La privacy: tra sfide alle tutele e bilanciamento dei diritti[*].

Di Elena Falletti, ricercatore in diritto privato comparato dell'Università Carlo Cattaneo - LIUC di Castellanza (VA)

Sommario: Introduzione. 2 Internet e copyright. 3. Data retention. 4. Paura, terrorismo e gestione della sicurezza. 5. Rivelazione di sé e degli altri.

1. Introduzione

Nel linguaggio colloquiale tutela della privacy e tutela della riservatezza sono considerate espressioni equivalenti e spesso vengono interscambiate, ma sotto il profilo giuridico esse indicano la protezione di beni differenti: da un lato la privacy, che mira a garantire la libertà di autodeterminazione nelle scelte di vita e dall'altro la riservatezza, che riguarda la non ingerenza di terzi nella propria sfera personale[1]. L'articolo 8 della Carta europea dei diritti fondamentali, ora avente piena efficacia giuridica con l'entrata in vigore del Trattato di Lisbona dispone al secondo comma che i dati di carattere personale riguardanti la persona devono essere trattati secondo il principio di lealtà e in base al consenso della persona interessata o in circostanze previste dalla legge. Il comma prosegue affermando che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Su questo punto in dottrina si è affermato che una violazione di tale disposto può costituire una lesione alla sfera di libertà e dignità dell'individuo ed interferire con la formazione della sua identità[2]. In ogni caso occorre osservare che è alquanto difficoltoso per ciascuna persona riuscire a seguire tutte le tracce di sé lasciate durante i percorsi della sua quotidianità: dai dati relativi all'uso delle carte di credito, alle passeggiate sui marciapiedi cittadini trapuntati di telecamere, dall'uso di chip nelle carte magnetiche del trasporto urbano all'uso di Internet. In questa occasione si cercherà di tratteggiare alcuni itinerari tematici su diritto alla realizzazione di sé e cattura dei dati personali da parte di istituzioni pubbliche o private.
Il tema della tutela della riservatezza si intreccia con altri temi di notevole importanza nella società attuale. Tra questi verranno sommariamente analizzati il rapporto tra la diffusione dell'utilizzo di Internet e la protezione dei diritti patrimoniali inerenti alla proprietà intellettuale; la gestione della minaccia terroristica con le esigenze di sicurezza, sia sotto il profilo della conservazione dei dati, sia sotto il profilo della invasione della sfera personale; la questione dalla rivelazione di sè del diritto all'oblio.

2. Internet e copyright.

Uno dei più importanti ambiti dove si svolge il dibattito sulla tutela della riservatezza dei dati personali in Internet riguarda la tutela dei diritti patrimoniali d'autore su beni digitali che possono essere scambiati in Rete. Prima di affrontare il discorso squisitamente giuridico, occorre premettere alcune considerazioni di natura sociale onde comprendere pienamente il problema e gli interessi in gioco. Una recente corrente della sociologia[3] ha osservato come il fenomeno di diffusione di massa della Rete abbia creato, nelle ultime generazioni di utenti, la categoria dei "nativi digitali", ovvero di coloro che interagiscono con le tecnologie informatiche e con Internet fin dall'infanzia. Questa categoria si contrappone a quella degli "immigrati digitali", cioè coloro che hanno subito la rivoluzione tecnologica soltanto in età adulta e quindi avrebbero una percezione di tale rivoluzione più legata alla realtà rispetto alla virtualità. Anche se il dibattito su questa teoria è ancora molto acceso, essa si può considerare quale parametro di verifica della crescente tendenza al mutamento di

* Testo della relazione, approfondita e corredata di apparato annotatorio, presentata a Venezia in occasione del I Seminario di diritto comunitario e internazionale del 27-28 marzo 2010.

1 G. Tiberi, *Riservatezza e protezione dei dati personali*, in M. Cartabia (a cura di), *I diritti in azione*, Bologna, 2007, p. 352.

2 A. Torrice, *Commento Art. 8*, in La *Carta dei diritti dell'unione europea. Casi e materiali*, Taranto, 2009, p.120.

3 J. Palfrey, U. Gasser, *Born Digital. Understanding the First Generation of Digital Natives,* New York, 2008.

approccio del godimento dei beni digitali da parte dei più giovani. Secondo alcune ricerche i nativi digitali non percepiscono lo scambio dei beni digitali[4] come illecito, ma come comportamento socialmente condiviso e quindi realizzabile senza consapevolezza della sua illegalità[5].
In tema di riservatezza dei dati personali su Internet il punto principale concerne se l'indirizzo di Internet Protocol sia da considerare un dato personale o meno. L'indirizzo di Internet Protocol è il dato numerico identificativo collegato ad una rete informatica, paragonabile al di fuori del ciberspazio ad un indirizzo stradale. Si tratta di una questione essenziale perchè se l'IP è dato personale il trattamento del medesimo deve essere sottoposto a tutte le garanzie previste dalle vigenti normative convenzionali e comunitarie, da ultima la Carta europea dei diritti fondamentali che ha assunto piena efficacia giuridica dopo l'entrata in vigore del Trattato di Lisbona. Nel dibattito internazionale dottrina e giurisprudenza sono divise. Ad esempio negli Stati Uniti, in una recente decisione della Corte federale distrettuale del Southern District of New York ha stabilito che l'Internet Protocol non è diverso dallo User Id, cioè non è una informazione sufficiente ad identificare con certezza quale sia il soggetto cui esso si riferisce[6].
La giurisprudenza comunitaria non ha ancora affrontato in modo diretto cosa sia l'Internet Protocol e se sia da considerarsi un dato personale, tuttavia è possibile rispondere affermativamente a questo dubbio con una ricostruzione interpretativa. Nella ordinanza LSG – *Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH contro Tele2 Telecommunication GmbH*[7], la Corte afferma che "*La Tele2 è un fornitore di accesso a Internet, che assegna ai propri clienti un indirizzo IP («Internet Protocol»), per lo più dinamico. Sulla base di quest'ultimo e del periodo o momento preciso in cui esso è stato assegnato, la Tele2 è in grado di identificare un cliente.* Si tratta di una visione opposta rispetto a quella adottata dalla Corte federale americana sopra citata. La medesima Corte di Giustizia, nella precedente causa *Bodil Lindqvist*[8]*,* ha affermato che "*La nozione di «dati personali» accolta nell'art. 3, n. 1, della direttiva 95/46 comprende, conformemente alla definizione che figura nell'art. 2, lett. a), di questa, «qualsiasi informazione concernente una persona fisica identificata o identificabile». Tale nozione ricomprende certamente il nome di una persona accostato al suo recapito telefonico o ad informazioni relative alla sua situazione lavorativa o ai suoi passatempo".* Se la nozione di dato personale comprende "qualsiasi informazione", e questa a sua volta comprende "il nome accostato al suo recapito telefonico" risulta alquanto complicato negare che l'indirizzo fornito dal provider all'utente per mezzo di una connessione telefonica non sia un dato personale. Posto dunque che l'Internet Protocol, che consente l'identificazione di un soggetto connesso alla Rete, sia un dato personale, occorre bilanciare il diritto fondamentale del suo titolare alla riservatezza e al corretto trattamento del dato con i diritti di altri soggetti. A questo proposito si può fare riferimento ad alcuni interessi contrapposti alla tutela della riservatezza: da un lato la tutela della proprietà intellettuale, dall'altro la tutela della sicurezza pubblica da presunte minacce terroristiche.
Sul punto, sempre la Corte di giustizia, ha invocato un bilanciamento degli interessi con la nota sentenza Promusicae, dove si afferma che "*Analogamente, per quanto riguarda gli artt. 41, 42 e 47 dell'Accordo sugli aspetti dei diritti di proprietà intellettuale attinenti al commercio (accordo TRIPs), alla luce dei quali devono essere interpretate, nella misura del possibile, le norme comunitarie che disciplinano un settore al quale si applica il detto accordo, se è vero che essi impongono la tutela effettiva della proprietà intellettuale e l'istituzione di diritti di ricorso*

4 In tema di beni digitali, B. Piola Caselli, voce "*Internet ed il diritto d'autore*", in Digesto delle discipline privatistiche. Sezione Civile. Aggiornamento II, tomo II, Torino, 2003, p. 800.
5 J. Palfrey, U. Gasser, op. cit.
6 United States District Court, Southern District of New York, 07 Civ. 2103 (LLS),Viacom v. YouTube, 1 agosto 2008, p. 13 e ss.
7 Corte di giustizia delle Comunità Europee, 19 febbraio 2009, C-557/07, ordinanza consultata su www.curia.europa.eu
8 Corte di giustizia delle Comunità Europee, 6 novembre 2003, C-101/01, sentenza consultata su www.curia.europea.eu

giurisdizionale per assicurare il rispetto di quest'ultima, essi non contengono tuttavia disposizioni che impongano di interpretare le suddette direttive nel senso che vincolano gli Stati membri ad istituire un obbligo di comunicare dati personali nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che gli Stati membri, in occasione della trasposizione di queste direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Poi, in sede di attuazione delle misure di trasposizione delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità"[9].

