UGO PAGALLO

Sul principio di responsabilità giuridica in rete

(in "Il Diritto dell'Informazione e dell'Informatica", 2009, 3, pp. 705-734)

> "*Mi vantavo del fatto di poter spiegare a chiunque pressoché qualsiasi cosa, ad un livello sufficientemente semplice, sulla base di analogie. Orbene, ho cambiato idea*" (Piet Hut 2009, 70)

1. Introduzione

Nell'ultimo numero del dicembre 2006, la rivista "Time", come tradizione, ha eletto la persona dell'anno. A vincere sorprendentemente il premio in quell'occasione fu ciascuno di noi: "You". I giornalisti intendevano celebrare il modo in cui il sistema della produzione e condivisione delle informazioni in rete fosse radicalmente mutato. Se, in ciò che in retrospettiva possiamo definire il Web 1.0, l'utente appariva come un passivo ricettore di dati e informazioni, viceversa, nel Web 2.0, si assiste a un'inedita interattività: i contenuti sono per lo più prodotti dagli utenti stessi della rete, con la possibilità di condividere e immettere immediatamente le informazioni nel sistema d'internet, dove altri utenti potranno selezionare e rivedere criticamente i dati con processi di sindacato come la *really simple syndication* (RSS) e il *peer reviewing* (secondo il modello di tutte le più prestigiose riviste scientifiche anglosassoni). Insomma, con le motivazioni del premio: "Yes, you. You control the Information Age. Welcome to your world".

Rispetto all'ottimistico quadro d'assieme offerto dalla prestigiosa rivista americana, il successo del Web 2.0 ha però comportato una serie di *nuovi problemi giuridici* che, in parte, derivano dalla circostanza che gli utenti *non* controllano affatto i loro dati nell'età dell'informazione. Basti accennare fin d'ora ai rischi connessi alla possibilità di caricare nella rete, senza alcuna mediazione o filtri di sorta, dati e informazioni su terzi, oppure si pensi al costume invalso in molti social network di creare pagine e profili di soggetti che abbiamo incontrato o che avremmo voluto conoscere, attribuendo loro un punteggio, immagini o quant'altro, senza che il diretto interessato ne sia minimamente a conoscenza.

Del resto, non è certo questa la prima volta che le innovazioni tecnologiche contribuiscono a ridefinire e, in certi casi, a creare nuove fattispecie giuridiche. È il caso delle fotografie istantanee che la Eastman Kodak Company ha reso disponibili al grande pubblico sin dal 1884: la circolazione abusiva d'immagini personali, per la prima volta sfruttabile su scala industriale *quasi in tempo reale*, è infatti alla base di quel breve saggio, in cui due avvocati di Boston proponevano d'introdurre un nuovo diritto nell'ordinamento federale statunitense: *The Right to Privacy* (Warren, Brandeis 1890).

Del pari, la tecnica costringe a ripensare natura e scopo d'istituti giuridici preesistenti. È sufficiente citare l'esempio del diritto di copyright, introdotto nel 1709 con l'editto di Anna e disciplinato su scala internazionale dalla Convenzione di Berna sul diritto d'autore (1886). Con l'avvento d'internet e la digitalizzazione delle informazioni in rete, quest'ultimo quadro normativo che, per oltre cento anni, aveva dato buona prova di sé, è uscito a dir poco stravolto. A partire dai due trattati WIPO del dicembre 1996, ossia il *Copyright Treaty* (WCT) e il *Performances and Phonograms Treaty* (WPPT), si è assistito a una fitta serie d'interventi dei legislatori, specie comunitario e statunitense, che, a dir poco, tradisce l'incapacità di regolare un settore in rapido mutamento. Là dove, teoreticamente, non esiste più alcuna differenza tra originale e copia, tale innovazione tecnologica ha fatto sì che al tradizionale 'lungo percorso' tra creatori, produttori, distributori e consumatori, si sia affiancato il "percorso breve" dei *prosumers* (Anderson 2008, Ricolfi 2009).

Quali, dunque, i riflessi giuridici delle nuove tecnologie come quelle compendiate con la formula del "Web 2.0"? Quali le conseguenze della possibilità che le persone hanno d'immettere nell'infosfera (Floridi 2009), dati e informazioni destinati a essere condivisi, selezionati, modificati e rivisti criticamente dagli altri? Quali obblighi e responsabilità dei prestatori di servizi nel campo della comunicazione elettronica e, più in dettaglio, dei prestatori dei servizi di social network? Si tratta di applicare a queste nuove fattispecie le categorie (e norme) giuridiche già a disposizione, oppure, al

modo di Warren e Brandeis, occorre forgiarne delle altre, sulla base dei principi fondamentali dell'ordinamento?

Al fine di venire a capo di questi e ulteriori quesiti, il presente saggio intende analizzare alcuni dei problemi giuridici sorti con il mutamento tecnologico in corso, suddividendo l'argomentazione in quattro parti.

Innanzitutto, intendo precisare quale sia la mia tesi complessiva, e cioè che si abbia a che fare con fenomeni *inediti* tanto dal punto di vista tecnico quanto da quello giuridico.

Quindi, per confermare l'assunto, confuto la tesi avversa che si avvale del procedimento analogico: con l'esempio dei responsabili dei servizi di social network, questi ultimi assomigliano maggiormente a un gestore d'autostrade, a un direttore di giornale o a una sorta di sceriffo digitale?

Dopo di che, chiarisco quale sia l'odierno stato dell'arte in rapporto alla normativa vigente e ai principi alla base dell'ordinamento (comunitario, nel caso italiano). Più in particolare, nel distinguere i *luoghi* dai *piani* della responsabilità personale, esamino alcune questioni territoriali di competenza e il nodo della responsabilità verso terzi.

Infine, traggo alcune conclusioni operative su alcune fattispecie che ritengo cruciali: essendo questioni di principio, sarebbe auspicabile un ampio consenso in un ambito per altri versi così incerto e controverso.

2. "The Uniqueness Debate"

È trascorso un quarto di secolo allorché la comunità di *computer ethics* dibatteva se la rivoluzione informatica avrebbe comportato soltanto "nuove versioni di problemi e dilemmi morali standard" (Johnson 1985), oppure avrebbe richiesto categorie inedite e un punto di vista più consono alle prospettive aperte dalla "logica malleabilità" dei computer (Moor 1985).

Mutatis mutandis, con la consueta prudenza, questo è stato il tema che i giuristi più avvertiti hanno cominciato a discutere una decina d'anni più tardi. Penso al dibattito tra Jack Goldsmith (1998) e David Post (2002) sugli effetti transfrontalieri del cyberspazio: alle tesi del primo, per cui le tradizionali categorie del diritto internazionale, pubblico e privato, sarebbero state in grado di dar conto delle nuove fattispecie create da internet, nel Web, ecc., Post contestava la novità di un mondo informatico in cui, virtualmente, *tutti* gli eventi e transazioni finiscono per presentare carattere transnazionale.

A ridosso del secondo decennio del nuovo secolo, tuttavia, ritengo che non sia lecito nutrire dubbi su chi abbia avuto ragione nel dibattito sulla 'unicità' del computer. Il solo massiccio numero delle norme che il legislatore, a tutti i livelli, ha dovuto creare nei campi del diritto penale (computer crimes), industriale (copyright) o della protezione dei dati (privacy), è segno della radicale soluzione di continuità avvenuta in molti settori chiave del sistema. Di qui che, a mio avviso, non si tratti di insistere ancora sull'ubiquità degli eventi e transazioni in rete o sulla malleabilità dei calcolatori: in realtà, occorre interrogarsi su come gli ordinamenti giuridici siano venuti reagendo alla rivoluzione tecnologica in corso e, in parte, abbiano tentato di dirigere alcune delle trasformazioni in atto.

A questo fine, prima ancora di esaminare la normativa (e giurisprudenza) di riferimento, pare opportuno affrontare la questione sulla base dei principi in gioco con l'avvento del Web 2.0. È la stessa *velocità* delle trasformazioni in atto che consiglia di chiarire preliminarmente il quadro generale entro cui esaminare il ruolo che legislatori e giudici sono chiamati a svolgere, nel definire diritti e obblighi dei cittadini con le loro responsabilità.

Passo quindi a considerare, sia pur brevemente, la nozione chiave di principio (2.1) e, nello specifico, del principio di responsabilità (2.2); dopo di che, potremo tornare ad affrontare l'attualità del dibattito sulla 'unicità' del computer (2.3).

2.1. A proposito di principi

Per 'principio' non intendo riferirmi *solo* a quanto stabilito dalla Carta fondamentale di questo o quel paese, né, eventualmente, alla *sola* giurisprudenza della relativa Corte costituzionale. Senza intendere di dedicarmi a uno scritto di diritto naturale, l'intenzione è di mettere a fuoco alcuni problemi del Web 2.0 che sfuggono allo *iure condito* e, perché no?, richiedono una buona dose d'immaginazione.

Che dire delle trattative, negoziati e contratti siglati quotidianamente, già al giorno d'oggi, da parte di agenti artificiali 'intelligenti'? Che dire della possibilità di intendere questi agenti non solo come agenti giuridici ma, al modo di Floridi (2009), veri e propri agenti *morali*?

I filosofi e teorici del diritto hanno proposto, almeno, due angolazioni diverse per chiarire il *quid* proprio dei principi.

Per un verso, come suggerito da Ronald Dworkin (1985), dobbiamo distinguere i principi dalle regole quali norme e prescrizioni, in quanto si tratterebbe di disposizioni *implicitamente* presenti nell'ordinamento giuridico che sollevano tipici problemi di bilanciamento. Ne è un esempio il caso della responsabilità, ovvero quel principio cardine della convivenza umana che già gli antichi Romani riassumevano all'insegna dell'*Alterum non laedere*. Come riferisco tra breve (2.2), è dato infatti pensare a diverse modalità, secondo cui distribuire il rischio nonché la responsabilità sottesa alle proprie azioni: responsabilità oggettiva, per dolo o colpa, ecc.

D'altro canto, Jürgen Habermas (1995) ha proposto di distinguere ulteriormente tra principi e valori: mentre i primi avrebbero un significato deontologico e, in quanto proposizioni normative, ubbidirebbero alla logica del si o del no, ossia del 'buono per tutti', i valori, invece, implicherebbero un senso teleologico definibile secondo relazioni di preferenza, del tipo o più o meno, come alcunché che è 'bene per noi'. Quanto i giuristi definiscono come diritti fondamentali dell'ordinamento dovrebbe di qui essere concepito, a detta di Habermas, alla stregua dei principi giuridici deontologici propugnati da Dworkin, oppure come beni giuridici ottimizzabili *à la* Alexy (1986).

