fenomeno del **cyber-bullismo** non è oggetto di specifiche previsioni legislative, ma rientra tra le fattispecie alle quali sono applicabili,

[7] Sul dibattito relativo alla *net neutrality* nel Regno Unito e negli Stati Uniti d'America si veda anche: C. Ijezie, *Net neutrality regulation debate in the UK and the US*.

soprattutto, le norme più generali in materia di **diffamazione** (*Defamation Act 2013*). Le disposizioni del *Defamation Act 2013* dedicate alle comunicazioni elettroniche formano una disciplina complessivamente orientata ad individuare il punto di equilibrio tra la libertà di espressione e la tutela dell'onore e della reputazione, in un ambito connotato sia dalle peculiarità tecniche degli strumenti di comunicazione elettronica, che li distinguono dai tradizionali canali informativi, sia della varietà dei ruoli assunti dagli operatori del settore, i quali – sebbene ricompresi nella generale categoria degli *Internet service providers* (ISP) - possono essere, di volta in volta, fornitori di servizi di rete (*host*), gestori di piattaforme di comunicazione (come *Facebook*) oppure motori di ricerca (come *Google*).

Le nuove regole mantengono fermo il criterio generale dell'**esonero da responsabilità dei *providers*** rispetto ai contenuti immessi dagli utenti nei canali di comunicazione elettronica (*user-generated contents*); tale esclusione della responsabilità discende, com'è noto, dal diritto comunitario, segnatamente dalle norme in materia di commercio elettronico del 2000 (direttiva 2000/31/CE), le cui disposizioni (art. 12) isolano l'attività di "semplice trasporto" (*mere conduit*) svolta dagli operatori per affrancarla dall'imputabilità di illeciti commessi da terzi attraverso i mezzi di comunicazione elettronica ricadenti nel loro controllo.

In linea di principio, la posizione del fornitore di accesso a servizi Internet, che si limita a veicolare in rete l'informazione e non incorre in responsabilità per il suo contenuto, è dunque diversa da quella del *provider* in grado di esercitare un controllo sulle risorse infomative rese accessibili al pubblico, il quale è per tale motivo assimilabile al *publisher* e soggetto alle medesime regole. La differenza dei due ruoli non è però così nitida nella prassi, poiché l'operatività dei *provider* può non esaurirsi nella prestazione di un servizio di connessione, ma configurarlo come *secondary publisher*, qualora essa comporti un certo grado di discrezionalità circa la durata e le modalità dell'accesso pubblico ad un determinato contenuto informativo pubblicato attraverso la sua piattaforma di comunicazione.

Per tale ragione, il legislatore ha perseguito l'obiettivo di un attivo coinvolgimento dei fornitori di servizi di comunicazione, i quali, anche se non tenuti ad effettuare preventivi controlli sui contenuti diffusi attraverso le loro piattaforme, nondimeno devono provvedere, nel caso della diffusione di **contenuti diffamatori** (nella forma, ad esempio, di messaggio "postato" in un *blog* oppure di *tweet* inviato od inoltrato dall'utente), alla loro **rimozione** entro un breve termine e nel quadro di una specifica procedura che prende avvio con il **reclamo** notificatogli dalla parte lesa.

Tale obbligo è posto dalle legge quale contrappeso dell'esimente generale prevista per gli *operators of websites* (*Defamation Act 2013*, art.5), i quali non sono considerati responsabili della diffusione di contenuti diffamatori effettuata per loro tramite (anche quando i messaggi di tale natura sono pubblicati da utenti

di od "ambienti" di comunicazione sottoposti a "moderazione"), se non in presenza di determinate condizioni: quando la parte lesa dimostri l'impossibilità di identificare l'autore materiale del messaggio (il quale deve invece essere individuabile, anche se anonimo, dal *provider*), di avere presentato reclamo al *provider* e di non averne ricevuto risposta entro i termini, o che lo stesso *provider* ha agito con dolo (*malice*).

La disciplina così delineata è integrata dalle regole di dettaglio introdotte dalla normativa secondaria: le *Defamation (Operators of Websites) Regulations 2013* prescrivono le operazioni che il *provider*, al fine di non incorrere nella relativa responsabilità, deve compiere una volta che venga a conoscenza di contenuti diffamatori diffusi attraverso la sua piattaforma di comunicazione.

L'organo giudiziario titolare del potere di esercizio dell'azione penale, il *Crown Prosecution Service*, ha adottato nel 2012 linee-guida per la repressione dei reati commessi mediante l'utilizzazione di reti di comunicazione (CPS, *Interim guidelines on prosecuting cases involving communications sent via social media*).

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 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.

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

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

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).