In Italia vi è stato un contenzioso giudiziario che ha affrontato in modo controverso la questione sulla natura dell'IP come dato personale, come nel caso "Peppermint". Molti si ricorderanno della casa discografica tedesca che aveva utilizzato un certo programma software per la raccolta degli indirizzi IP di coloro che si connettevano a reti peer to peer onde scaricare materiali anche protetti dal diritto d'autore. Dopo la raccolta di tali dati, i difensori della casa discografica si rivolgevano al Tribunale di Roma, competente per territorio, considerata la sede dei provider convenuti, ai quali veniva chiesta con provvedimento d'urgenza la disclosure dei dati personali di titolari degli indirizzi IP intercettati. Dopo un primo orientamento di accoglimento[10], la giurisprudenza di merito ha rigettato tali richieste poichè "*non può ritenersi sussistere a carico del "provider" alcun obbligo di comunicazione ed estensione dei dati anagrafici necessari all'identificazione degli autori delle suddette violazioni allorché i titolari del diritto d'autore agiscano in sede civile (anche con istanza cautelare) per la tutela dei propri interessi economici. Invero, l'applicazione del combinato disposto degli art. 156 e 156 bis l. auton. non è estensibile ai dati e informazioni che attengono alle comunicazioni "lato sensu" elettroniche, né ai dati di traffico da queste generate, visto l'espresso divieto che deriva sia dal sistema normativo interno (primario e costituzionale) sia da quello comunitario. Unica deroga ammessa è quella relativa all'uso e alla comunicazione dei dati solo per la tutela di valori di rango superiore e che attengono alla difesa della collettività ovvero alla protezione di sistemi informatici"*[11]. Anche l'Autorità Garante della Privacy ha accolto questa impostazione[12], tuttavia la questione è stata riproposta, sempre presso il Tribunale di Roma, in materia di "dati aggregati" sulla fruizione di contenuti cinematografici illeciti attraverso reti peer to

9 Corte di giustizia delle Comunità Europee, 28 gennaio 2008, C-275/06, sentenza consultata su www.curia.europa.eu

10 Trib. Roma, 18 agosto, 2006, in Riv. dir. ind. 2008, 4-5, 328, dove si afferma che: "*Il titolare di diritti d'autore ha diritto diottenere in via d'urgenza ex art. 156 bis L.d.A. dal provider in capo al quale sussiste la legittimazione passiva nel relativo procedimento l'ostensione dei dati anagrafici degli assegnatari di indirizzi IP che sulla base dei dati raccolti in Rete appaiono autori di condotte illecite attraverso piattaforme di peer to peer . L'esercizio di tale diritto non è precluso dalla vigente disciplina in materia di privacy e trattamento dei dati personali. È applicabile alla fattispecie l'art. 24 del codice Privacy che consente il trattamento dei dati personali senza il consenso dell'interessato quando sia necessario per far valere o difendere un diritto in sede giudiziaria*".

11 Trib. Roma, 14 luglio 2007, in Bancadati De Jure e pubblicata su Il Merito, 2007, 10, 22. Specifica il giudice in motivazione che "*La prevalenza sulla riservatezza, quale valore fondamentale della persona, è stata recentemente ribadita dalla Corte Costituzione con la sentenza 372/2006 in relazione alla legittimità costituzionale dell'art. 132 D.Lgs. 196/2003 ed alla possibilità di conservazione dei dati di traffico delle comunicazioni tra privati per un tempo maggiore rispetto a quello previsto dalla stessa norma, ritenendo la legittimità della norma in considerazione della necessità del contemperamento e bilanciamento del diritto alla riservatezza solo per esigenze di tutela di beni della collettività prevalenti minacciati dai gravi illeciti penali.Tutto ciò esclude, quindi, la possibilità di applicazione dell'art. 156 bis L.A. e dell'art. 24 del D.Lgs. 196/2003 al trattamento dei dati personali relativi alle comunicazioni elettroniche e telematiche tra privati per finalità connesse alla tutela dei diritti soggettivi dei privati"*.

12 Aut. protez. dati person., 28 febbraio 2008, in Banca dati De Jure e in Publica, 2008: "Il trattamento dei dati personali, relativo a soggetti ritenuti responsabili di aver scambiato file protetti dal diritto ddautore tramite reti peer - to - peer , è contrario ai principi di buona fede e trasparenza, quando la raccolta dei dati è avvenuta senza il preventivo consenso informato degli interessati".

peer[13]. Il giudice romano ha confermato l'impostazione già accolta nella precedente controversia riguardante Peppermint aggiungendo che ai sensi della disciplina sul commercio elettronico non grava sull'intermediario della comunicazione alcun generico obbligo di sorveglianza ma solo taluni obblighi c.d. di protezione accomunati dall'avere ad oggetto comportamenti di collaborazione con l'Autorità giudiziaria o amministrativa di vigilanza investite nell'accertamento delle violazioni commesse attraverso il servizio reso al fine di prevenire o reprimere tali violazioni. Ulteriormente il giudicante ha chiarito che in presenza della sola informativa ricevuta attraverso la diffida inviata dalla Fapav, Telecom non solo non avrebbe dovuto ma nemmeno avrebbe legittimamente potuto interrompere il servizio, non essendo responsabile delle informazioni trasmesse, ai sensi dell'art. 14, comma 1 [della Direttiva 2000/31/CE] ed essendo contrattualmente tenuta alla prestazione[14].
In Francia, invece si è deciso recepire con legge la policy dei "three strikes", la quale, invece di bilanciare gli interessi in modo equo, privilegia gli interessi dei pochi detentori dei diritti di proprietà intellettuale distaccando la connessione Internet. Il punto di partenza della discussa legge HADOPI (conosciuta ancche come "Dottrina Sarkozy") concerne il progetto DADVSI[15] (acronimo di Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information) che avrebbe dovuto implementare nell'ordinamento francese tanto la direttiva 2001/29/CE e del Trattato WCT del 1996. La prima versione prevedeva l'istituzione di una "Haute Autorité pour la diffusione des œuvreset la protection des droits sur internet" (l'HADOPI, appunt) incaricata di comminare le sanzioni di coloro che, avvertiti formalmente per due volte dell'illiceità della condivisione di contenuti protetti dal diritto d'autore, avessero continuato a utilizzare programmi di file sharing. Al terzo avvertimento l'Autorità HADOPI inderdice al soggetto colpito la connessione Internet per un periodo tra i 3 e i 12 mesi, a seconda della gravità della condotta. Il soggetto "disconnesso" da HADOPI deve tuttavia continuare a versare i canoni dell'abbonamento al fornitore di connettività[16]. Il primo vaglio preventivo del Conseil Constitutionnel aveva parzialmente dichiarato illegittima tale

13 G. Pontico: Fapav contro Telecom: fuori i nomi, Punto Informaitico, 10 febbraio 2010, http://punto-informatico.it/2808919/PI/News/fapav-telecom-fuori-nomi.aspx

14Tribunale di Roma, 15 aprile 2010. In dottrina si veda, G. Scorza, Gli obblighi di protezione dell'ISP: Fapav c. Telecom, in Il Quotidiano Giuridico, 19 aprile 2010, dove si osserva che *"La decisione del Tribunale di Roma del 15 aprile, liquida, tuttavia, tale questione in poche battute, semplicemente rilevando che la FAPAV non avrebbe mai trattato alcun dato personale degli utenti in quanto "le indagini commissionate da FAPAV il cui risultato è stato dedotto a prova delle violazioni commesse attraverso l'accesso ai siti web indicati" avrebbero "ad oggetto dati aggregati (numero degli accessi a ciascun opera in un determinato periodo di tempo) che non consentono l'identificazione di alcun indirizzo IP degli utenti". Gli stessi indirizzi IP usati per formare il dato aggregato" continua il Giudice nel provvedimento, sarebbero "stati resi anonimi nel procedimento mediante l'obliterazione di parte del codice". Fapav, peraltro, nel corso del procedimento – sempre stando a quanto emerge dal provvedimento – avrebbe espressamente chiarito al Giudice di non aver mai "inteso includere nella domanda la comunicazione di dati personali".*

15 A sua volta, la legge DADVSI è stata oggetto di una censura costituzionale da parte del Conseil constituionnel con sentenza del 27 luglio 2006, n. 2006-540. La sentenza è riassunta e commentata su Les Cahiers du Conseil constitutionnel, Cahier n° 21 Commentaire de la décision n° 2006-540 DC du 27 juillet 2006 consultati su http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2006-540-dc/commentaire-aux-cahiers.13167.html. Tra i molti autori francesi si segnalano in via non esaustiva: C. Castets-Renard*, La décision du 27 juillet 2006 du Conseil constitutionnel sur la loi du 1er août 2006,* Recueil Dalloz, 2006, pp. 2157 e ss.; P. Reynaud, T. Verbiest, *Adoption de la loi DADVSI et décision du Conseil constitutionnel : point de répit estival!,* Revue Lamy Droit de l'Immatériel, 2006, p. 47 e ss. L. Thoumyre, *Les faces cachées de la décision du Conseil constitutionnel sur la loi "DADVSI",* Revue Lamy Droit de l'Immatériel, 2006, p. 6 e ss.; F. Chaltiel, *Turbulences au sommet de la hiérarchie des normes. A propos de la décision du Conseil constitutionnel du 27 juillet 2006 sur la loi relative aux droits d'auteurs*, Revue du marché commun et de l'Union européenne, 2007, p. 61 e ss.