Senza trasformare un possibile saggio di diritto naturale in uno di teoria generale del diritto, l'idea di massima che possiamo ricavare dal dibattito è che i principi sono chiamati a orientare il nostro comportamento, nel presiedere e dotare di senso la fitta giungla di norme e prescrizioni con cui siamo alle prese nella vita di tutti i giorni. In fondo, uno dei paradossi dell'odierna civiltà dei computer consiste nell'impossibilità di quantificare anche solo il numero delle disposizioni di legge vigenti oggi in Italia!

In ragione di questa definizione preliminare di principio, occorre verificare a continuazione come tutto questo funzioni nel caso specifico della responsabilità personale.

2.2. Sul principio di responsabilità

Esistono tre condizioni in cui, astrattamente, un dato agente (individuale, sociale, artificiale) viene a ritrovarsi in rapporto al principio di responsabilità.

In primo luogo, si ha una condizione di assoluta esenzione di responsabilità. Sebbene siano molteplici le ragioni del principio nei vari campi, quale il criminale (*habeas corpus*) o il civile (*ad impossibilia nemo tenetur*), i motivi possono essere riassunti con la vecchia formula che fu già di Hobbes, per cui, in buona sostanza, tutto ciò che non è vietato è permesso. Si tratta di un tipico principio caro anche alla tradizione liberale (Popper 1974, Hayek 1999).

In secondo luogo, gli agenti possono essere ritenuti, all'opposto, sempre e comunque responsabili. Escluse a priori tentazioni totalitarie, la *ratio* del principio di responsabilità oggettiva nasce da svariate esigenze sociali, stante le quali i datori di lavoro rispondono per gli illeciti dei propri dipendenti, i padroni di animali per le malefatte di questi ultimi (salvo caso fortuito), i genitori per il comportamento dei figli, ecc.

Infine, tra le due posizioni estreme, c'è la responsabilità che nasce per colpa, o dolo, e che riconduce al principio romano dell'*Alterum non laedere*. È qui, a mio avviso, che si annidano molti degli equivoci che affollano l'odierno dibattito (non solo giuridico) sul Web 2.0.

Infatti, esistono alcuni rilevanti problemi relativi alla natura degli accordi tra le parti, su cui, alla luce degli interventi legislativi degli stati, insisto nel corso del saggio: quanto occorso nel febbraio 2009, con il tentativo (fallito) di Facebook di cambiare unilateralmente i termini del proprio servizio – con la pronta reazione degli utenti a tutela dei propri dati personali – ne è solo un esempio.

Tuttavia, tra gli utenti e i prestatori di servizi in rete, dall'accesso alla comunicazione elettronica ai motori di ricerca ai social network, ne va anche della responsabilità verso i 'terzi'. La loro presenza fa infatti sorgere un duplice ordine di problemi: l'uno di natura più strettamente sociologica e psicologica; l'altro più squisitamente giuridico.

Il primo ordine di questioni concerne le nozioni di 'colpa' e 'danno' cruciali per i giuristi esperti in responsabilità extra-contrattuale, ma che sbiadiscono spesso nelle menti dei nativi digitali. Non insisterò mai abbastanza sul fatto che nelle scuole *elementari* giapponesi abbiano introdotto l'insegnamento di *computer ethics* da svariati anni! Uno dei maggiori motivi di preoccupazione che accompagnano l'evolvere del Web 2.0 e, in specie, dei social network, riguarda infatti la *consapevolezza* dei giovani, nel momento di caricare (o permettere l'accesso a) dati e immagini personali, anche di terzi.

Il secondo ordine di questioni riguarda più da vicino i giuristi, avendo a che fare, in particolare, con il momento in cui scatta la responsabilità per 'colpa' del prestatore di servizi nel trattare i dati che gli utenti hanno immesso nella rete. Nel caso di danni ingiusti a terzi, si ha colpa da quando i dati sono stati caricati nel sistema, oppure dal momento in cui l'ente riceve la segnalazione che accende, per così dire, la *sua* responsabilità?

Tornano i dubbi di rappresentare i fatti nuovi con le lenti della tradizione: nel caso di responsabilità del prestatore di servizi per la diffamazione relativa ai dati immessi dal proprio utente in rete, si applicano forse le categorie consuete (come ad esempio quelle della sentenza 4741 della Suprema corte di Cassazione nel 2000), per cui, in quanto reato d'evento, la diffamazione va giudicata nel luogo in cui dei terzi percepiscono le espressioni offensive? Oppure rileva il luogo in cui i dati sono stati immessi e poi trattati? E, però, non è forse il reato d'illecito trattamento dei dati personali più grave del reato di diffamazione? E se il trattamento dovesse avvenire interamente all'estero?

2.3 Ritorno all'"unicità' del computer

A ribadire la velocità delle trasformazioni in corso e il loro impatto sugli ordinamenti giuridici contemporanei – con la conseguente difficoltà di fronteggiare o chiarire le nuove fattispecie in ragione di categorie e norme ereditate dalla tradizione – mi limito a segnalare un altro aspetto della 'unicità' degli elaboratori elettronici, evidenziato dal Comitato per l'informazione, computer e politiche della comunicazione (CSISAC). Nel sommario predisposto il 30 giugno 2009 per il rapporto dell'OCSE, e cioè l'Organizzazione per la cooperazione e lo sviluppo economico, il Comitato ha infatti sottolineato i problemi sottesi a una "visione statica" degli intermediari del mondo digitale, suggerendo di suddividerli in rapporto alle funzioni da essi svolte. Tenuto conto che "nel corso degli anni, gli intermediari su internet sono passati dall'offerta di servizi di base per l'accesso a internet e le e-mail, a un'ampia gamma di strumenti sul Web che consentono agli utenti di pubblicare qualsiasi cosa in formato elettronico, a costi ridotti o nulli" – secondo ciò che si legge del resto nel rapporto del CSISAC (a p. 6) – quest'ultimo organismo ha dunque proposto di distinguere detti intermediari in tre gruppi.

Innanzitutto, abbiamo i tradizionali fornitori di servizi in internet o internet service provider (ISP), il cui scopo è di offrire connettività alla rete.

Quindi, ci sono gli intermediari del commercio elettronico.

Infine, il riferimento va ai prestatori di servizi in rete volti alla distribuzione e reperimento delle informazioni, nonché alla messa a disposizione di piattaforme e applicazioni digitali. Si tratta di quel variegato insieme d'imprese e soggetti che comprende motori di ricerca, mondi virtuali, siti di social network, piattaforme video e vendite all'asta, blog, hosting provider, ecc.

In questa sede, *concentrando l'attenzione soprattutto su quest'ultimo gruppo di intermediari*, converrà tuttavia distinguere ulteriormente queste figure, in modo da far emergere la specificità dei casi relativi ai temi della responsabilità giuridica. Se è infatti abbastanza intuibile la differenza che passa tra un fornitore di connettività alla rete e un sito web vero e proprio, è nondimeno necessario tenere ben distinte le funzioni di un motore di ricerca – che, in risposta alle domande dell'utente, fornisce i link delle pagine web create e pubblicate da altri – da un sito che immette in rete materiale proprio oppure ospita quello altrui.

Stante l'emergenza e la novità dei problemi che hanno spinto le autorità garanti della privacy in Europa a tornare più volte sul punto, concentro prevalentemente l'attenzione sui servizi di social network, rimarcando, quando il caso, identità e differenze con altri intermediari della rete. In omaggio alle categorie tradizionali della dottrina, propongo così di inquadrare la questione nei suoi termini generali, ricorrendo innanzitutto all'analogia, per argomentare più chiaramente la mia tesi sul carattere inedito dei problemi giuridici con i quali siamo chiamati a confrontarci: la rete digitale, cardine

dell'odierna società dell'informazione, assomiglia di più alle autostrade, all'editoria o, semplicemente come protestano in molti, al Far West telematico?

3. Gestori, Direttori e Sceriffi

Abbiamo visto nel paragrafo precedente (2.2), la triplice, astratta condizione in cui ognuno di noi viene a trovarsi alle prese con il principio dell'*Alterum non laedere*. L'ordinamento prevede infatti casi di esenzione di responsabilità, altri di responsabilità obiettiva e, infine, di responsabilità per colpa. L'aspetto interessante di questa distinzione consiste nella circostanza, altamente significativa, che, nell'attuale dibattito sul Web 2.0, le tre ipotesi sono state variamente evocate dagli studiosi per chiarire le responsabilità, civili e penali, cui vanno incontro i prestatori dei servizi che caratterizzano il mondo del social network.

Innanzitutto, è dato rappresentare questi ultimi soggetti come il classico gestore delle autostrade nel mondo reale. Normalmente, nelle società democratiche occidentali, è pacifico che il gestore non risponda per il comportamento e uso dell'autostrada da parte degli automobilisti. Va da sé che, *dietro segnalazione*, egli dovrà porre rimedio all'eventuale malefatta del proprio utente (altrimenti, non ci sarebbe più un'autostrada da gestire). Ma, la tipica 'irresponsabilità' per fatto altrui salta nitidamente agli occhi, solo che si contempli l'ipotesi opposta: vale a dire, immaginare un gestore d'autostrade con funzioni di polizia e sorveglianza (che non sia la propria, ai fini del servizio). Come del resto viene confermato dal modo in cui le autostrade venivano organizzate ai tempi della Germania dell'Est (DDR), ciò contraddirebbe il principio, non solo liberale, d'esenzione di responsabilità sul quale ho insistito in precedenza, come fulcro di ogni società aperta (Popper 1974) e libera (Hayek 1999). Sono per ciò i gestori dei servizi nei social network responsabili al modo in cui lo sono i loro omologhi per le autostrade nel mondo reale?

In realtà, per una parte dell'odierno dibattito, si dovrebbe considerare seriamente la legittimità di optare per la soluzione opposta, rappresentando i responsabili dei social network come se essi fossero direttori di testate giornalistiche o, quantomeno, proprietari o editori di una pubblicazione a stampa (per cui in Italia avremmo sempre responsabilità civile ai sensi dell'art. 11 della legge 47 del 1948). Con la tesi condivisa da una parte della giurisprudenza, si ritiene infatti "ormai acquisito all'ordinamento giuridico *il principio* della totale assimilazione della pubblicazione cartacea a quella diffusa in via elettronica, secondo quanto stabilito esplicitamente dall'articolo 1 della legge 62/2001" (sentenza 6127 della seconda sezione civile di Milano nel maggio 2002). E, però, se così stessero veramente le cose, seguirebbe che, almeno in Italia, avremmo distrutto la creatura giustamente celebrata da Time: *Twitter* dovrebbe per forza 'chiudere' a ruota e, insieme a lei, molti altri…

Ma, a parte il fatto che la summenzionata legge 62 equipara "il prodotto realizzato su supporto cartaceo" a quello elettronico *soltanto* "ai fini della presente legge" – e cioè in materia di trasparenza proprietaria, erogazione di provvidenze, intervento per lo sviluppo editoriale, ecc. – si può dire che i prestatori dei servizi siano veramente assimilabili ai direttori della carta stampata? Stanno proprio così le cose?