L'art. 66 della legge 9/2014 concerne la **neutralità tecnologica** e dei servizi nell'uso del demanio pubblico radioelettrico, per cui nelle bande di radiofrequenze disponibili per i servizi di comunicazione elettronica si può impiegare qualsiasi tipo di tecnologia utilizzata per i servizi di comunicazioni elettroniche in conformità al diritto dell'Unione europea. Sono possibili restrizioni proporzionate e non discriminatorie ai tipi di tecnologia di accesso wireless o rete radioelettrica utilizzati per i servizi di comunicazioni elettroniche, quando ciò sia necessario per: evitare interferenze dannose; proteggere la salute pubblica dai campi elettromagnetici; garantire la qualità tecnica del servizio; assicurare la massima condivisione delle radiofrequenze; garantire un uso efficiente dello spettro; garantire il raggiungimento di un obiettivo di interesse generale. È altresì possibile utilizzare in tale contesto qualsiasi tipo di comunicazione elettronica.

Un ulteriore aspetto da considerare concerne due fattispecie di reato: la **calunnia** (*calumnia*) e l'**ingiuria** (*injuria*), che costituiscono i "reati contro l'onore" (*delitos contra el honor*)[9], disciplinati dal libro II, titolo XI, artt. 205-216, del codice penale del 1995, e il loro collegamento con Internet.

La **calunnia**, secondo l'articolo 205 del codice, consiste nell'attribuire falsamente (o con "temerario disprezzo della verità") a qualcuno la commissione di un reato; quando ciò avviene **pubblicamente** (*con publicidad*), cioè **attraverso la stampa, la radiodiffusione o mediante un altro mezzo avente un'efficacia similare** (art. 211), il codice prevede una pena detentiva compresa tra i sei mesi e i due anni oppure, in alternativa, una sanzione pecuniaria[10] tra i 12 e i 24 mesi[11] (art. 206).

L'**ingiuria**, in base all'articolo 208 del codice, consiste in un'azione o un'espressione che lede la dignità di un'altra persona, sminuendo la sua fama o

[9] La Costituzione spagnola riconosce "il diritto alla tutela dell'onore, dell'intimità personale e familiare e della propria immagine" (art. 18, comma 1).

[10] Con il codice penale del 1995 è stato introdotto il sistema dei "giorni di multa" (*días-multa*): ogni giorno di multa può variare da un ammontare minimo di 2 a un massimo di 400 euro e l'estensione della pena può oscillare da un minimo di 10 giorni a un massimo di 2 anni; ciascun "mese" di multa si intende composto di 30 giorni e un "anno" si considera formato da 360 giorni. Spetta al giudice fissare l'importo giornaliero all'interno dei limiti indicati, tenendo conto della situazione economica del condannato, nonché determinare tempi e modi di pagamento (art. 50 del codice penale).

[11] Negli altri casi è prevista una sanzione pecuniaria da 6 a 12 mesi.

attentando alla sua considerazione; anche in tale fattispecie l'ipotesi di reato scatta allorché è evidente la falsità o la temerarietà dell'accusa e qualora, inoltre, le espressioni ingiuriose - per la loro natura, gli effetti prodotti e le circostanze - siano ritenute gravi secondo il giudizio corrente. Per l'ingiuria grave pronunciata **pubblicamente** è prevista una pena pecuniaria, per l'esattezza una multa da 6 a 14 mesi[12] (art. 209)[13].

In base all'articolo 212 del codice, è prevista anche la **responsabilità civile solidale dei proprietari dei mezzi d'informazione**, attraverso i quali è stata messa in circolazione la calunnia o l'ingiuria.

L'ampia formulazione utilizzata dall'art. 211 del codice, per cui la calunnia e l'ingiuria si considerano commesse pubblicamente quando sono diffuse attraverso la stampa, la radiodiffusione o mediante un altro mezzo avente un'efficacia similare, non lascia dubbi sul fatto che **anche Internet rientri nella fattispecie considerata**.

Quanto alla responsabilità civile, la normativa sul punto risulta integrata dalla *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio* electrónico, i cui artt. 9-17 prescrivono **gli obblighi e le responsabilità dei fornitori di servizi in rete**. In particolare l'art. 13, relativo alla responsabilità dei fornitori di servizi della società dell'informazione, riconosce che essi sono soggetti alla responsabilità civile, penale e amministrativa stabilita in via generale dall'ordinamento giuridico. L'art. 14 prevede tuttavia che gli operatori delle reti di telecomunicazione ed i *provider* di accesso a una rete di telecomunicazioni che forniscono un servizio di intermediazione, consistente nel trasmettere mediante una rete di telecomunicazioni dati forniti dal destinatario del servizio o nel consentire l'accesso alla rete, **non sono responsabili per l'informazione trasmessa**, salvo nel caso in cui essi abbiano originato la trasmissione, modificato i dati o selezionato i dati ovvero i destinatari dei dati.

[12] Negli altri casi è prevista una sanzione pecuniaria da 3 a 7 mesi.

[13] In entrambe le circostanze il reato non sussiste solo se l'accusato prova, nel caso della calunnia, il fatto oggetto delle sue affermazioni (art. 207) o, nel caso dell'ingiuria, la verità delle sue espressioni offensive rivolte a funzionari pubblici, in relazione a fatti concernenti l'esercizio delle loro funzioni o riferiti alla commissione di contravvenzioni penali o di infrazioni amministrative (art. 210).