16 J. W. Kinn, N. Jondet, *A 'New Deal' for End Users? Lessons from a French Innovation in the Regulation of Interoperability*, William & Mary Law Review, Vol. 51, No. 2, p. 547, 2009, http://ssrn.com/abstract=1419750; V. L. *Bernabou, Glose de la loi favorisant la création et la protection de la création su internet (dite HADOPI) (A jour de la cénsure du Conseil Constitutionnel)*, 2009, consultato su www.juriscom.net; E. De Marco, *Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux,* 2009, consultato su www.juriscom.net.

legge perchè prevedeva uno sbilanciamento di tutela a favore dei detentori di diritti patrimoniali ed a sfavore dei diritti fondamentali, quali quello di comunicazione e informazione degli utenti nonché la garanzia di un processo equo poichè il meccanismo adottato dalla legge Hadopi comporta il ribaltamento della presunzione di innocenza. Il cittadino colpito dalla sospensione della connessione avrebbe dovuto dimostrare la propria innocenza, invece, ai sensi dell'art. 9 della *Déclaration des droits de l'homme et du citoyen* del 1789, che in Francia è fonte di importanza costituzionale, chiunque è presunto innocente fino a che non sia stato dichiarato colpevole da un'autorità giudiziaria, nè è possibile per il legislatore istituire presunzioni di colpevolezza in materia repressiva e senza il rispetto dei diritti di difesa dell'imputato[17]. La seconda stesura della legge HADOPI è stata promulgata in data 22 ottobre 2009. Il Conseil constitutionnel, nuovamente interpellato[18], ha sostanzialmente confermato la costituzionalità della nuova versione del provvedimento in quanto consente l'intervento dell'autorità giudiziaria nel procedimento sommario inerente alla contraffazione commessa attraverso un servizio telematico[19]. Ciò nonostante va rimarcato come la strategia del "three strikes" stia ottenendo risultati controversi. Secondo una indagine recentemente pubblicata da un ente di ricerca francese (si tratta dell'istituto Môle Armoricain de Recherche sur la Société de l'Information et les Usages d'INternet, M@rsouin, istituito presso l'Università di Rennes) la legge sta contribuendo all'abbandono dell'uso della tecnologia p2p nella misura del 15% da parte degli utenti, mentre crescono i download illegali del materiale protetto nella misura del 3%[20]. Tali dati tendono a dimostrare come la criminalizzazione di un protocollo di comunicazione, ovvero le reti peer to peer, abbia colpito soprattutto l'utilizzo legale della tecnologia in questione. Nella medesima indagine empirica viene evidenziato come la produzione e lo scambio di beni digitali a contenuto culturale sia diminuita nella misura del 27%, ma non abbia intaccato, piuttosto il contrario, lo scambio illegale di materiale protetto[21]. Da questi dati è possibile dedurre come la tecnologia vada trattata in quanto tale e non criminalizzata, mentre gli operatori di settore dovrebbero concentrare i loro sforzi relativamente al miglioramento ovvero al mutamento del loro modello di business, come già avvenuto in altre esperienze commerciali. Un possibile esempio di contemperamento tra gli interessi sembrerebbe essere stata la piattaforma "iTunes" che attraverso un accordo con i produttori di fonogrammi consente la vendita legale di musica online, per mezzo un apposito lettore di files in formato mp3 (iPod) a costi notevolmente più bassi di quelli abituali sul mercato fonografico[22].
Come si pongono gli altri Paesi Europei? Mentre l'Inghilterra[23] ha recentemente approvato il Digital

17 In dottrina, J. M. Bruguière, *Loi "sur la protection de la création sur internet": mais à quoi joue le Conseil constitutionnel* ?, Recueil Dalloz, 2009, p. 1170 e ss.

18 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2009/2009-590-dc/saisine-par-60-deputes.47589.html.

19 Conseil Constitutionnel, 22 octobre 2009, n. 2009 -590. In dottrina, E. Derieux, *Validation par le Conseil constitutionnel de l'essentiel des dispositions de la loi "Hadopi 2*", Revue Lamy Droit de l'Immatériel, 2009, p. 6 e ss.

20 S. Dejean, T. Pénard, R. Suire, *Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français*, marzo 2010, www.marsouin.org

21 S. Dejean, T. Pénard, R. Suire, op. cit.

22 B. Danaher, S. Dhanasobhon, M. D Smith, R. Telang, *Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy,* http://ssrn.com/abstract=1381827, 2010; M. E. K. Reder, *Case Study of Apple, Inc. for Business Law Students: How Apple's Business Model Controls Digital Content Through Legal and Technological Means,* Journal of Legal Studies Education, 2009, pp. 185 e ss.; A. Osterwalder, Y. Pigneur, *Business Model Generation*, Toronto, 2009, p. 47; U. Gasser, *iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media - A Case Study*, http://ssrn.com/abstract=556802, 2004.

23 Nel Regno Unito di Gran Bretagna la procedura di approvazione del Digital Economy Bill è stata terminata l'8-4-10 con l'apposizione del Royal Asset. Tale provvedimento legislativo ricalca le scelte francesi del modello "three strikes". Il "Digital Economy Bill [HL] 2009-10" è consultabile sul sito web: "http://services.parliament.uk/bills/2009-10/digitaleconomy.html".

Economiy Bill su ispirazione del modello "three strikes", e così l'Irlanda[24], in Spagna[25] e Germania lo hanno rigettato perchè Internet viene considerato un diritto fondamentale della persona[26]. Come orientarsi tra la protezione dei diritti di proprietà intellettuale su Internet e la tutela della riservatezza e dei dati personali? Una soluzione auspicabile potrebbe consistere nel bilanciamento in via di eccezione tra art. 17 co 2 Carta di Nizza con tutti gli altri diritti fondamentali, tra cui quella alla riservatezza previsto dall'art. 8 della medesima Carta.
In sede internazionale, però, si sta formulando un nuovo trattato: l' Anti-Counterfeiting Trade Agreement (ACTA), con la previsione di nuove fattispecie di natura penale a carico di coloro che downloadano illegalmente materiali protetti dal diritto d'autore, con il rischio, però di privilegiare i diritti patrimoniali di pochi titolari rispetto ai diritti fondamentali di tutti[27].

3. Data retention

Il problema della "Data retention" è strettamente collegato con le tematiche della sicurezza e della prevenzione degli attentati terroristici. In materia sono gli Stati Uniti, successivamente agli attentati dell'11 settembre 2001, sono stati i capofila nella ideazione e realizzazione di una policy particolarmente invasiva per quanto concerne la tutela della riservatezza, contenuta nei c.d Patriot Act[28]. In Europa la minaccia terroristica di matrice islamica sembrava meno incombente e più

24 nel caso "Emi Records e Ors. v. Eircom Ltd[2010] IECH 108 del 16 - 4 - 2010 la giurisprudenza ha accolto le ragioni dei titolari dei diritti d'autore.

25 http://www.edri.org/edrigram/number7.22/spain-no-three-strikes-law. Tuttavia, dopo la recente e minoritaria sentenza del Juzgado Mercantil di Barcellona del 11 marzo 2010, la quale afferma che il p2p non è violativo del copyright, il governo spagnolo ha dichiarato di voler inasprire la normativa in materia, R. Muñoz, Primera sentencia civil que declara legales las redes P2P de descargas, El Pais, 13 marzo 2010, http://www.elpais.com/articulo/tecnologia/Primera/sentencia/civil/declara/legales/redes/P2P/descargas/elpeputec/20100313elpeputec_2/Tes

26 La giuriprudenza costituzionale tedesca è orientata a garantire all'utente della Rete e delle tecnologie digitali il c.d. Habeas Data: BVerfG, 2 marzo 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Id., 28 febbraio 2008, 1 BvR 370/07.

27 M. Blakeney, International Proposals for the Criminal Enforcement of Intellectual Property Rights: International Concern with Counterfeiting and Piracy, 2009, SSRN: http://ssrn.com/abstract=1476964.