In effetti, per esserlo, dovrebbe esistere un *obbligo generale di vigilanza*, stante il quale i responsabili dei servizi in rete dovrebbero controllare *preventivamente* i contenuti delle informazioni immesse dagli utenti. Senza entrare nel merito di altre sentenze e ordinamenti, come quello statunitense (v. sotto 4.2.2), i quali negano risolutamente l'equiparabilità della responsabilità di blogger, motori di ricerca o social network, a quella di editori e proprietari della carta stampata, basterebbe nondimeno osservare che, adottando il principio di responsabilità oggettiva, si finirebbe per violare l'ulteriore principio di proporzionalità garantito dalla Corte di giustizia europea nel bilanciare i diversi diritti costituzionali in gioco. Questo è stato del resto il parere del Parlamento europeo, il 10 aprile 2008, nella risoluzione in cui invita la Commissione e gli Stati membri a evitare misure che entrino in conflitto con le libertà civili e i diritti umani, come nel caso dell'interruzione (in)discriminata dell'accesso a internet tramite politiche che lo rendano 'parziale'.

La responsabilità oggettiva cui si fa riferimento, potrebbe naturalmente essere mitigata; e declinata, per esempio, con il 'semplice' dovere di tempestiva rettifica per le informazioni caricate in rete. Oltre le difficoltà di individuare un comune significato di tempestività della rettifica per enti così diversi come i

motori di ricerca o i prestatori di servizi nel Web 2.0, rimarrebbe tuttavia l'insormontabile difficoltà di spiegare, *in linea di principio*, perché mai, identificando i prestatori di servizi in rete con i direttori (o editori) di giornali, lo scopo dell'ordinamento dovrebbe essere quello di ottenere, sulla base di un'analogia a dir poco azzardata, una (presunta) maggiore sicurezza nei rapporti virtuali su internet, al prezzo di strangolarne l'ultima creatura. Se il principio di responsabilità oggettiva di direttori, editori e proprietari di giornali, fa infatti leva sull'architettura 'uno-a-molti' dei media tradizionali, la peculiarità d'internet e del Web 2.0 consiste nel fatto che la trama delle informazioni si snoda in un percorso 'molti-a-molti' (Lessig 2001).

La radicale diversità tra le due architetture dei media digitali e tradizionali ha così suggerito di proporre una soluzione all'apparenza meno drastica, paragonando questa volta i gestori del Web allo sceriffo che è preposto al mantenimento dell'ordine e al rispetto della legge in una contea. Almeno, questa è stata l'idea che ha ispirato per lungo tempo l'amministrazione di George W. Bush: ad esempio, nel 2006, il Dipartimento di giustizia chiese ad alcuni motori di ricerca come American on line, Yahoo! e Google, di mettere a disposizione del governo un campione a caso delle parole chiave più ricercate dagli utenti nel corso di una settimana, oltre a un milione di siti Web scelti senza speciali criteri dall'indice del motore (la richiesta era formalmente giustificata dal dovere di combattere la pornografia in rete). Un'ulteriore forma di collaborazione ai fini del ripristino dell'ordine è poi emersa anche in Europa, con i nuovi obblighi previsti dalla direttiva 24 del 2006 per "i fornitori di servizi nel campo della comunicazione elettronica accessibile al pubblico" e con i numerosi casi in cui è stato richiesto agli operatori del settore (come Wind in Italia per il caso Peppermint innanzi al Tribunale di Roma, Telefónica d'España nel caso Promusicae davanti alla Corte di giustizia europea, ecc.) di comunicare i dati personali degli utenti onde garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile (l'ambiguità della decisione da parte della Corte di giustizia, il 29 gennaio 2008, consiste nel fatto che *non* sarebbe incompatibile con il diritto comunitario la normativa di uno stato membro che imponesse eventualmente al prestatore del servizio l'obbligo di comunicare a terzi i dati personali dell'utente).

Tuttavia, l'analogia con lo sceriffo o, quantomeno, un suo aiutante, solleva il problema che era già stato avanzato da Bob Marley in *I shot the sheriff*: siamo forse certi che *I didn't shoot no deputy*?

Infatti, mi limito a segnalare, per un verso, le preoccupazioni espresse dal Garante europeo per la protezione dei dati (GEPD), Peter Hustinx, nell'opinione del 25 luglio 2007, a proposito dei rischi sottesi alla "società della nuova sorveglianza". D'altro canto, la questione era emersa prepotentemente l'anno prima con il caso PNR, che aveva contrapposto il Parlamento europeo al Consiglio e alla Commissione, là dove, a parere dell'Avvocato generale Léger, "la presente causa concerne praticamente *un nuovo insieme di problemi*, relativi all'uso di dati commerciali per garantire l'applicazione della legge" (la decisione della Corte di giustizia, il 30 maggio 2006, che ha annullato gli accordi sottoscritti da Commissione e Consiglio con i rappresentanti degli Stati Uniti d'America, ha tuttavia avuto l'effetto indesiderato che, con il passaggio di competenza dalla Comunità all'Unione, non è più concesso alla Corte di giustizia di garantire il rispetto della legge nel trattamento dei dati relativi ai cittadini europei, in volo per o dagli stessi Stati Uniti).

In sostanza, esistono due ragioni di principio, per le quali risulta estremamente pericoloso o fuorviante accostare i responsabili dei vari servizi in rete alla figura dello sceriffo. Se, da un lato, compagnie e imprese a tutti gli effetti private avrebbero il compito di perseguire fini tipicamente pubblici, dall'altro affideremmo ai prestatori di servizi non solo l'obbligo di conservare determinati dati da essi generati o trattati, "allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi" (come previsto dall'art. 1.1 della ricordata direttiva 24 del 2006). In realtà, il prestatore di servizi dovrebbe prevenire il possibile comportamento illecito dell'utente, controllando preventivamente i contenuti dei dati da caricare in rete.

A conforto della tesi, basta del resto fare attenzione alle conclusioni cui sono inequivocabilmente pervenute le più importanti autorità garanti della privacy in Europa, nell'*escludere l'equiparabilità* delle mansioni dei vari prestatori di servizi in rete a quelle di un improbabile sceriffo. Suddivido i pareri con

la summenzionata tripartizione proposta dall'OCSE per gli intermediari di internet (v. sopra 2.3).

Innanzitutto, per quanto concerne i servizi di telecomunicazione, il Garante europeo (GEPD) ha dichiarato nel parere del 23 giugno 2008 che "la sorveglianza delle telecomunicazioni è (…) una questione discutibile, sia essa diretta al controllo dei contenuti protetti da diritti di proprietà intellettuale o di altri contenuti illeciti. Questo punto solleva la questione dell'intervento di un soggetto commerciale, che offre un servizio (di telecomunicazione) specifico, in una sfera in cui *in linea di principio* non è previsto che intervenga, vale a dire il controllo del contenuto delle telecomunicazioni. Il GEPD ricorda che, *in linea di principio*, tale controllo non dovrebbe essere esercitato dai prestatori di servizi e certamente non in modo sistematico" (§ 32 del parere, corsivi miei).

Per quanto riguarda, invece, gli intermediari del commercio elettronico, il Gruppo di lavoro ex art. 29, nel parere del 18 gennaio 2005, ha fatto presente come non possa essere imposto ai prestatori di servizi in rete alcun obbligo sistematico di sorveglianza e collaborazione, citando in questo senso l'art. 15 della direttiva 2000/31/CE sul commercio elettronico (disposizione recepita in Italia con l'art. 17 del D.L. n. 70 del 2003).

Ma che dire dell'ultimo gruppo, vale a dire i servizi di piattaforme e applicazioni digitali, nonché di reperimento delle informazioni in rete? Sarebbero, essi, i soli prestatori di servizi per i quali non vale il principio d'esenzione di responsabilità riconosciuto ai due precedenti gruppi di intermediari?

A ben vedere, vi sono sia ragioni di principio sia di stretto diritto positivo, che escludono decisamente una tale conclusione. Pretendere un controllo preventivo sui contenuti da immettere in rete comporterebbe infatti la palese violazione della direttiva comunitaria (e del relativo decreto d'attuazione in Italia), che, nel fissare i termini della responsabilità nelle attività di semplice trasporto (*mere conduit*), di memorizzazione temporanea (*caching*) e di memorizzazione delle informazioni (*hosting*), esclude a chiare lettere l'obbligo generale di sorveglianza per *tutti* i "prestatori di servizi della società dell'informazione" (come individuati ai sensi dell'art. 2 del D.L. 70/2003 che recepisce la citata D-2000/31/CE).

Inoltre, tale eventuale obbligo generale costituirebbe una palese violazione del principio di proporzionalità, dato che condurrebbe necessariamente alla paralisi, o distruzione, dell'intero sistema. Siamo disposti a pagare simile prezzo pur di prevenire qualche reato come la diffamazione o la violazione del copyright? Non è forse dipesa la straordinaria fortuna di internet dalla sua architettura e cioè, come affermato dal padre del Web, Tim Berners-Lee (1999), dall'essere stato progettato senza centro in modo da risultare "fuori controllo"?

Tuttavia, a scanso di equivoci e come segnalato in precedenza (2.3), è importante distinguere all'interno della tipologia messa a punto dall'OCSE, le funzioni e responsabilità dei diversi prestatori di servizi e applicazioni in rete. Per chiarire le ragioni per le quali penso che non sia il caso di individuare in questi ultimi soggetti lo sceriffo cui sparare al modo di Bob Marley, propongo l'esempio specifico dei responsabili dei servizi per il social network. Avremo in questo modo la lente concettuale per decidere finalmente se, per caso, non vi sia ancora qualcuno 'là fuori' intento a dar la caccia a un falso 'sostituto'.