28Il nome esteso di questo provvedimento emanato dal legislatore americano sette settimane dopo gli attentati dell'11 settembre 2001 è Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001(Patriot Act). A. Blin, Gli Stati Uniti di fronte al terrorismo, cit., p. 444. Dottrina e giurisprudenza statunitensi ed europee hanno molto dibattuto sulla natura ecostituzionalità di queste norme così invasive nel quadro dei diritti personali, sia dei cittadini americani, sia da parte di coloro che pur non essendo cittadini sono legalmente residenti negli USA. Tuttavia va sottolineato il momento emotivo della promulgazione di questa normativa: sembrava che tutti i cittadini fossero concordi nel rinunciare ad alcune lorolibertà e tutele in cambio di maggiore sicurezza. Per la ricostruzione diquesto percorso sia sociale sia legislativo, B. A. Howell, Seven Weeks: The Making Of The Usa Patriot Act, in 72 Geo. Wash. L. Rev. 1145 (2004). In seguito, è stato elaborato un nuovo provvedimento legislativo noto come "Patriot Act II", di notevole invasività in diversi aspetti della vita privata di qualsiasi cittadino americano. Nonostante il Patriot Act sia stato al centro di molte controversie giudiziarie, al momento un nuovo provvedimento di estensione delle norme è stato approvato sia dal Senato, sia dalla House of Representatives ed è in attesa del sigillo del Presidente Obama. Sul punto è possibile consultare sulla banca dati Thomas il provvedimento medesimo denominato: "To extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011. (Enrolled as Agreed to or Passed by Both House and Senate)[H.R.3961.ENR]" (http://thomas.gov/cgi-bin/query/D?c111:6:./temp/~c1113zdHbS::). Tra i diversi provvedimenti giudiziari sull'incostituzionalità ed illegittimità del programma di sorveglianza posto in essere dalla Amministrazione di G. W. Bush si ricorda United States District Court Eastern District of Michigan Southern Division, August 17th 2006, American Civil Liberties Union and Others v. National Security Agency and Others, Case No.06-CV-10204, con nota di E. Falletti, La lotta al terrorismo e la violazione della sfera privata individuale: il caso delle intercettazioni abusive di massa, in Diritto dell'Internet, 2007, p. 50. Il principio giuridico di tale decisione è riassumibile come segue: "Il Terrorist Surveillance Program (TSP) è incostituzionale e si affida la National Security Agency dal proseguire nell'intercettare le conversazioni dei cittadini al di fuori delle garanzie riconosciute dalla Costituzione e in violazione del Foreign Intelligence Surveillance Act (FISCA), il quale riconosce ai ricorrenti e a chiunque la libertà di intrattenere conversazioni telefoniche, comunicazioni elettroniche e corrispondenza via mail. Qualora questa Corte decidesse altrimenti, l'azione presidenziale relativa alle

circoscritto a realtà locali francesi e spagnole[29], tuttavia la minaccia terroristica concretizzatisi negli attentati alla metropolitana londinese del 7 luglio 2005[30] ha provocato il rafforzamento delle misure di sorveglianza, anche in Rete con l'emanazione di una decretazione d'urgenza, nota come "Decreto Pisanu". In obbedienza al "Decreto Pisanu[31]" chiunque utilizzi Internet da servizi aperti al pubblico vede registrato il proprio nominativo per accedere alla connessione (nella convinzione che i terroristi utilizzino internet point e cyber cafè per organizzare gli attentati). Si tratta di una misura urgente e provvisoria ormai rinnovata da cinque anni[32], senza che sia chiaro cosa succeda ai dati già registrati e conservati. Sul punto la giurisprudenza ha stabilito che scaduto il termine dei sei mesi, tali dati non possono essere utilizzati all'interno di un processo penale[33].
Per quanto concerne la materia relativa all'acquisizione dei dati relativi a conversazioni telefoniche, telematiche ed elettroniche, essa è regolata da una direttiva, la 2006/24/CE, recepita nell'ordinamento italiano dal d. lgs. 30 maggio 2008, n. 109[34]. Con tali norme si è assistito ad un

registrazioni abusive violerebbe il FISA, il Primo e il Quarto Emendamento della Costituzione degli Stati Uniti rimanendo immune dall'azione giudiziaria. Non è stata certo intenzione dei Padri Fondatori assegnare al Presidente un potere senza controllo, specie quando questo potere tende a disgregare i valori chiaramente elencati nel Bill of Rights".

29 P. Migaux, Panorama della situazione dopo il 2004, in Storia del terrorismo, cit., pp. 467 e ss.

30 P. Migaux, op. cit., p. 468.

31Art. 7. Legge 31 luglio 2005, n. 155 "Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale" pubblicata nella Gazzetta Ufficiale n. 177 del 1 agosto 2005. Tale articolo è rubricato "Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet" 1. A decorrere dal quindicesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2007, chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, deve chiederne la licenza al questore. La licenza non e' richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale. 2. Per coloro che già esercitano le attività di cui al comma 1, la licenza deve essere richiesta entro sessanta giorni dalla data di entrata in vigore del presente decreto. 3. La licenza si intende rilasciata trascorsi sessanta giorni dall'inoltro della domanda. Si applicano in quanto compatibili le disposizioni dei Capi III e IV del Titolo I e del Capo II del Titolo III del testo unico delle leggi di pubblica sicurezza di cui al regio decreto 18 giugno 1931, n. 773, nonche' le disposizioni vigenti in materia di sorvegliabilità dei locali adibiti a pubblici esercizi. Restano ferme le disposizioni di cui al decreto legislativo 1° agosto 2003, n. 259, nonche' le attribuzioni degli enti locali in materia. 4. Con decreto del Ministro dell'interno di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione tecnologica, sentito il Garante per la protezione dei dati personali, da adottarsi entro quindici giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono stabilite le misure che il titolare o il gestore di un esercizio in cui si svolgono le attività di cui al comma 1, e' tenuto ad osservare per il monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati, anche in deroga a quanto previsto dal comma 1 dell'articolo 122, e dal comma 3 dell'articolo 123 del decreto legislativo 30 giugno 2003, n. 196, nonche' le misure di preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili. 5. Fatte salve le modalità di accesso ai dati previste dal codice di procedura penale e dal decreto legislativo 30 giugno 2003, n. 196, il controllo sull'osservanza del decreto di cui al comma 4 e l'accesso ai relativi dati sono effettuati dall'organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni. In dottrina, A. Genovese, Il diritto alla privacy e le disposizioni relative al traffico telefonico e telematico, in AA.VV., Terrorismo internazionale: modifiche al sistema penale e nuovi strumenti di prevenzione, a cura di Rosi e Scopelliti, in Supplemento a Dir. e giust., 2006, n. 16, p. 119 ss.; G. Melillo, Acquisizione dei dati di traffico telefonico e garanzie costituzionali: incidenti chiusi e nodi ancora irrisolti, in Cass. pen., 2007, p. 933.

32Decreto legge 30 dicembre 2009, n. 194 (il c.d. mille proroghe), Art. 3 Proroga di termini in materia di amministrazione dell'interno 1. Al comma 1 dell'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, le parole: «fino al 31 dicembre 2009» sono sostituite dalle seguenti: «fino al 31 dicembre 2010».

33 Cass., 23 ottobre 2007, n. 44576, in Bancadati De Jure, dove i giudici di legittimità confermavano un provvedimento del GIP il quale affermava che "sebbene in assenza di esplicito divieto di legge avrebbe potuto ipotizzarsi l'acquisizione anche oltre quel termine dei dati effettivamente conservati dal fornitore, una tale interpretazione estensiva della normativa - di natura eccezionale - si sarebbe posta in contrasto con la tutela della privacy".

34 relativo all"Attuazione della direttiva 2006/24/CE riguardante la conservazione dei 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" pubblicato nella Gazzetta Ufficiale n. 141 del 18 giugno 2008. In dottrina, A.

inasprimento delle condizioni di conservazione dei dati sulle conversazioni telefoniche, telematiche ed elettroniche. Nello specifico:
a) nuove definizioni di operatori, dati, utenti ex art. 1 del d.lgs 109/2008;
b) le categorie dei dati da conservare ex art. 3 del medesimo decreto legislativo per sei mesi per quanto concerne i dati con finalità commerciali e per 24 mesi per finalità giudiziarie e di polizia;
c) l'art. 4, che detta per i fornitori l'obbligo di inviare con scadenza annuale un rapporto con i dati sulle informazioni trasmesse alle autorità competenti;
d) l'art. 5, c. 2, che prevede pesanti sanzioni amministrative, contestate e applicate dal Ministero per lo sviluppo economico, per l'omessa o l'incompleta conservazione dei dati ai sensi dell'articolo 132, commi 1 e 1-bis e nel caso di assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato[35].
Sotto un profilo applicativo del d. lgs. 109/2008, il Garante della Privacy ha recentemente censurato alcune compagnie di telecomunicazioni che hanno conservato i suddetti dati per termini ancora più lunghi di quelli previsti dalla normativa comunitaria implementata dal D. Lgs. 109/2008. In particolare, il Garante ha affermato che l'art. 3 del d.lg. n. 109/2008 non include, tra le categorie di dati da conservare per le finalità di cui all'art. 132 del Codice, l'oggetto dei messaggi di posta elettronica; e che, d'altra parte, trattasi di dato potenzialmente correlato al contenuto della comunicazione di cui il predetto articolo 132 vieta la conservazione[36]". Per la medesima ragione è vietata la conservazione dell'indirizzo IP di destinazione poiché "nel rispetto dei principi di necessità nel trattamento e proporzionalità dei dati, i fornitori di un servizio di comunicazione elettronica (nel caso specifico, l'accesso alla Rete) devono conservare soltanto i dati di traffico telematico necessariamente correlati alle attività tecniche strumentali alla resa del servizio offerto e alla sua eventuale fatturazione (artt. 3, 11 e 123 del Codice)"[37] e che l'art. 3 del d.lg. n. 109/2008 non include, tra le categorie di dati da conservare per le finalità di cui all'art. 132 del Codice, l'indirizzo IP di destinazione[38].
Per quanto concerne le censure di legittimità subite dalla Direttiva 2006/24/CE si può osservare che le osservazioni di natura giurisprudenziale sono opposte. Da un lato, sotto il profilo comunitario, con la sentenza della Corte di Giustizia Irlanda contro Commissione e Parlamento, i giudici del Lussemburgo hanno difeso l'impianto normativo che giustifica la conservazione dei dati personali per un periodo che può variare dai sei mesi ai due anni, dall'altro tale impianto normativo è stato sottoposto a dure critiche da una giurisprudenza costituzionale di grande prestigio, come quella di Karlsruhe, con una importante pronuncia del Bundesverfassungsgericht del 2 marzo 2010. La Corte di giustizia afferma che "Più precisamente le disposizioni della direttiva 2006/24 sono dirette al ravvicinamento delle legislazioni nazionali concernenti l'obbligo di conservazione dei dati (art. 3), le categorie di dati da conservare (art. 5), i periodi di conservazione dei dati (art. 6), la protezione e la sicurezza dei dati (art. 7) nonché le condizioni di immagazzinamento di questi ultimi (art. 8)"[39]. Al contrario, le misure previste dalla direttiva 2006/24 non implicano, di per se stesse, un intervento repressivo delle autorità degli Stati membri. Infatti, "è previsto che i fornitori di servizi debbano