4. "…but I didn't shoot no deputy…"

Le questioni di responsabilità in rete si presentano secondo una ricca e articolata fenomenologia che va dal momento in cui l'utente legge, o dovrebbe accuratamente leggere, i termini del servizio – prima di immettervi il proprio materiale – fino ai feedback, spesso inopinati, dei consociati. Penso, ad esempio, ai casi in cui alcuni quotidiani italiani hanno ritenuto di pubblicare foto di persone vittime di incidenti o di fatti di sangue, prese da Facebook senza alcun consenso e adeguato controllo, con l'imbarazzante risultato che le foto in questione riguardavano in realtà tutt'altre persone[1].

[1] Mi sia permessa una prima, breve nota, per far notare che lo stesso problema si è verificato nel corso di alcuni programmi televisivi con la diffusione di immagini e foto tratte sempre da Facebook. Per l'illecito trattamento dei dati personali nell'utilizzo di immagini tratte da social network si v. i provvedimenti del Garante italiano per la protezione dei dati personali del 6 maggio 2009. Sul punto è tornato il presidente Francesco Pizzetti nella relazione 2008 del 2 luglio 2009, doc. web n. 1628428, p. 9. In ogni caso, viene confermato in questo modo ciò che avevo già rilevato nel mio scritto sulla privacy (2008, 152): "Il fatto, poi, emerso fin troppo di continuo nelle cronache giornalistiche italiane, per cui simile auto-disciplina [del codice per l'esercizio dell'attività giornalistica] ha lasciato molto a desiderare, non è certo ragione sufficiente per abbandonare uno dei motivi più innovativi e interessanti della disciplina europea sulla privacy", vale a dire,

In questa sede, propongo di incentrare l'attenzione su due punti particolarmente rilevanti di questa fenomenologia: il primo riguarda i 'luoghi della responsabilità', vale a dire le questioni di competenza e giurisdizione relative ai termini del servizio offerto all'utente. Il secondo punto concerne invece i problemi di responsabilità verso terzi che nascono per via delle informazioni immesse in rete dagli utenti. Su queste basi, saremo in grado di valutare più precisamente i motivi di principio sottesi ai nostri casi: mentre infatti, nel ricordato parere del 30 giugno 2009 il *Civil Society Information Society Advisory Council* (CSISAC) ha inteso evidenziare le straordinarie opportunità sottese al ruolo degli intermediari in internet, il Gruppo di lavoro ex art. 29, nell'opinione 5/2009 del 12 giugno, ha soprattutto sottolineato i rischi relativi ai servizi di social network. Si tratta forse di un gioco a somma zero?

4.1. I luoghi della responsabilità

Ho segnalato più sopra (2), il dibattito sul cyberspazio occorso tempo addietro tra Jack Goldsmith e David Post: mentre il primo, in sostanza, sosteneva che le categorie e norme di conflitto del diritto internazionale, pubblico e privato, sarebbero state in grado di dirimere le varie questioni di competenza e giurisdizione destinate a sorgere nel mondo di internet, la tesi di Post, al contrario, era che questo quadro tradizionale sarebbe stato messo in mora dalle nuove tecnologie. Quanto infatti costituiva, una volta, l'eccezione – e poteva essere disciplinato in quanto tale dall'ordinamento – è diventato nel frattempo la regola; ossia, il fatto che tutti gli eventi e transazioni finiscano per avere sempre, virtualmente, natura e carattere transnazionali.

Quali, per ciò, i criteri, o meccanismi, per risolvere la sovrapposizione tra ordinamenti in internet?

Per chiarire la questione nei suoi termini generali, suddivido la presente sezione in tre parti: innanzitutto (4.1.1), presento un caso concreto, avente ad oggetto i servizi di Facebook in Canada; quindi (4.1.2), illustro il modo in cui tale problema canadese viene variamente dibattuto in Europa; infine (4.1.3), torno sull'alternativa emersa nel dibattito tra Goldsmith e Post.

4.1.1. Facebook in Canada

Pochi giorni dopo l'opinione 5/2009 del Gruppo di lavoro ex art. 29, su cui torno nel prossimo paragrafo, è stato il turno del Garante della privacy in Canada di occuparsi di social network e, in particolare, dei servizi di Facebook. L'ufficio del *Commissioner*, in effetti, ha reso pubblico un rapporto sulle "Indagini seguite alla denuncia presentata dalla Consulta per le politiche canadesi su internet e il pubblico interesse" – vale a dire il *Canadian Internet Policy and Public Interest Clinic* o CIPPIC – in cui venivano contestati a Facebook ventiquattro possibili violazioni della normativa sulla privacy vigente in quel paese, ovvero il *Personal Information Protection and Electronic Documents Act* (PIPEDA). Laddove, in maniera analoga alla Comunità europea, la legge canadese prevede che il trattamento dei dati avvenga, in genere, con il consenso dell'interessato, al quale spetta inoltre il diritto di essere a conoscenza della natura delle informazioni a disposizione dei prestatori di servizi nonché della lista dei terzi ai quali quella informazione è rilasciata, il CIPPIC ha eccepito a Facebook, tra le altre cose, di non informare correttamente i suoi utenti circa il modo in cui i dati personali sono utilizzati e finanche rilasciati a più di 950 mila sviluppatori di applicazioni. Inoltre, è stato contestato di monitorare comportamenti anomali e di impiegare cookies permanenti anche per l'uso mobile di Facebook; di non cancellare, semplicemente disattivando, gli account degli utenti che ne abbiano fatto richiesta; e, infine, di non ottenere il consenso dei terzi estranei ai servizi di Facebook, al fine del caricamento e conservazione dei loro dati personali.

---

appunto, i codici di auto-disciplina.

La reazione di Facebook, società nordamericana con stabilimento in Palo Alto, California, e sede per gli affari internazionali a Dublino, in Irlanda, è stata particolarmente istruttiva. Dichiarandosi d'accordo con molte delle proposte del Commissario canadese, Facebook ha infatti suggerito alcune "ragionevoli alternative" in quanto il vigente "regime di diritti e responsabilità" richiederebbe, a suo avviso, di consultare i propri utenti, prima di modificare eventualmente determinate *policies*. Questa, del resto, è stata la 'lezione' che Facebook avrebbe appreso nel febbraio 2009, allorché aveva provato a modificare (unilateralmente) i termini del proprio servizio o TOS (*terms of service*). Innanzi all'immediata critica degli utenti, Facebook non solo si vide costretta a ripristinare il vecchio TOS, ma indisse una sorta di referendum interno al fine di stabilire quali avrebbero dovuto essere i nuovi termini del servizio. Mentre la società statunitense intraprendeva nel frattempo i primi passi per ridurre lo scambio di dati con gli sviluppatori di applicazioni, oltre a limitare il numero di licenze in capo a terzi e migliorare i meccanismi di cancellazione degli account, il 75 per cento degli interessati stabiliva che il nuovo TOS avrebbe dovuto essere deciso dagli utenti. Il risultato è stato che essi hanno visto riconosciuto il "diritto di possedere e controllare la loro informazione".

Davanti a questo (bel) caso di auto-regolamentazione in rete, tuttavia, l'alto Commissario canadese, nel rapporto sulle "indagini seguite alla denuncia presentata dal CIPPIC", ha rilevato che "se noi comprendiamo l'importanza che Facebook assegna al feedback degli utenti, i requisiti normativi e le obbligazioni stabilite dalla legge [PIPEDA] non dipendono dalla loro approvazione". A differenza, cioè, del modello USA, in cui il consenso degli interessati gioca un ruolo determinante in materia di privacy e, in genere, nei rapporti tra i privati (Pagallo 2008, 62, 93-94, 99-101, *passim*), esistono altri ordinamenti, come quello canadese o quello comunitario, in cui il consenso appare spesso principio *necessario ma non sufficiente* ai fini della liceità nel trattamento dei dati. Donde, come risultato, il problema di competenza e giurisdizione prospettato all'inizio del presente paragrafo: a che titolo l'Autorità canadese può imporre a una società statunitense, con uffici internazionali a Dublino, le previsioni della legge nazionale PIPEDA?

Per approfondire la questione nei termini più abituali al lettore italiano, inquadro a continuazione il tema della competenza degli ordinamenti giuridici in internet, alla luce di quanto previsto nello specifico dalla normativa del sistema comunitario. Dopo di che, dovremmo essere in grado di valutare le ragioni di entrambe le parti.

4.1.2. Sull'esegesi dell'art. 4 (D-95/46/CE)

Per definire l'applicazione internazionale del diritto comunitario in materia di tutela e trattamento dei dati personali – da parte di prestatori di servizi in internet non stabiliti nell'Unione europea – occorre muovere dall'art. 4 della direttiva quadro in materia di privacy (la n. 46 del 1995). Questa disposizione, in effetti, funge quale 'norma di conflitto' del diritto internazionale classico, nel senso che essa precisa i criteri in base ai quali la normativa degli stati membri, con cui si attua la direttiva comunitaria sulla tutela dei dati personali, risulta eventualmente rilevante.

In particolare, l'art. 4 stabilisce due criteri.

Il primo fattore di connessione, che rende applicabile la normativa comunitaria, concerne il luogo di stabilimento del responsabile del trattamento che, ai sensi dell'art. 4.1 (a), si trovi nel territorio di uno o più stati membri.

Il secondo fattore di connessione riguarda invece il legame fisico tra agente e ordinamento: anche se il responsabile del trattamento non sia stabilito nel territorio della Comunità, esso sottostà alla sua normativa quando ricorra, ai sensi dell'art. 4.1 (c), a "strumenti, automatizzati o non automatizzati" situati in uno stato membro.

Queste disposizioni, da una parte, sembrano pertanto escludere dal raggio di azione della disciplina comunitaria quelle società, i cui stabilimenti si trovino fuori dall'Unione. Infatti, ai sensi del 19° considerando della direttiva 31 del 2000 sul commercio elettronico, "il luogo di stabilimento, per le società che forniscono servizi tramite siti Internet, non è là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica". Tale esclusione del raggio di applicabilità della normativa comunitaria pare inoltre confermata dall'ipotesi contemplata dal secondo fattore di connessione sopramenzionato, e cioè nel caso di tutte quelle società i cui server si ritrovino, ancora una volta, all'infuori dell'Unione. Del resto, questa sembra essere l'interpretazione adottata dal Garante italiano per la privacy in alcuni provvedimenti e lettere[2].

D'altra parte, molto dipende dal significato dei termini impiegati e dalla loro resa nelle diverse lingue dell'Unione. Quanto, infatti, nella versione italiana dell'art. 4.1 (c) è riportato sotto il lemma "strumenti" diventa "*equipment*" e non "*means*" nella versione inglese. Fermo restando che tra le definizioni offerte dall'art. 2 della direttiva comunitaria non c'è spazio per quella di "strumento", "apparato" o "dispositivo", il Gruppo di lavoro ex art. 29 ha tuttavia sostenuto sin dal documento adottato il 30 maggio 2002, che "il PC dell'utente può essere considerato uno strumento ai sensi dell'articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE". Infatti, l'idea è "che il diritto nazionale dello Stato membro in cui è ubicato il personal computer dell'utente sia applicabile con riguardo alla domanda in quali condizioni i suoi dati personali possono essere rilevati collocando cookie sul suo disco rigido".

Si tratta, in definitiva, di un parere più volte ribadito di recente dal Gruppo di lavoro ex art. 29. Rimandando all'opinione 1/2008 in tema di tutela dei dati trattati dai motori di ricerca, esso ha infatti confermato nella successiva opinione 5/2009 del 12 giugno, che "le previsioni della direttiva sulla protezione dei dati si applicano ai prestatori di servizi di social network nella maggior parte dei casi, anche quando la loro sede sia stabilita fuori dallo Spazio economico europeo. Il Gruppo di lavoro ex art. 29 si rifà alla sua precedente opinione sui motori di ricerca per una guida ulteriore alle questioni concernenti lo stabilimento e uso di strumenti [*equipment*] quali fattori decisivi ai fini dell'applicazione della direttiva sulla protezione dei dati e la normativa conseguentemente adottabile per via del trattamento degli indirizzi IP e l'uso dei cookie" (si tratta del § 3 di detta Opinione).

L'equiparazione di cookie e indirizzi IP agli strumenti di cui all'art. 4.1 (c), nondimeno, sembra rappresentare più una scelta di politica normativa che una semplice esegesi dei testi *de quo*. A parte la constatazione che il legislatore comunitario non si era posto semplicemente il problema, risulta assai discutibile asserire che gli indirizzi IP debbano di per sé essere considerati sempre e solo alla stregua di "dati personali". A ben vedere, ciò dipende dal tipo di prestatori di servizi di cui si tratta: un conto è infatti il provider grazie al quale si accede a internet, essendo esso a fornire gli indirizzi IP ai propri abbonati, di cui conosce evidentemente nome, indirizzo e altre informazioni, per l'appunto, personali; altra cosa, però, sono molti dei siti web che l'utente visita con quel dato indirizzo e che, tuttavia, non consentono al sito in questione di identificare il soggetto visitante.

Inoltre, per quanto riguarda il caso dei cookie, parte della dottrina ha avvertito non solo la pratica difficoltà, per non dire l'impossibilità, di far valere la conseguente giurisdizione pan-europea; ma, anche le incongruenze che discenderebbero da simile interpretazione della direttiva. Ad esempio, Christopher Kuner ha rimarcato tre punti deboli della possibile equiparazione dei cookie agli strumenti dell'art. 4.1 (c).

In primo luogo, se molte disposizioni del diritto comunitario in tema di tutela dei consumatori e di privacy si applicano indubbiamente ai soggetti di paesi terzi che abbiano *deciso* di vendere beni e servizi

[2] Si v. ad esempio i provvedimenti del 9.11.2005, del 18.1.2006 e del 31.1.2008, oppure la lettera del 24.11.2006, in cui, a proposito dei servizi offerti da Google Video, viene esclusa l'applicabilità della normativa nazionale, "posto che il trattamento in questione è risultato, allo stato degli atti, effettuato fuori dal territorio nazionale".

a cittadini e società dell'Unione, non vi sarebbe però alcun modo semplice affinché i siti web che fanno uso di cookie, possano escludere dai propri servizi utenti dell'Unione: "infatti, per fare ciò sarebbe pur sempre necessaria l'identificazione dei dati dei soggetti che navigano in rete, sulla base della loro residenza, ciò che finirebbe per riproporre questioni relative alla tutela dei dati" (Kuner 2003, 101).

Secondariamente, la tesi che i cookie costituiscano a tutti gli effetti "strumenti" ai sensi dell'art. 4.1 (c) finirebbe per far dipendere l'applicabilità della normativa non più dal luogo in cui si trova lo stabilimento del responsabile del trattamento dei dati, bensì, volta per volta, dal luogo in cui si trova il soggetto di cui si intendono proteggere i dati personali; ciò che, palesemente, contraddice il principio ispiratore sotteso alla normativa.

Infine, nell'estendere il diritto comunitario a tutti i siti web del pianeta che ricorrono all'uso di cookie, non solo si assisterebbe a un salto di qualità rispetto alla decisione di assoggettare alle proprie norme chi abbia deciso di fare affari con i cittadini europei. In realtà, alle difficoltà pratiche di far valere nel concreto la propria giurisdizione, si aggiungerebbero le difficoltà dei responsabili stranieri nel trattamento dei dati che "dovrebbero conformarsi simultaneamente alla legislazione di ogni singolo stato membro dell'Unione, ciò che appare come un onere impossibile" (Kuner 2003, 102).

Tuttavia, senza entrare ulteriormente nel dettaglio di queste, o altre, posizioni critiche, rimane il problema di fondo relativo all'esegesi dell'art. 4 che, in linea con l'impostazione del presente saggio, solleva a mio avviso una questione di principio. Delineata chiaramente dal ricordato documento di lavoro adottato dal Gruppo ex art. 29 nel maggio 2002, la questione riporta al dibattito tra Goldsmith e Post sulle novità (o meno) che il cyberspazio propone al mondo del diritto. È tempo di esaminare nel merito le ragioni di un paradosso.

4.1.3. Le ragioni di un paradosso

Allorché il Gruppo ex art. 29 si è posto il problema di decidere, nel documento di lavoro del 30 maggio 2002, se "il PC dell'utente può essere considerato uno strumento (…) con riguardo alla domanda in quali condizioni i suoi dati personali possono essere rilevati collocando cookie sul suo disco rigido", la risposta (positiva) era motivata sulla base di un duplice ordine di ragioni.

Innanzitutto, in sintonia con le tesi di Goldsmith[3], il Gruppo ricorreva implicitamente al *principio di sovranità nazionale* quale criterio principe per dirimere potenziali sovrapposizioni tra ordinamenti: "da un'indagine sul diritto internazionale emerge che gli Stati hanno la tendenza a utilizzare molteplici criteri alternativi per determinare estensivamente il campo d'applicazione del diritto nazionale al fine di coprire il maggior numero di casi possibili a beneficio della più ampia tutela dei consumatori e delle imprese nazionali" (si v. il "caso A: cookie" del ricordato documento 5035/01/IT/def. WP 56).

Tuttavia, in sintonia con le tesi di Post[4], il Gruppo sosteneva altresì l'applicabilità del diritto comunitario in ragione della *tutela dei diritti fondamentali* delle persone. In virtù della *ratio* sottesa all'art. 4.1 (c), l'idea è infatti che, estendendo ai siti web utilizzatori di cookie la normativa comunitaria sul trattamento dei dati, sarebbe possibile "garantire che una persona non sia priva di tutela per quanto riguarda il trattamento effettuato nel suo paese per il solo fatto che il responsabile non è stabilito sul territorio comunitario. (…) È opportuno notare come non sia necessario che la persona sia un cittadino comunitario o sia fisicamente presente o residente nell'UE. La direttiva non opera alcuna distinzione sulla base della nazionalità o della residenza in quanto armonizza le normative degli Stati membri in materia di diritti fondamentali riconosciuti a tutti gli esseri umani" (si v. il § 2 del documento).

La duplice, contraddittoria ispirazione del documento, sovranocentrica e cosmopolitica al tempo stesso, dipende a mio giudizio dalla *novità* dei problemi giuridici sorti nel cyberspazio – soprattutto se esaminati in rapporto a una mera lettura esegetica degli articoli che compongono la direttiva 46 del '95 – con la conseguente difficoltà che discende da ciascuna delle possibili opzioni interpretative. A leggere,

---

[3] Lo studioso americano insiste infatti sulla tesi che "a nation's right to control events within its territory and to protect the citizens permits it to regulate the local effects of extraterritorial acts" (Goldsmith 1998, 1234).

[4] Secondo Post, la novità del cyberspazio consiste non solo nel fatto che i cittadini vengano ad essere lesi da condotte che lo stato è semplicemente incapace di disciplinare. In realtà, il rischio è che lo stato pretenda di imporre norme per le quali gli individui non hanno alcun peso nel momento di assumere decisioni che li coinvolgono direttamente, per ciò stesso creando una situazione illegittima che mette a repentaglio il principio democratico della "rule of law" (v. Post 2002, 1382).

infatti, in senso restrittivo la nozione di "strumento" di cui all'art. 4.1 (c), il rischio cui si va incontro è pur sempre quello paventato dal Gruppo ex art. 29 e, più tardi, dal Commissario canadese nei confronti di Facebook: in sostanza, non saremmo più in grado di proteggere, nel mondo transfrontaliero di internet, i dati delle persone presenti nel territorio nazionale. E, però, a leggere in senso estensivo quella stessa nozione di "strumento", si giunge al paradosso di rivendicare una giurisdizione mondiale paneuropea: quest'ultima dovrebbe in effetti venire applicata anche nel caso del rapporto di un cittadino statunitense o cinese che, per sorte, dovesse avvalersi dei servizi di un 'proprio' sito web nel Vecchio Continente.

Al Gruppo ex art. 29 non sfuggono naturalmente alcune lacune e ambiguità dell'ordinamento vigente: nella recente Opinione sui social network, ad esempio, si dichiara che "manca di base legali" la creazione di profili di soggetti che non appartengono a tali network e che, tuttavia, sono tecnicamente possibili tramite l'aggregazione di dati immessi indipendentemente da altri utenti (v. § 3.5 dell'Opinione). Peraltro, anche nel caso in cui il social network in questione avesse la possibilità di contattare il diretto interessato per comunicargli l'esistenza di dati e informazioni che lo riguardano, il risultato è che un eventuale invito, tramite e-mail, di unirsi al social network per avere accesso a quei dati personali, cadrebbe sotto la scure dell'art. 13.4 della direttiva 2002/58/CE!