Stracuzzi, Data Retention: il faticoso percorso dell'art 132 Codice Privacy nella disciplina della conservazione dei dati di traffico, Dir.Informazione e dell'informatica N. 4-5/2008,

35 M(anlio), C(ammarata), Dati del traffico: i nuovi tempi di conservazione, in www.interlex.com del 17 settembre 2008. Questa dottrina correttamente rileva la confusione tra i diversi operatori istituzionali e si chiede: *"Come si vede, il massimo della confusione possibile, con norme e sanzioni che si incrociano tra loro (che c'entra il Ministero per lo sviluppo economico con la prevenzione e repressione dei reati?)"*.

36 Autorità Garante per la protezione dei dati personali, 19 novembre 2009, in www.garanteprivacy.it. In questa circostanza l'operatore delle telecomunicazioni sanzionato conservava dati relativi a comunicazioni tra gli utenti a partire dal 1999.

37 Autorità Garante per la protezione dei dati personali, 19 novembre 2009, in www.garanteprivacy.it

38 "d'altra parte, trattasi di dato potenzialmente correlato al contenuto della comunicazione di cui il predetto articolo 132 vieta la conservazione" (Autorità Garante per la protezione dei dati personali, 19 novembre 2009, cit.).

39 Corte di Giustizia delle Comunità europee del 10 febbraio 2009, causa C-301/06 Irlanda contro Parlamento e Consiglio.

conservare solo i dati generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati. Tali dati sono unicamente quelli strettamente collegati all'esercizio dell'attività commerciale dei fornitori stessi. La direttiva 2006/24 disciplina quindi operazioni che sono indipendenti dall'attuazione di qualsiasi eventuale azione di cooperazione di polizia e giudiziaria in materia penale. Essa non armonizza né la questione dell'accesso ai dati da parte delle autorità nazionali competenti in materia di repressione, né quella relativa al ricorso ai medesimi ed al loro scambio fra le autorità in parola"[40].

Si tratterebbe, quindi, di una attività meramente organizzativa dello stoccaggio dei dati raccolti e questa attività non sarebbe sottoponibile alle norme sulla privacy, come l'art. 8 CEDU, poichè i dati non inerirebbero condizioni personali e informazioni individuali. Per tali ragioni la Corte rigetta l'istanza irlandese, mentre alla dottrina permangono dubbi sul corretto bilanciamento tra esigenze della sicurezza e i limiti alla privacy[41], infatti nella ricostruzione della Corte, viene sottolineata la scelta a favore dell'adozione di atti normativi comunitari nell'elaborazione delle politiche europee anti-terrorismo, senza però vagliare la possibile violazione di diritti fondamentali conseguenti a tale scelta[42].

Invece il Bundesverfassungsgericht tedesco, con la citata decisione del 2 marzo 2010[43] accoglie le istanze di incostituzionalità della *Telekommunikationgesetz*, in particolare gli §§113a e 113b, sulla conservazione dei dati, che recepiscono le norme comunitarie e, di riflesso, pone in discussione la stessa normativa comunitaria[44]. I giudici di Karlsruhe affermano che così come impostata la TKG viola l'art. 10.1 GG, il quale afferma che la riservatezza della corrispondenza, delle comunicazioni telefoniche e postali è inviolabile. Seppure i dati conservati non ineriscano al contenuto delle conversazioni, è possibile giungere alla rete di rapporti tra le persone attraverso la mappatura delle medesime e ciò consente di insinuarsi nella sfera privata delle persone, ricostruire il loro profilo, tracciare i loro movimenti[45]. Inoltre, questa raccolta collettiva è organizzata senza uno scopo preciso, presumendo una pericolosità dei soggetti ad essa sottoposti che in realtà non è dimostrata. Non va trascurato che la raccolta di tali dati non è effettuata direttamente dallo stato, ma da soggetti privati terzi fornitori del servizio di comunicazione. La raccolta dei dati come è organizzata dalla TKG non è giustificata neanche il profilo del principio di proporzionalità, in quanto essa prevede la suddetta raccolta nei confronti di tutti gli utenti delle telecomunicazioni senza dimostrazione che essa sia fondata su specifici ovvero seri fatti rilevanti sotto il profilo penale. I requisiti che giustificherebbero una tale raccolta nei confronti di una persona sarebbero dovuti da prove concrete che dimostrino la messa in pericolo della vita, dell'integrità fisica o della libertà di una persona ovvero del pericolo di un attentato contro l'esistenza o la sicurezza del governo federale o statale. Tale decisione riprende i concetti già manifestati dal Bundesverfassungsgericht con la nota sentenza del 27 febbraio 2008[46], la quale afferma riconosce l'esistenza di un principio relativo al c.d. "*habeas data*", ovvero che ciascun fruitore delle tecnologie telematiche ha diritto alla propria libertà digitale in quanto espressione di una personalità digitale[47] e quindi anche di un domicilio digitale dove si

40 Corte di Giustizia delle Comunità europee del 10 febbraio 2009, causa C-301/06 Irlanda contro Parlamento e Consiglio.

41F. Fabbrini, Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio, in Quaderni costituzionali, 2009, p. 419.

42 F. Fabbrini, op. cit.

43 Bundesverfassungsgericht, 2 marzo 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

44 I paragrafi §§113a e 113b della TKG (Telekommunikationgesetz) erano già stati oggetto di una pronuncia del Bundesverfassungsgericht dell'11 marzo 2008, - 1 BvR 256/08 -, che però aveva consentito la comunicazione dei dati da parte dei provider dei servizi di telecomunicazione su richiesta delle autorità investigative.

45 In tema di anonimizzazione e incrocio dei dati personali raccolti, si veda P. Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 2009, http://ssrn.com/abstract=1450006.

46 cause 1 BvR 370/07 e 1 BvR 595 consultabile sul sito Internet www.bundeverfassungsgericht.de

47 Ne consegue quindi che possono venire effettuate intercettazioni telematiche solo in casi di estrema gravità concernenti la vita, l'integrità fisica e la libertà delle persone ovvero la sicurezza nazionale. Il caso era giunto di fronte ai giudici costituzionali tedeschi a seguito della previsioni nella costituzione del Land Nord Rhein Westphalen

racchiudono le comunicazioni digitali, siano esse raccolte in una casella di posta webmail o il laptop di uso quotidiano. Questa sentenza ha avuto una vasta eco[48] sui mezzi di comunicazione sia tedeschi sia europei ed è fonte di vivace dibattito politico nella coalizione giallo-nera tra i liberali del *Vizekanzler*, Guido Westerwelle, da sempre contrario alla TKG, e la *Kanzlerin* democristiana Angela Merkel grande sostenitrice della legge censurata[49]. Si attendono quindi gli sviluppi politici e legislativi dopo la forte presa di posizione del BVerfG sul tema, considerando che pochi i mesi prima della pronuncia del BVerfG il gruppo "Article 29 Data Protection Working Party - Working Party on Police and Justice", formato dai Garanti europei della privacy, ha stilato un documento per rispondere alla consultazione pubblica[50] aperta dalla Commissione europea sul futuro della protezione dei dati personali[51]. Il gruppo di lavoro dei Garanti europei della privacy ha affermato la validità dell'impianto normativo stabilito tanto dalla direttiva 95/46/CE quanto dalla direttiva 2002/58/CE (criticata così aspramente dal BVerfG), invocando tuttavia un coordinamento con le innovazioni apportate dall'entrata in vigore del Trattato di Lisbona. Tra queste, come è noto, va ricordata l'attribuzione di forza giuridica vincolante alla Carte europea dei diritti fondamentali che all'art. 8 riconosce quale diritto fondamentale la tutela della riservatezza dei dati personali. In questo senso occorrerebbe la previsione di strumenti effettivi di tutela a favore dei cittadini, anche attraverso innovazioni di natura processuale quali l'introduzione di class action o favorendo il ricorso di sistemi alternativi di risoluzione delle controversie. Altresì viene caldeggiata l'introduzione di un obbligo giuridico a carico di chi tratta di dati personali di dimostrare di aver adottato tutte le misure previste dalla legge affinchè la protezione dei dati diventi un elemento portante attorno al quale costituire l' organizzazione interna favorendo un approccio comunemente definito di "privacy by design"[52].

---

della possibilità di inserire all'insaputa dell'utente dei programmi software (i c.d. “trojan di Stato”) che tracciassero i percorsi effettuati dagli individui attraverso Internet e il computer.