In realtà, tornando ai problemi ermeneutici sollevati dall'art. 4.1 (c), le radici del paradosso vanno ricercate ancor più in profondità. La ragione per cui rimangono forti motivi di perplessità al di là della specifica soluzione giuridica per la quale si opti a proposito della nozione di strumento, dipende infatti dalla progressiva digitalizzazione dell'ordinamento che va di pari passo con la crescente globalizzazione della privacy. Come già sottolineato dall'Opinione del Garante europeo (GEPD) nel luglio 2007, anche le disposizioni previste dagli art. 25 e 26 della direttiva comunitaria in tema di trasferimento dei dati a paesi terzi, incontrano severe limitazioni nel disciplinare un mondo sempre più globale, interdipendente e informatizzato; e, questo, nonostante gli sforzi delle istituzioni comunitarie per far funzionare al meglio tale "regime speciale" attraverso clausole contrattuali standard, norme di auto-disciplina, accordi con la Camera internazionale di commercio o con il perfezionamento del giudizio sull'adeguatezza nella tutela dei dati accordata da paesi terzi. Per dirla con Peter Hustinx, "questo sistema, una conseguenza logica e necessaria delle limitazioni territoriali dell'Unione europea, non garantirà la piena protezione dei dati ai soggetti europei in una società disposta a rete, in cui le frontiere fisiche perdono importanza (…): l'informazione su Internet è onnipresente, ma la giurisdizione del legislatore europeo non lo è" (§ 42 dell'Opinione).

Sulla stessa lunghezza d'onda e a riprova di una prospettiva convergente, basta poi fare attenzione alle conclusioni cui è giunto il 2 luglio 2009 il Garante italiano per la protezione dei dati personali. A giudizio di Francesco Pizzetti, in effetti, "c'è bisogno urgente di regole nuove e condivise", tanto più che "l'epoca delle Autorità nazionali ed europee di sola garanzia è al tramonto. C'è sempre più bisogno di nuove Autorità di regolazione e di controllo, capaci di lavorare congiuntamente" secondo le modalità di un "nuovo e più vasto WTO" che sia in grado di "dare disciplina e certezza all'immenso sistema di reti di telecomunicazioni, che è il cuore pulsante del mondo contemporaneo".

In attesa di un intervento del legislatore comunitario auspicato dalle sue stesse Autorità, la morale da trarre è duplice.

Per un verso, se si privilegia l'interpretazione della direttiva comunitaria imperniata *à la* Goldsmith sul principio di sovranità, sembra tuttavia necessario *ridimensionare* "i luoghi della responsabilità" paneuropea tra privati, quantomeno sul piano del diritto penale, in omaggio al *principio di legalità*. Senza entrare nel merito della *vexata quaestio* sulla possibilità di distinguere l'interpretazione estensiva da quella analogica (Bobbio 1938), basta infatti notare che l'applicabilità internazionale del diritto comunitario in materia di tutela e trattamento dei dati, come nel caso paradigmatico dell'art. 4 D-95/46/CE, solleva questioni che sono spesso di politica normativa, più che di semplice lettura e interpretazione dei testi, stante i silenzi della legge di cui all'art. 2 della medesima direttiva.

D'altra parte, se si pensa che il fine della normativa comunitaria sia invece quello di garantire i diritti fondamentali della persona umana, si tratta di tornare ai suggerimenti del GEPD, maturando la consapevolezza della necessità di un intervento su scala transfrontaliera o internazionale. Solo mediante accordi bilaterali o multilaterali con paesi terzi anche in materia giurisdizionale, oltre alla cooperazione con altri organismi internazionali e tramite l'elaborazione di un "quadro globale" per la protezione dei

dati sulla scia delle linee guida elaborate dall'ONU e dall'OCSE, saremo finalmente in grado di "trovare un giusto equilibrio tra i diversi interessi dei paesi implicati" (secondo quanto recita il primo paragrafo del più volte citato documento di lavoro del Gruppo ex art. 29, nel maggio 2002).

È giunto il momento di analizzare "i piani della responsabilità".

4.2. I piani della responsabilità

Dopo aver fatto cenno ai nodi della competenza e giurisdizione, è opportuno chiarire alcuni dei motivi principali connessi ai diversi "piani della responsabilità". Essi possono essere agevolmente distinti tra le responsabilità che nascono dagli accordi tra le parti e con i termini del servizio in rete, e le responsabilità che sorgono viceversa nei confronti dei terzi. Per approfondire questa distinzione, suddivido la sezione in tre parti, relative ai diritti degli utenti e agli obblighi dei prestatori di servizi (4.2.1), alla responsabilità verso i terzi sia nell'ordinamento statunitense (4.2.2), sia in quello comunitario (4.2.3). Quindi, saremo finalmente in grado di trarre le conclusioni del discorso (5).

4.2.1. Sui diritti degli utenti e gli obblighi dei provider

Come emerso precedentemente con il caso Facebook in Canada (4.1.1), e con l'approccio generale del Gruppo di lavoro ex art. 29 circa l'applicabilità internazionale del diritto comunitario in materia di tutela e protezione dei dati personali (4.1.2), la definizione dei diritti degli utenti e degli obblighi dei prestatori di servizi in rete risulta strettamente collegata al tema della ripartizione delle competenze tra ordinamenti su scala mondiale. Nella più volte citata Opinione 5/2009 del Gruppo ex art. 29, tutta la prima parte del documento è non a caso dedicata a questo punto. Sulla base dell'assunto che "la direttiva sulla tutela dei dati si applica in genere al trattamento dei dati personali da parte dei servizi di social network, anche qualora la loro sede si trovi al di fuori dello Spazio economico europeo", segue che "i prestatori di servizi di social network sono considerati responsabili del trattamento dati" sebbene questi servizi "fuoriescano dallo scopo della definizione di servizio di comunicazione elettronica e pertanto la direttiva sulla conservazione dei dati non si applica ai servizi di social network" (si v. i punti 1, 2 e 6 del sommario dell'opinione, al § 5).

Senza entrare ancora una volta nel merito della cifra adottata dal Gruppo ex art. 29, è importante rilevare come i termini del servizio e il conseguente accordo tra prestatori e utenti debbano intendersi *all'interno* del quadro normativo di riferimento che, volta per volta, definisce diritti ed obblighi inderogabili. Ciò, evidentemente, vale tanto per l'ordinamento comunitario quanto, ad esempio, per il diritto statunitense, dove, ai sensi del *Children's Online Privacy Protection Act* o COPPA del 1998, *tutti* i gestori di siti Web diretti a bambini di meno di tredici anni, non solo hanno l'obbligo di ottenere il consenso verificabile di un genitore, ma devono altresì fornire le informazioni e garantire il livello di sicurezza come stabilito perentoriamente dalla legge.

Nel quadro europeo dei social network delineato dal Gruppo ex art. 29, quest'ultimo ha per ciò chiarito il quadro normativo in ragione di un elenco di diritti e doveri sottratti alla volontà delle parti.

Da un lato, abbiamo gli obblighi in capo ai servizi di social network, riassunti nei punti 7-15 del sommario approntato dall'Opinione 5/2009. Tra le altre cose, i prestatori di tali servizi devono fornire una chiara ed esaustiva informazione delle finalità e diverse modalità secondo cui essi intendono trattare i dati personali; del pari, essi devono mettere in guardia gli utenti circa i rischi per la propria privacy allorché caricano dati nel network; inoltre, essi devono prevedere un periodo massimo per la conservazione dei dati degli utenti inattivi e, comunque, gli account non più utilizzati devono essere eliminati; infine, riguardo ai minori, i prestatori di servizi devono intraprendere le opportune azioni onde limitare i rischi[5].

D'altro canto, i membri del social network, indipendentemente dai termini del servizio, devono essere considerati "persone interessate" ai sensi degli art. 10-14 D-95/46/CE, per cui occorre informarli sull'identità del responsabile del trattamento dei dati, sulle finalità del trattamento cui sono

[5] Va peraltro segnalato che, nel § 3.2 dell'Opinione, il Gruppo si sofferma sugli ulteriori obblighi di sicurezza in capo ai prestatori di servizi con la necessità di approntare una configurazione del sistema che permetta agli utenti di dare liberamente e specificamente il loro consenso ad ogni accesso al loro profilo personale che travalichi i propri contatti, "in modo da diminuire il rischio di trattamento illecito dei dati da parte di terzi".

destinati i dati, sull'esistenza o meno di trattamenti di dati che li riguardano, sui destinatari o le categorie dei destinatari dei dati, oltre al diritto di rettifica, cancellazione o congelamento dei dati, al diritto di opporsi al trattamento di dati a fini di invio di materiale pubblicitario, ecc. Tenuto poi conto dell'art. 6.1 (c) della direttiva, stante il quale i dati devono essere "adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati", il Gruppo di lavoro fa inoltre presente, nel § 3.9 della propria opinione, che, sebbene "i servizi di social network possano aver bisogno di registrare alcuni dati al fine di identificare i propri membri, ciò non implica la necessità di pubblicare il loro vero nome su internet". Anzi, i prestatori dei "servizi di social network dovrebbero riflettere attentamente sulla legittimità di forzare i propri utenti ad usare la loro reale identità piuttosto che uno pseudonimo". Con il risultato, sancito nel 18° e ultimo punto del sommario dell'Opinione, che "agli utenti dovrebbe essere concesso, in linea di massima, di adottare uno pseudonimo".

Oltre ai diritti degli utenti e membri di social network, con i conseguenti obblighi dei prestatori di servizi, esistono naturalmente gli obblighi degli utenti stessi. Così, l'eccezione prevista dall'art. 3.2 della direttiva per i trattamenti di dati personali "effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico" non si applica se l'utente agisce a nome di un'impresa o un'associazione, o allorché l'accesso all'informazione "va[da] al di là dei contatti scelti dall'utente, come quando l'accesso al profilo è concesso a tutti i membri del servizio di social network o i dati sono indicizzabili dai motori di ricerca". In ogni caso, "un alto numero di contatti può essere indice del fatto che l'eccezione domestica [ex art. 3.2 della direttiva] non si applica e, pertanto, l'utente dovrebbe essere considerato responsabile del trattamento dei dati" (si tratta dei §§ 3.1.1 e 2 dell'Opinione 5/2009).

Inoltre, sempre a proposito dell''eccezione domestica' della direttiva, il Gruppo di lavoro ex art. 29 ha preso in considerazione l'ipotesi della responsabilità degli utenti in rapporto alle disposizioni generali dell'ordinamento in materia civile e penale, come nel caso di diffamazione, responsabilità civile per danni alla persona, responsabilità penale, ecc., oltre all'inapplicabilità dell'eccezione nei casi in cui entrino in gioco "i diritti di terzi" (si v. infatti il § 3.1.3 dell'Opinione).

Tuttavia, fuoriusciamo in questo modo dal campo dei rapporti tra i prestatori di servizi e i loro utenti, per entrare nell'ambito della responsabilità, civile e penale, verso terzi. Come segnalato in precedenza, a proposito di gestori, direttori e sceriffi, si tratta certamente di uno dei temi più dibattuti e, purtroppo, controversi del principio di responsabilità giuridica in rete. Stante la sua autonomia, converrà discuterne a parte.

4.2.2. Sulla responsabilità verso terzi negli USA

Può essere utile introdurre l'analisi sulla responsabilità giuridica verso terzi per azioni (e omissioni) nel mondo di internet, prendendo spunto dall'ordinamento americano. Mentre, infatti, l'impressione è che in Europa e, per molti versi, soprattutto in Italia, predominino ancora dubbi o semplice confusione, il quadro generale che si può trarre invece dal diritto statunitense risulta piuttosto chiaro. Nonostante alcuni nodi irrisolti e problemi, su cui torno tra poco, vige la regola della assoluta immunità, per cui, ai sensi del *Communications Decency Act* (47 U.S.C., § 230), *nessun prestatore di servizi in rete o intermediario su internet può essere ritenuto responsabile per i danni arrecati dagli utenti del servizio.* La ragione che ha suggerito al Congresso di abbracciare senza dubbi di sorta il *principio di esenzione di responsabilità*, dipende dalla convinzione che solo questo principio sia in grado di promuovere e garantire alcuni diritti e libertà fondamentali: mi limito a segnalare tre punti essenziali.

In primo luogo, in omaggio alla tradizione costituzionale del *freedom of speech*, le Corti americane hanno interpretato l'art. 230 quale baluardo della protezione dei prestatori di servizi contro la responsabilità per fatto altrui, poiché lo scopo è "di incoraggiare lo sviluppo senza vincoli né regole della libertà di parola su internet"[6]. In questo modo viene eliminata alla radice la possibilità di concepire la responsabilità dei provider alla stregua della responsabilità oggettiva dei direttori di giornali, con gli inevitabili disincentivi che seguirebbero all'obbligo editoriale di controllare il materiale immesso nella rete, nei social forum, nei blog, ecc., dato che l'art. 230 ha per l'appunto lo scopo di esimere i prestatori di servizi dalla responsabilità "che segue all'esercizio delle tradizionali prerogative degli editori (…)

[6] Questo il giudizio della Corte d'Appello USA, nono circuito, in *Batzel v. Smith*, 333 F.3d 1018, 1027-28 (9th Cir. 2003).

nell'aver cura del materiale pubblicato"[7]. In caso contrario, non si avrebbe null'altro che "un'altra forma di intrusione del governo nella disciplina [della libertà] di parola"[8].

Secondariamente, il principio di esenzione di responsabilità, per il tramite dell'art. 230, rappresenta un elemento chiave per la promozione e supporto dell'innovazione in internet, grazie allo sviluppo di un proteiforme settore di servizi, social network, blog e finanche di commercio elettronico. Basti pensare a come eBay inviti i propri utenti a valutare le transazioni con gli altri utenti in rete, o al sito di Amazon in cui gli interessati possono esprimere il proprio giudizio sui prodotti acquistati in rete, da cui altri utenti traggono informazioni su quali prodotti eventualmente acquistare. Dai siti in cui il contenuto è prodotto dagli stessi utenti, come YouTube o Flickr, a social network come Facebook, MySpace o Twitter, a siti per l'informazione dei consumatori come Yelp, a motori di ricerca come Google o Yahoo!, a nessuno, negli Stati Uniti, verrebbe in mente di chiamarli in causa per i giudizi ivi espressi dagli utenti.

Infine, *last but not least*, il principio di esenzione di responsabilità favorisce la flessibilità che segue all'auto-disciplina in rete, che si attua mediante forme di *peer review*, come nei ricordati casi di eBay e Amazon, oppure attraverso il 'potere di veto' degli utenti sui video di YouTube, fino a quella straordinaria modalità di collaborazione distribuita offerta da Wikipedia. Si tratta senz'altro di uno degli aspetti più rilevanti e straordinari che connotano l'attualità d'internet e il Web 2.0, sul quale, giustamente, si è soffermata più volte l'attenzione degli studiosi (per tutti Benkler 2007).

Non di meno, come accennato in precedenza, esistono pur sempre eccezioni: l'immunità dell'art. 230, ad esempio, non esime dalla responsabilità il prestatore di servizi che abbia materialmente contribuito alla creazione del contenuto illecito immesso in rete o che abbia violato determinate disposizioni del diritto penale federale. Un discorso a parte meriterebbero poi le clausole di salvaguardia in tema di diritto d'autore: se, infatti, il *Digital Millennium Copyright Act* (17 U.S.C. § 512) prevede l'esenzione di responsabilità per tutti i fornitori di connettività in internet o per la memorizzazione di informazioni in cache, oltre ai motori di ricerca e ai siti i cui contenuti sono prodotti dagli stessi utenti, la medesima norma, tuttavia, contempla un meccanismo di rimozione dei contenuti che, non di rado, ha avuto effetti controproducenti. A richiesta dell'interessato – per lo più un privato, ossia il presunto titolare dei diritti d'autore violati con il caricamento di file audio o video in rete – i prestatori di servizi provvedono spesso a rimuovere *ut sic* i contenuti oggetto di controversia, ancor prima di sincerarsi della fondatezza delle lamentele. Basti pensare a quanto occorso durante la campagna presidenziale del 2008, allorché, su richiesta della CBS, Fox News, the Christian Broadcasting Network e la NBC, vennero ritirati alcuni video della campagna di Obama e del senatore McCain, caricati su YouTube. Del resto, come confermano *ad abundantiam* i ripetuti casi di Scientology, il rischio, spesso consumato, è che la disciplina dell'art. 512 venga utilizzata semplicemente per censurare idee e opinioni altrui, sulla base della semplice denuncia d'illecito da parte di un privato.

Nonostante la peculiarità della disciplina statunitense sul copyright e i conseguenti problemi sorti per la tutela della privacy dei naviganti in rete, il quadro generale rimane tuttavia inequivocabile. In linea di principio, in effetti, *sono gli utenti a rispondere per il contenuto illecito dei materiali immessi nella rete e per i danni eventualmente arrecati*. I prestatori di servizi, in altri termini, sono esenti da ogni responsabilità verso terzi, anche quando il diretto responsabile non sia rintracciabile o non sia in grado di risarcire adeguatamente il danneggiato. La ragione dipende dal fatto che, nel bilanciamento dei diversi interessi in gioco, prevale il principio della libera circolazione delle idee e dello sviluppo dei servizi e piattaforme nel Web 2.0, stante la scelta politica di *non prevenire* comportamenti illeciti in rete "imponendo responsabilità extra-contrattuale [*tort*] alle imprese che servono da intermediari per i messaggi potenzialmente nocivi di altre parti"[9].

Alla luce di quanto avviene al di là dell'Atlantico, quale, dunque, lo stato dell'arte in Europa?

4.2.3. La responsabilità verso terzi in Europa

---

7 Questa volta il giudizio è della Corte del quarto circuito in *Zeran v. America Online*, 129 F.3d 330 (4th Cir. 1997).

8 *Ibidem*.

9 Si v. ancora il caso *Zeran v. America Online*, 129 F.3d 330-331 (4th Cir. 1997).

Ho già rimarcato nella sezione dedicata a 'gestori, direttori e sceriffi' tanto le ragioni di principio quanto di stretto diritto, per cui ritengo che l'*esenzione di responsabilità vigente negli USA* per i prestatori di servizi in rete, *valga anche in Europa*. Ho infatti ricordato sia il parere del 18 gennaio 2005, in cui il Gruppo di lavoro ex art. 29, richiamandosi all'art. 15 della direttiva sul commercio elettronico (D-2000/31/CE), esclude un obbligo sistematico di sorveglianza e collaborazione in capo ai prestatori di servizi, sia il parere del 23 giugno 2008, in cui il Garante europeo (GEPD) ritiene che il controllo sul contenuto delle telecomunicazioni non dovrebbe essere esercitato, in linea di principio, dalle imprese.

A conferma della tesi, valga ora riportare il più recente giudizio del Gruppo ex art. 29, e cioè la più volte citata Opinione del 12 giugno 2009, in cui viene offerta una compiuta fenomenologia dei servizi di social network che, come detto più sopra (4.1.2), procede dalle questioni preliminari di competenza e giurisdizione (§ 3 dell'Opinione), e di chi debba essere considerato responsabile del trattamento (§ 3.1), per analizzare sistematicamente sia i temi della sicurezza e della configurazione del sistema (§ 3.2), sia l'informazione che i servizi di social network devono fornire agli utenti (§ 3.3), sia il regime dei dati sensibili (§ 3.4), fino al trattamento dei dati di coloro i quali non fanno parte del social network (§ 3.5) e l'accesso di "terze parti" (§ 3.6). Lasciando da parte gli ulteriori punti sulle questioni di marketing (§ 3.7), conservazione dei dati (§ 3.8), diritti degli utenti (§ 3.9) e il caso dei bambini e minorenni (§ 4), il quadro complessivo che se ne trae non lascia adito a dubbi. *In nessun caso* emerge, né potrebbe sorgere, *una responsabilità verso terzi in capo ai prestatori di servizi in rete*.

Da un lato, infatti, come già riferito (4.1.3), il Gruppo ex art. 29 sottolinea come il trattamento dei dati personali di chi non faccia parte di un determinato social network, non solo "manchi di basi legali", ma conduca finanche al paradosso per cui il responsabile del servizio che eventualmente decidesse di avvertire il diretto interessato sulla presenza di tali dati personali, finirebbe inopinatamente per incorrere nella violazione di quanto predisposto dall'art. 13.4 D-2002/58/CE.

D'altra parte, quando il Gruppo ex art. 29 mette a punto le varie obbligazioni che, stante la presenza dei terzi, gravano sul prestatore del servizio in rete, il richiamo va alla possibilità che il social network ha di offrire ai propri utenti ulteriori applicazioni e servizi predisposti da "terzi sviluppatori" (§ 3.6.1). In questo caso, i servizi di social network devono far sì da "assicurare che le applicazioni predisposte dai terzi [gli sviluppatori] soddisfino le direttive sulla tutela dei dati e la privacy elettronica (…) quanto implica, in particolare, che essi forniscano agli utenti un'informazione chiara e specifica sul trattamento dei loro dati personali e che soltanto essi abbiano accesso ai dati personali necessari" (*ib.*).

Ma c'è di più. Quando, infatti, il Gruppo ex art. 29 definisce i doveri d'informativa dei prestatori di servizi di social network (§ 3.3), esso "raccomanda" nello specifico tre cose.

Innanzitutto, i provider "devono avvertire adeguatamente gli utenti circa i rischi per la privacy che possono recare a sé *e agli altri quando caricano informazione* sul servizio di social network".