48Karlsruhe kippt deutsche Regelung, 2.3.2010, http://www.sueddeutsche.de/politik/561/504770/text/; "Eine richtige Klatsche", 2.3.2010, http://www.sueddeutsche.de/politik/554/504763/text/; J. von Altenbockum, Die Richtlinie, nach der sich nicht alle richten, 4.3.2010, http://www.faz.net/s/Rub99C3EECA60D84C08AD6B3E60C4EA807F/Doc~E6B113022D0F44026893C9957DE18371E~ATpl~Ecommon~Scontent.html; German court orders stored telecoms data deletion, 2.3.2010, http://news.bbc.co.uk/2/hi/8545772.stm; H. Mahony, German court strikes blow against EU data-retention regime, 3.3.2010, http://euobserver.com/9/29595.

49A questo proposito ha provocato molta preoccupazione in Germania la creazione di una banca dati, nota come ELENA (acronimo di Elektronischer Entgeltnachweis, traducibile come "documentazione elettronica del reddito"). Si tratterebbe di una gigantesca raccolta pubblica di dati fiscali e reddituali creata al fine di combattere l'evasione fiscale nonché redistribuire su parametri oggettivi il reddito, tuttavia ELENA dovrebbe immagazzinare altre informazioni delicate quali la partecipazione a scioperi ovvero l'iscrizione a sindacati, tali informazioni dovrebbero essere rese disponibili direttamente dai datori di lavoro. Il progetto è stato pensato dal Governo Schroeder nel 2002 ed è da sempre stato molto avversato dai lavoratori nonché dai grandi giornali d'opinione come Die Zeit (G. Lütge, Elena, das Datenmonster, Die Zeit, 18.3.2010, in www.zeit.de) ovvero Suddeutsche Zeitung (S. Braun, G. Bohsem, Datenschutz-Check für "Elena", Sueddeutsche Zeitung, 2.1.2010). Anche se il controllo sociale in Germania è assai forte e presente, è tuttora molto vivo nella memoria collettiva tedesca il ricordo delle delazioni naziste a favore della Gestapo (P. Ayçoberry, La società tedesca sotto il Terzo Reich, Torino, 2005, p. 40) ovvero comuniste nella defunta DDR a favore della Stasi, come ben illustrato anche dalla cinematografia recente (Das Leben der Anderen, (Le vite degli altri), di Florian Henckel von Donnersmarck, Germania, 2006) che ispirano le illustrate resistenze. Tuttavia, l'intero progetto è stato messo in discussione dalla citata sentenza del BVerfG del 2 marzo 2010.

50 Il 9 luglio 2009 la Commissione ha lanciato una consultazione pubblica sul quadro normativo in vigore relativamente alla protezione della riservatezza dei dati personali come diritto fondamentale: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

51

52Article 29 Data Protection Working Party - Working Party on Police and Justice , The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN WP 168, consultabile su http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf. Per una sintesi e discussione del documento: http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=1794

4. Paura, terrorismo e gestione della sicurezza

La ricorrente minaccia terroristica[53] ha provocato nel mondo un generale inasprimento delle misure di sicurezza a scapito delle libertà personali dei singoli. Tra queste ad essere maggiormente compressa è la privacy. La paura[54] di tali attentati terroristici di matrice fondamentalista e dei loro effetti destabilizzanti, ha provocato un costante aumento di irrazionalità emotiva sull'opinione pubblica, che tende quindi ad accettare la tesi del Clash of Civilization[55] rispetto ad un tentativo di integrazione e reciproca tolleranza tra visioni del mondo differenti. Tale situazione ha contribuito a causare, in un certo senso, il ribaltamento del presunzione di innocenza. Quando si sostiene che l'altro, essendo diverso per tradizioni, culture, colore della pelle, potrebbe essere un potenziale nemico, di buon grado si accettano limitazioni alla sfera privata collettiva ed individuale. In realtà a vedersi limitati ed invasi nella propria sfera intima sono gli impauriti. Gli effetti concreti di queste policy sono tanto assurdi quanto sconfortanti. Ad esempio: quando ci si appresta ad un viaggio aereo si viene sottoposti a controlli e perquisizioni sempre più invasivi. Appena superati i rigorosi controlli di sicurezza alla ricerca di armi o esplosivi sul corpo e sugli effetti personali, si giunge nello spazio commerciale dei terminal dove si possono acquistare liberamente nei duty free i materiali pericolosi necessari per far le bombe con i cosmetici o con gli alcoolici sostituendo quelli già intercettati dalla security. Proprio per aumentare la sicurezza dei voli, dopo l'ultimo attentato di

53 Essa si è fatta più intensa dopo gli attentati al World Trade Center di New York dell'11 settembre 2001, provocando la morte di circa 3000 persone e dando il via ad una serie di misure restrittive della libertà personale, tanto negli Stati Uniti quanto nel resto del mondo. Tra tutti si ricorda l'emanazione del Patriot Act limitativo della libertà e segretezza della corrispondenza. La spirale violenta provocata dalle conseguenti guerre ed invasioni in Afghanistan e Iraq ha a sua volta causato ulteriore instabilità sia nei Paesi dove è presente una agguerrita componente islamica wahabita che ha organizzato attentati come quelli di Bali (2002), di Sharm el Sheikh (2005), Mumbai (2006- 2008) , sia nei Paesi europei dove è forte la presenza di immigrati di che a tale setta islamica si ispirano come a Madrid (2004) e Londra (2005). Anche in Europa si è fatta forte la presenza di norme che privilegiano la sicurezza rispetto alla tutela della privacy, come ha rilevato la stessa Corte di Giustizia nella causa Irlanda contro Parlamento e Consiglio, C- 301/06 del 10 febbraio 2009. Le principali normative sul tema sono: COUNCIL DECISION 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences; COUNCIL REGULATION (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union; DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; COUNCIL FRAMEWORK DECISION of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States; COUNCIL FRAMEWORK DECISION of 13 June 2002 on joint investigation teams; COUNCIL FRAMEWORK DECISION 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence; COUNCIL FRAMEWORK DECISION of 13 June 2002 on combating terrorism (2002/475/JHA), COUNCIL DECISION of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA); COUNCIL DECISION of 28 November 2002 establishing a mechanism for evaluating the legal systems and their implementation at national level in the fight against terrorism (2002/996/JHA). In dottrina, E. Gross, The Struggle of a Democracy Against Terrorism - Protection of Human Rights: The Right to Privacy Versus the National Interest - The Proper Balance, Cornell International Law Journal, 2004, pp. 28-93; F. Bignami, European versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining, 2007, http://ssrn.com/abstract=955024; F. Fabbrini, Silent enim leges inter arma? La Corte Suprema degli Stati Uniti e la Corte di Giustizia Europea nella lotta al terrorismo, Riv. trim. dir. pubbl. 2009, p. 591. In lingua italiana si segnala la raccolta di saggi a cura di G. Chaliand e A. Blin, Storia del Terrorismo. Dall'antichità ad Al Quaeda, Torino, 2007, in particolare i contributi di A. Blin, Gli Stati Uniti di fronte al terrorismo, p. 423 e di R. Gunaratna, Il nuovo volto di Al Quaeda: la minaccia del terrorismo islamista dopo l'11 settembre, p. 446.

54 Sul tema dell'ossessione della paura, si rimanda a L. Svendsen, Filosofia della paura. Come, quando è perchè la sicurezza è diventata nemica della libertà, Roma, 2010.

55 Si ricorda sul punto il notissimo testo di S. P. Huntington, The Clash of Civilizations and the remaking of world order, New York, 1996 e l'accesa polemica che ne seguì, tra cui si segnala: E. .W. Said, The Clash of Ignorance, The Nation, 2001, issue October 22. In questo dibattito vi è anche chi sostiene che in realtà sono gli estremismi delle più importanti religioni che provocano l'instabilità dell'equilibrio internazionale: D. Zeidan, The Resurgence of Religion, Leiden - Boston, 2003. Per una analisi più specifica sui concetti illusori di "identità" e "appartenenza culturale", F. Remotti, L'ossessione identitaria, Roma - Bari, 2010.

Natale[56], quando un maldestro terrorista tentò di far saltare l'aereo in fase di atterraggio sulla tratta Amsterdam Detroit fallendo l'innesto dell'esplosivo contenuto nella biancheria, è stata predisposta l'introduzione dei c.d. body scanner. Questi sono "*Whole Body Imaging (WBI) technologies, including backscatter x- ray and millimeter wave devices, to detect threat objects carried on persons entering airport sterile areas. WBI creates an image of the full body, showing the surface of the skin and revealing objects that are on the body, not in the body*"[57].
Questa tecnologica, in fase di studi avanzati anche per altri usi[58], se imposta in questo contesto può porre dubbi e problemi soprattutto in tema di privacy e di tutela della salute. Ci si può chiedere fino a quanto siano invasivi, se le immagini vengono registrate, oppure no - come sembra essere stato assicurato - se esse possono venire comunque intercettate ai fini di registrazione, quanto tempo tali dati sono conservati, chi può accedere ai medesimi. In tema di salute, si pongono questioni in tema di conseguenze a seguito delle esposizione delle onde, sia per i passeggeri, sia per gli operatori, quali qualifiche anche professionali devono avere gli operatori che interagiscono con questi scanner. Per quanto riguarda i passeggeri, quali conseguenze per chi non voglia accedervi per motivi di salute? occorre munirsi di certificato medico? e le donne incinte? Vi possono essere altri motivi per cui un soggetto non voglia sottoporsi alla scannerizzazione: per il rispetto del proprio pudore, per esempio, oppure per ragioni religiose. Ad esempio, è successo che una donna mussulmana all'aeroporto di Manchester abbia rifiutato di sottoporsi alla pratica perchè temeva di vedere esposto il proprio corpo e sia stata lasciata a terra[59]. Quale è il giusto bilanciamento tra i timori collettivi e i diritti dei singoli? A questo proposito è da segnalare che proprio negli Stati Uniti, che per primi hanno implementato l'uso dei body scanner negli aeroporti, è stata depositata una petition presso il Departmen Homeland Security (DSA) per interdire l'utilizzo di body scanner negli aeroporti poiché violativi della Costituzione degli Stati Uniti, del Religious Freedom Restoration Act ("RFRA"), del Privacy Act of 1974 ("Privacy Act") nonché del Administrative Procedures Act ("APA")[60].
Anche la libertà di movimento è fortemente inficiata dalla paura del terrorismo: questa rischia di tacciare ogni pretesa di privacy quando, per esempio, si cammina per strade sotto occhi automatizzati, si utilizzano biglietti magnetici in grado di ricostruire i percorsi effettuati in metropolitana o sui bus (come succede per esempio a Londra, una delle città maggiormente pervase dalla paura di minacce alla sicurezza, dove il chip della Oyster card memorizza tutti i passaggi sui mezzi di trasporto). Di fronte a questa incessante raccolta dati sembrano quasi ingenue le resistenze delle autorità europee a consegnare gli elenchi dei passeggeri in volo negli Stati Uniti[61]: da un lato questi hanno adottato il sistema elettronico di richiesta preventiva del visto ESTA (Electronic System for Travel Authorization), dall'altro appena scesi dall'aereo non si può far nulla se non si è muniti di carta di credito, cioè di uno strumento che consente di risalire, attraverso i pagamenti, alla mappatura esatta dei luoghi visitati dal viaggiatore straniero.
Nel 1941 nel suo discorso sullo stato dell'Unione il presidente americano Franklin Delano Roosvelt enunciò la famosa dottrina delle quattro libertà: la libertà di parola e di espressione, la libertà di culto, la libertà dal bisogno e la libertà dalla paura[62]. I provvedimenti analizzati in questo breve

56 Fallito attentato su volo per Detroit. Il terrorista: «Addestrato da Al Qaeda» in www.corriere.it, 26 dicembre 2009

57 Privacy Impact Assessment for TSA Whole Body Imaging, October 17, 2008 consultabile su http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf

58 Tra cui scopi diagnostici ovvero industriali: http://www.bodyscan.human.cornell.edu/scene0037.html

59 W. Pavia, Muslim woman refuses body scan at airport, http://www.timesonline.co.uk/tol/news/uk/article7048576.ece, March, 3rd 2010.

60 J. Cohen, Civil rights groups seek suspension of airport full body scanners, http://jurist.law.pitt.edu/, April 22 2010.

61 Corte di giustizia delle Comunità europee, 30 maggio 2006, Parlamento Europeo contro Consiglio dell'Unione Europea, (C-317/04) e Commissione delle Comunità Europee (C-318/04), cause riunite, in dottrina: A. Mantelero, Note minime in margine alla pronuncia della Corte di giustizia delle Comunità europee sul trasferimento dei dati personali dei passeggeri dei vettori aerei verso gli Stati Uniti, Contratto e impresa / Europa 2006 p.1075-1081

62 "*In the future days which we seek to make secure, we look forward to a world founded upon four essential human freedoms. The first is freedom of speech and expression --everywhere in the world. The second is freedom of every person to worship God in his own way-- everywhere in the world. The third is freedom from want, which, translated*

excursus sembrano invece andare nel senso opposto da quanto auspicato da F. D. Roosevelt. Anche se tali auspici sono stati fatti propri da Barack Obama nel suo discorso di insediamento[63] al momento non si notano significativi miglioramenti nella tutela della riservatezza, unico presupposto che possa concretamente realizzare la sussistenza e la coesistenza delle Four Freedoms.

5. Rivelazione di sé e degli altri

Il tema è uno tra i più complessi e in divenire di tutta l'area giuridica. Esso riguarda da un lato l'invasività della sfera di interesse pubblico su quella privata, dall'altro l'uso non appropriato delle tecnologie, siano esse "nuove" o "nuovissime".

Anche in questo ultimo caso Internet può fornire degli esempi. Quale primo esempio si può ricordare l'uso non prudente dei c.d. social network. Il caso deciso dalla giurisprudenza di merito lombarda[64] riguarda due adolescenti che, contattatisi su Facebook[65] e conosciutisi successivamente hanno intrapreso una "relazione sentimentale" conclusasi poco dopo. Nonostante l'interruzione del loro rapporto, i due ragazzi continuarono a frequentarsi attraverso il social network comunicando attraverso amici in comune. In una delle comunicazioni l'ex boy friend scrisse un messaggio greve alla ragazza dove la offendeva per un suo difetto visivo (una esotropia congenita che la giovane, vergognandosi, era solita a celare con una frangia) nonché facendo espliciti riferimenti denigratori rispetto ai gusti sessuali della medesima. Il ragazzo tentò di difendersi in giudizio da tali accuse affermando che non vi era prova della riconducibilità a sé del messaggio denigratorio né che l'ex amica del cuore fosse la destinataria del medesimo, mentre in via subordinata chiedeva l'applicazione dell'esimente ex art. 599, co.2, c.p. in combinato disposto con l'art. 1227 c.c. in quanto la ragazza avrebbe assunto un comportamento persecutorio nei suoi confronti a seguito dell'interruzione del rapporto amoroso. Nell'accogliere tutte le pretese di parte attrice, il giudice riconosce *"il carattere pubblico delle offese arrecate: offese certamente riconducibili in modo immediato e diretto (al convenuto), non solo per la riferita forzata condivisione con i comuni*

into world terms, means economic understandings which will secure to every nation a healthy peacetime life for its inhabitants --everywhere in the world. The fourth is freedom from fear, which, translated into world terms, means a world-wide reduction of armaments to such a point and in such a thorough fashion that no nation will be in a position to commit an act of physical aggression against any neighbor --anywhere in the wold. That is no vision of a distant millennium. It is a definite basis for a kind of world attainable in our own time and generation. That kind of world is the very antithesis of the so-called "new order" of tyranny which the dictators seek to create with the crash of a bomb", F. D. Roosevelt, The Four Freedoms, Washington, 6 gennaio 1941, in B. MacArthur, (ed.),The Penguin Book of Twentieth Century Speeches, London, 1999. In dottrina P. Costa, Dai diritti del cittadino ai diritti dell'uomo: alle origini della Dichiarazione Onu del 1948, in T. Mazzarese, P. Parolari (a cura di), Diritti fondamentali e nuove sfide, Torino, 2010, p. 21; T. Hoopes, D. Brinkley, FDR and the Creation of UN, New Haven, London, 1997.

63 *"As for our common defense, we reject as false the choice between our safety and our ideals. Our Founding Fathers (...) faced with perils that we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man -- a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience sake"*, B. H. Obama, Inaugural Address, Washington, 20 gennaio 2009, http://www.whitehouse.gov/blog/inaugural-address/. M. R. Shulman, The 'War on Terror' is Over - Now What?: Restoring the Four Freeomds as a Foundation for Peace and Security, 2010, SSRN: http://ssrn.com/abstract=1333146.

64 Trib. Monza, 2 marzo 2010, in Il Quotidiano Giuridico del 2 aprile 2010

65 Come è noto Facebook permette a chiunque sia di età superiore ai dodici anni di iscriversi gratuitamente creando un "profilo" al fine di mantenere i contatti con i propri "amici" in modo trasversale. Detti profili contengono fotografie, liste di interessi personali, nonché accordano l'utilizzo della bacheca propria o degli altri utenti, chat e messaggistica per scambiare comunicazioni con gli "amici" autorizzati ad accedere al profilo secondo il livello di privacy e di pubblicità dei contenuti deciso da ciascun utente. I contenuti inseriti sul sito fuoriescono dalla disponibilità dei loro autori attraverso un procedimento di "tagging", o "taggare", che realizza una rete di contatti tra i materiali, il loro autore e la rete di amici Facebook. Tale attività crea il senso stesso del social network e consente ai materiali di sopravvivere in Rete anche dopo la loro eventuale cancellazione dal social network da parte dei loro autori. In dottrina, G. Hull, H. Richter Lipford, C. Latulipe, Contextual Gaps: Privacy Issues on Facebook, 2009, SSRN: http://ssrn.com/abstract=1427546; C. Peterson, Losing Face: An Environmental Analysis of Privacy on Facebook, 2010, SSRN: http://ssrn.com/abstract=1550211; J. Hendry, K. E. Goodall, Facebook and the Commercialisation of Personal Information: Some Questions of Provider-to-User Privacy, 2010, SSRN: http://ssrn.com/abstract=1550821.