Quindi, "agli utenti dei servizi di social network deve essere ricordato che *caricando informazioni su altri individui essi possono violare la privacy di questi ultimi e i loro diritti alla tutela dei dati*".

Infine, i responsabili dei social network dovrebbero avvertire i loro utenti che "se essi desiderano caricare *foto o informazioni su altri individui, ciò deve avvenire con il consenso dell'interessato*".

Come ben si vede, l'obbligo del provider non è nei confronti del terzo che, eventualmente, sia stato danneggiato: l'obbligo è, piuttosto, d'informare adeguatamente il proprio utente sui rischi e le responsabilità cui va incontro, nel caricare nel sistema foto e informazioni di terzi. Tant'è vero che nel § 3.1.3 dell'Opinione, a proposito del "trattamento dei dati di terzi da parte degli utenti" e l'ipotesi dell'"eccezione domestica' di cui all'art. 3.2 D-95/46/CE (di cui sopra 4.2.1), il Gruppo di lavoro ex art. 29 afferma che se, per un verso, "l'applicazione dell'eccezione domestica è anche limitata dal bisogno di garantire i diritti dei terzi, particolarmente in rapporto ai dati sensibili", d'altro canto "dev'essere notato che anche qualora l'eccezione domestica si applichi, un utente può essere responsabile in ragione delle disposizioni generali delle leggi nazionali civili o penali in questione (come nel caso di diffamazione, responsabilità extra-contrattuale per danni alla persona, responsabilità penale)".

Giunti a questo punto, i diversi 'piani della responsabilità' dovrebbero per ciò essere chiariti: per amor di brevità, ne suggerisco i tre principali.

Il primo, anche in ordine cronologico, riguarda la responsabilità dei prestatori circa la sicurezza dei propri servizi nel trattare i dati degli utenti, con i doveri d'informativa sia sull'utilizzo di quei dati e la

possibile condivisione con categorie specifiche di terzi destinatari anche per finalità pubblicitarie, sia sui rischi e responsabilità cui gli utenti vanno incontro nel caso di caricamento in rete d'informazioni e dati relativi a terzi, ecc.

Il secondo piano riguarda invece le responsabilità degli utenti che, debitamente informati, abbiano tuttavia immesso contenuti illeciti nella rete: essi risponderanno dei danni eventualmente arrecati tanto in sede civile quanto in quella penale.

Infine, si avrà la responsabilità dei provider per fatto degli utenti solo quando, su richiesta delle autorità competenti, essi non si siano attivati per colpa o dolo. Secondo quanto prevede del resto l'art. 17.3 del D.L. n. 70 del 2003, con cui si è recepito in Italia l'art. 15 D-2000/31/CE, la responsabilità del prestatore scatta solo per non aver agito prontamente al fine di bloccare l'accesso a un dato contenuto e solo nel caso in cui fosse tenuto a farlo per legge. Scartato l'obbligo generale di vigilanza, rimane infatti la sola responsabilità che nasce per colpa (o dolo), e cioè quella di non aver prevenuto i danni (ulteriori) dipesi dalla propria inerzia.

In questo modo, secondo la formula cara alla Corte europea di giustizia, siamo finalmente in grado di definire "un opportuno bilanciamento tra i diversi diritti fondamentali protetti dall'ordinamento comunitario" (si v. infatti C-275/06, § 70).

5. Conclusioni

Abbiamo avuto modo di vedere nel corso dei paragrafi precedenti alcune delle novità tecnologiche con i relativi nodi giuridici sorti nel Web 2.0. Se, nell'era precedente del Web 1.0, la questione principale ruotava attorno alla necessità di determinare il regime dei dati che i soggetti inserivano nelle prime pagine web personalizzate, come nel caso Lindqvist deciso dalla Corte di giustizia europea il 6 novembre 2003 (C-101/01), nel Web 2.0, invece, i problemi dipendono dall'interattività del sistema. Basti ancora pensare all'aggregazione di dati immessi indipendentemente dagli utenti in rete e all'uso di dati commerciali per garantire l'applicazione della legge, fino ai temi di ordine generale sulle responsabilità dei prestatori di servizi e degli utenti che caricano, condividono, selezionano e rivedono senza mediazioni o filtri di sorta, informazioni, anche su terzi, in tempo reale.

La pletora di fattispecie altamente controverse, per di più in un settore per eccellenza in continua evoluzione, ha così consigliato di adottare una prospettiva di ampio respiro, fondata su principi, onde evitare il rischio di dover rincorrere la tecnologia sul suo terreno. È il duplice caso dei programmi di *data mining* o *profiling*, attraverso cui va mutando la nozione di dato personale, e delle nuove frontiere dell'*AmI* e del *computer clouding*, con i nuovi strumenti che presiedono allo stesso trattamento di quei dati e informazioni. Nella consapevolezza che i principi in gioco non sono di per sé in grado di risolvere univocamente la totalità delle nuove controversie, tali principi hanno tuttavia consentito di chiarire parte della loro peculiare specificità. I problemi della rete *non* sono infatti ri(con)ducibili ai tradizionali schematismi della dottrina o di certa giurisprudenza, come del resto è stato dimostrato *a contrario*, nel terzo paragrafo, per via analogica. Là dove l'immagine dello sceriffo si scontra con l'assenza di un obbligo generale di sorveglianza e collaborazione, a sua volta la figura del direttore di giornale è spiazzata dalla rivoluzionaria struttura 'molti-a-molti' propria del reticolo digitale. Ma che dire del gestore di autostrade?

In fondo, abbiamo appurato che, in alternativa al provider etico auspicato in svariati regimi totalitari, il prestatore di servizi in rete, al pari del gestore d'autostrade in occidente, non risponde in linea di principio per quanto fanno gli utenti (o gli automobilisti). Ciò si evince tanto dall'ordinamento statunitense quanto dalle direttive comunitarie sul commercio elettronico e la tutela dei dati personali, nelle opinioni del Gruppo ex art. 29 e del GEPD, per cui sono gli utenti, debitamente informati, a rispondere, al pari degli automobilisti, per gli eventuali danni arrecati nell'uso delle autostrade digitali o nel 'mondo reale'. Pretendere, infatti, il controllo preventivo sulle informazioni immesse in rete dagli utenti, condurrebbe alla paralisi o distruzione dell'intero sistema, violando per ciò stesso il principio di proporzionalità. Secondo quanto suggerito dal comitato dell'OCSE nel rapporto del 30 giugno 2009, l'unico modo per garantire un quadro istituzionale teso a promuovere lo sviluppo e l'innovazione in internet, non può che essere quello offerto dal principio di esenzione di responsabilità in capo ai prestatori dei servizi.

Tuttavia, sarei pronto a concedere al lettore poco convinto che anche il parallelismo con i gestori d'autostrade lasci il tempo che trova; e non solo, o non tanto, perché le informazioni che viaggiano sulle 'autostrade digitali' sono cosa ben diversa dalle informazioni che viaggiano insieme alle macchine nelle vere autostrade d'asfalto. In realtà, la ragione della differenza specifica dipende piuttosto dalla natura transnazionale e dall'ubiquità di internet, come attestano in fondo i problemi, gravi e tuttora aperti, relativi alle questioni di competenza e giurisdizione affrontate nel quarto paragrafo. Deve valere il principio di sovranità oppure, tutt'al contrario, la precedenza va accordata ai diritti fondamentali della persona che, storicamente, si sono sviluppati proprio in antitesi alla sovranità della ragion di stato? C'è qualche modo di evitare il paradosso cui è andato incontro il Gruppo ex art. 29, per cui, nel voler tutelare i diritti dei cittadini del mondo, si finisce per rivendicare una giurisdizione mondiale paneuropea?

Come detto, ritengo che la via maestra per risolvere i problemi di competenza connessi al nodo del consenso informato degli interessati, sia quella dell'elaborazione di un 'quadro globale' per la protezione dei dati sulla scia delle linee guida elaborate dall'ONU e dall'OCSE, parallelamente alla cooperazione con altri organismi internazionali e con accordi bilaterali o multilaterali tra i vari paesi.

Nondimeno, in attesa di definire le *regole* che accomunino le varie autostrade digitali del pianeta, rimane però fermo il *principio* di esenzione per il quale siamo in grado di stabilire i diversi piani della responsabilità. Questa è a ben vedere la condizione essenziale affinché le autostrade digitali siano disciplinate in accordo ai dettami di una società aperta e libera.

Riferimenti bibliografici

Alexy, R. (1986). *Theorie der Grundrechte*. Suhrkamp, Frankfurt am Main

Anderson, Ch. (2006). *The long tail: why the future of business is selling less of more*. Hyperion, New York

Benkler, Y. (2007), *La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta la libertà* [2006]. Tr. it. Egea, Milano

Berners-Lee, T. (1999). *Weaving the web: The original design and ultimate destiny of the world wide web by his inventor*. Harper, San Francisco

Bobbio, N. (1938). *L'analogia nella logica del diritto*. Istituto Giuridico, Torino

Dworkin, R. (1985). *A matter of principle*. Harvard University Press, Cambridge, Mass

Floridi, L. (2009). *Infosfera: etica e filosofia dell'informazione*. Giappichelli, Torino

Goldsmith, J. (1998). Against Cyberanarchy, *University of Chicago Law Review*, 65: 1199-1250

Habermas, J. (1995). *Fatti e norme. Contributi a una teoria discorsiva del diritto e della democrazia* (1992). Tr.it. Guerini, Milano

Hayek, F.A. (1999). *La società libera* (1960). Tr. it. Seam, Milano

Hut, P. (2009). *The limits of analogy*, in *What have you changed your mind about?*, a cura di J. Brockman. Harper, New York

Johnson, D.G. (1985). *Computer Ethics*, Prentice-Hall, Englewood Cliffs, NJ.

Kuner, Ch. (2003). *European data privacy law and online business*. Oxford University Press, Oxford-New York

Moor, J.H. (1985). What is Computer Ethics?, *Metaphilosophy* (numero speciale), 263-275

Lessig, L. (2002). *The future of ideas. The fate of the commons in a connected world* (2001), Vintage Books, New York

Pagallo, U. (2008). *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano

Popper, K.R. (1974). *La società aperta e i suoi nemici* (1945). Tr. it. Armando, Roma

Post, D. G. (2002). Against "Against Cyberspace", *Berkeley Technological Law Journal*, 17: 1365-1383

Ricolfi, M. (2009). Presentazione a *Copyright digitale: l'impatto delle nuove tecnologie tra economia e diritto*. Giappichelli, Torino

Warren, S., Brandeis, L. (1890). The Right to Privacy, *Harvard Law Review*, 14: 193-220