"amici Facebook" delle abitudini di vita dell'attrice e dei suoi asseriti comportamenti vessatori (...), ma anche più semplicemente per la evidente circostanza che il messaggio ingiurioso è immediatamente successivo a quello inviato dalla stessa (attrice) a commento della foto pubblicata dal comune "amico Facebook" G. F. (il quale, poi, a detta dello stesso convenuto ebbe a "cancellare" il messaggio de quo"). Per quanto concerne il risarcimento del danno non patrimoniale, il riconoscimento si fonda sul fatto che la fattispecie in esame costituisce reato: il giudice valuta se detta fattispece integri l'ingiuria ovvero la diffamazione ex art. 595 *"alla luce del cennato carattere pubblico del contesto che ebbe ad ospitare il messaggio de quo, della sua conoscenza da parte di più persone e della possibile sua incontrollata diffusione a seguito di tagging*", senza possibilità di eventuali esimenti. Ne consegue quindi che, alla luce del combinato disposto degli artt. 2059 c.c. e 185 c.p., "*l'evidente lesione di diritti e valori costituzionalmente garantiti (la reputazione, l'onore e il decoro della vittima) delle conseguenti indubbie sofferenze inferti all'attrice dalla vicenda della quale si discute"*, giustifica la condanna in via equitativa alla liquidazione del danno morale ovvero non patrimoniale nella somma di 15.000,00€.

Un altro caso, internazionalmente noto che ha visto contrapposti l'associazione che tutela i diritti dei disabili, Vividown contro Google per la diffusione di un video contenente atti di cyberbullismo. Il Tribunale di Milano ha condannato a 6 mesi di reclusione alcuni importanti dirigenti di Google con la condizionale[66]. Il fatto può essere riassunto come segue: nell'autunno 2006 veniva caricato su Google Video un video realizzato con un device elettronico che illustrava un ragazzo oggetto di denigrazione da parte dei suoi compagni di scuola. Il video è rimasto alla visione del pubblico così a lungo da rientrare nella classifica dei cento filmati più divertenti raggiungendo il 29° posto[67]. Oltre allo sdegno dell'opinione pubblica tale fatto ha provocato l'interesse della magistratura inquirente che ha formulato il rinvio a giudizio di alcuni dirigenti della società americana per due capi di imputazione: il primo relativo all'integrazione di una fattispecie di diffamazione per violazione degli artt. 110, 40, 595, commi 1 e 3, dalla quale gli imputati sono stati assolti poichè al momento tale fattispecie non è prevista quale reato penale, mentre il secondo relativo alla violazione del codice della privacy (D. Lgs. 30 giugno 2003, n. 196)[68].

Nella sua lunghissima motivazione, il giudice monocratico di prime cure ha ricostruito sia la serie di comunicazioni avvenute tra gli operatori di Google sulla cancellazione del video, nonché attraverso questa di dimostrare come i gestori del website cercassero di guadagnare delle posizioni sul mercato del video-sharing trascurando gli adempimenti di legge in materia di privacy. A questo proposito, scrive il giudice: *"ciò che è imponibile allo stesso [Google] è un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli (oltre che, naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultasssero correttamente segnalate come criminose). È peraltro evidente (...) che non costituisce condotta sufficiente ai fini che la legge impone, "nascondere" le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di "condizioni generali di servizio" il cui contenuto appare spesso incomprensibile, sia*

66 Tribunale di Milano, 12 aprile 2010, consultabile su www.giuristitelematici.it

67 I quotidiani hanno trattato ampiamento l'argomento informando l'opinione pubblica: F. Sansa, Botte al down nel video su Internet. Sequestrato il film della vergogna, pubblicato su La Repubblica del 12 novembre 2006 e consultabile sul sito http://www.repubblica.it/2006/11/sezioni/cronaca/video-down/video-down/video-down.html; Video choc sul web Ragazzo down torturato a scuola, articolo redazionale de Il Giornale di lunedì 13 novembre 2006, consultato su http://www.ilgiornale.it/interni/video_choc_web_ragazzo_down_torturato_scuola/13-11-2006/articolo-id=133388-page=0-comments=1.

68 Nello specifico per la violazione dell'art. 13 "difettando del tutto l'informativa sulla privacy - visualizzabile in italiano dalla pagina iniziale del servizio Google Video, in sede di attivazione del relativo account al fine di porre in essere l'upload dei files - in ordine a quanto prescritto dal comma 1 della richiamata norma e, per essa, del valido consenso di cui all'art. 23 comma 3; dell'art. 26 riguardando altresì dati idonei a rivelare lo stato di salute della persona inquadrata, dall'art. 17 per i rischi specifici insiti nel tipo di trattamento omesso nell'ipotesi in cui al presente procedimento, non attivandosi Google Italy s.r.l neppure in tal senso - tramite il prescritto interprello - presso l'Autorità Garante".

per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente; tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di "precostituzione di alibi" da parte del soggetto/web e non esclude, quindi, una valutazione negativa della condotta tenuta dagli utenti"[69]. Tale sentenza ha suscitato diverse perplessità tra gli operatori e tra gli commentatori in relazione alla presunta immunità del provider dalle conseguenze della pubblicazione da parte di terzi online. Chi fonda tali osservazioni si basa sull'art. 15 della Direttiva 2000/31/CE rubricato "Assenza dell'obbligo generale di sorveglianza", il quale al primo comma stabilisce che: *"Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*". Tuttavia si osserva da un lato che tale disciplina è limitata al commercio elettronico, mentre dall'altro si nota che Google Video (e servizi assimilabili, come la medesima YouTube), non possono più essere considerati fornitori di servizi neutri, in quanto essi svolgono un vero e proprio ruolo di natura editoriale relativamente ai materiali pubblicati con classifiche di gradimento, inserzioni pubblicitarie e di intervento sui materiali.

Un dato oggettivo emerge da questa sentenza, ovvero l'assenza di espliciti riferimenti normativi comunitari in tema di privacy. Nemmeno la Carta europea dei diritti fondamentali, seppur già vincolante al momento della pubblicazione del dispositivo, è stata citata per richiamare la necessarietà della protezione della parte lesa, nonostante l'esplicito riferimento contenuti nella medesima alla riservatezza dei dati sensibili dei soggetti sottoposti a quel tipo di riprese. A questo proposito soccorre il diritto comparato, dove, in un caso analogo, ovvero la pubblicazione di commenti denigratori e ingiuriosi consistenti in hate speech, la Court of Appeal of the State of California ha statuito che trattandosi di cyberbullismo, tale azione non può avvalersi delle garanzie di libertà di espressione fornite dal First Amendment del Bill of Rights della Costituzione americana poiché il contenuto (di natura diffamatoria) configura un reato[70]. Ne conseguirebbe quindi che la tutela del soggetto debole dalla pubblicazione di dati ovvero immagini diffamatorie online implicherebbe un aspetto delicato, ancora più profondo della stessa rivendicazione del diritto all'oblio[71], cioè la tutela della dignità della vittima. Si tratta di un elemento essenziale del dovere di solidarietà verso i più deboli, dovere che non viene meno neanche sul web.

Il servizio di Google "Street View" ha fatto molto discutere gli esperti di privacy in tutto il mondo: ci si chiede riprendere i dei volti dei passanti ovvero degli interni delle case attraverso le riprese effettuate con una telecamera apposta sul tettuccio dell'auto che percorre le strade cittadine viola la riservatezza dei cittadini? Secondo i ricorrenti che hanno visto pubblicate online le immagini dove, oltre i tendaggi, si intravedono gli ambienti della loro casa questa domanda ha una risposta affermativa. Tuttavia la loro richiesta di danni è stata soddisfatta solo parzialmente. Infatti il giudice ha riconosciuto il simbolico risarcimento di un dollaro perchè seppure consistente in astratto, il pregiudizio non è stato congruamente provato in concreto. In questo modo, il giudice ha riconosciuto una violazione di principio lasciando alla prova della parte l'effettiva quantificazione del danno subito.

I parametri tecnologici e la terminologia settoriale cui ci si riferisce ancora oggi, sia gli operatori del settore, sia i legislatori, sono stati creati negli anni settanta del Novecento. Tuttavia molto è mutato da allora: Internet è diventato un fenomeno di massa. Ciò ha comportato una partecipazione collettiva degli utenti senza precedenti. La ricostruzione della struttura di Internet evidenzia come siano gli Internet Service Providers ad avere un rapporto di vicinanza e prossimità con i loro utenti.

69 Trib. Milano, 12 aprile 2010, cit.

70 Court of Appeal of the State of California, B 207869, 15 marzo 2010, D. C. v. R. R. La sentenza contiene una opinione dissenziente del giudice Frances Rothschild il quale ha affermato che l'opinione di maggioranza “alters the legal landscape to the severe detriment of First Amendment rights.”

71 Sulle "nuove frontiere" del diritto all'oblio: M. Mezzanotte, Il diritto all'oblio. Contributo allo studio della privacy storica, Napoli, 2009, p. 259.

In questo contesto è difficile mantenere valida la distinzione tra controllori, provider e chi fruisce dei dati e a questo proposito lo strumento contrattuale offre un possibile rimedio preventivo sulla disciplina della responsabilità dei provider prevedendo al momento della sottoscrizione dell'abbonamento clausole contrattuali specifiche in materia di riservatezza, uploading e downloading a carico dell'utente che ponga in essere comportamenti illeciti.