GIORGIO GIANNONE CODIGLIONE

INDIRIZZO IP, RETI WI-FI E RESPONSABILITÀ PER ILLECITI COMMESSI DA TERZI

SOMMARIO: 1. Sviluppo tecnologico e modalità di accesso ad internet: il problema della responsabilità per illeciti commessi da terzi. — 2. Reti *wireless* e responsabilità dei terzi in Germania: *Störerhaftung*, doveri di vigilanza e violazione del *copyright*. — 2.1. Indirizzi IP dinamici, attendibilità e memorizzazione. — 3. La Francia e la legge HADOPI: l'intervento del *Conseil Constitutionnel*. Il principio di *négligence caractérisée*. — 4. IP *addresses* and Wi-Fi *networks*: l'ir-responsabilità dell'intestatario nell'esperienza statunitense. — 5. Regno Unito: il caso *Media CAT*. — 6. Indirizzi IP e responsabilità dell'intestatario: il quadro normativo e l'orientamento della giurisprudenza italiana. — 6.1. Ipotesi ricostruttive: Codice della privacy e misure di sicurezza. — 6.2. (*Segue*) Art. 2051 c.c. e rapporto di custodia. — 7. Reti Wi-Fi « aperte » e responsabilità: l'interessante opinione di un giudice di merito e la innovativa disciplina finlandese. — 8. L'indirizzo IP nel dibattito comunitario. — 9. Soluzioni diverse per un problema attuale: quale bilanciamento?

1. Sviluppo tecnologico e modalità di accesso ad internet: il problema della responsabilità per illeciti commessi da terzi.

La fluidità e l'estrema velocità con cui le tecnologie si sviluppano attorno all'uomo creano non pochi problemi di carattere tecnico-giuridico agli interpreti impegnati nel continuo tentativo di rendere « calzanti », « funzionali » ed « efficaci », normative e regole giuridiche da applicare al mondo digitale[1].

Una delle questioni maggiormente attuali e controverse ha come oggetto l'individuazione del reale autore dell'illecito su internet ai fini della sua perseguibilità civile e/o penale.

I caratteri pregnanti di immaterialità e transnazionalità della rete infatti hanno reso sempre difficile e per certi versi « quasi » impossibile tale com-

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

[1] Si vedano ad esempio gli spunti di riflessione sollevati di recente da S. Sica-V. Zeno-Zencovich, *Legislazione, giurisprudenza e dottrina nel diritto dell'internet*, in questa *Rivista*, 2010, pp. 377-389 o ancora A. Bevere-V. Zeno-Zencovich, *La rete e il diritto sanzionatorio: una visione d'insieme*, in questa *Rivista*, 2011, p. 375 ss.

pito, basato fondamentalmente sulla ricerca di « tracce », dati ed informazioni tecniche riguardanti il terminale che ha avuto accesso alla rete, la modalità di accesso, il tempo dell'accesso al momento della commissione dell'illecito: informazioni di carattere totalmente tecnico, che sfuggono ad una uniforme interpretazione e regolamentazione giuridica.

Il riferimento primario è all'indirizzo IP (*Internet Protocol Address*), codice numerico associato ad ogni terminale collegato alla rete ai fini della sua identificazione: ogni singolo indirizzo IP può difatti corrispondere ad un *personal computer* collegato ad internet, ad un *tablet*, o ancora ad un *router* Wi-Fi[2].

Il primo quesito che nasce spontaneo dall'analisi del rapporto tra responsabilità e tracciabilità, illecito e utente, è il seguente:

— può un indirizzo IP, collegato al nome dell'intestatario della rete, essere considerato alla stregua di un dato personale[3] e dunque indizio sufficiente ai fini dell'imputabilità dell'intestatario della connessione internet[4]?

— E ancora, qualora si riuscisse a pervenire al nome dell'intestatario (non violando la privacy degli utenti), non sarebbe altresì necessaria la sussistenza di un nesso di causalità tra l'illecito commesso e l'identità del reale autore?

[2] Gli Indirizzi IP possono essere distinti in due differenti tipologie: indirizzi IP statici e dinamici. L'indirizzo IP statico è un indirizzo assegnato staticamente a un'interfaccia: esso non subisce modifiche nel tempo, neanche a seguito dello spegnimento del terminale al quale l'indirizzo è stato assegnato o della disconnessione dalla rete. L'indirizzo IP dinamico, invece, non è una sequenza di numeri fissa ma cambia ogni qualvolta si accede alla rete e viene assegnato in maniera casuale e automatica. Sulla « storia » del protocollo TCP/IP si rimanda tra gli altri a J. Ryan, *Storia di Internet e il futuro digitale*, Torino, 2011, p. 38 ss. Sul tema v. anche I.J. Lloyd, *Information Technology Law*, 6th edition, Oxford, 2011, p. 570 ss.

[3] Sulla natura dell'indirizzo IP si veda ad esempio l'opinione di G. Resta, *Diritti esclusivi e nuove figure immateriali*, Torino, 2010, p. 601 s., il quale afferma che « l'indirizzo IP è sicuramente un mero indirizzo elettronico, che svolge nel *web* l'analoga funzione svolta dal numero di telefono nella rete telefonica », con riferimento a T. Firenze, 29 giugno 2000, in questa *Rivista*, 2000, p. 672, annotata da P. Sammarco. Ancora un autore sostiene che « di fatto l'IP, nel traffico Internet, non è altro che la targa di una macchina della quale nulla sappiamo (...) del conducente », così F. Cajani, *Internet Protocol. Questioni operative in tema di investigazioni penali e riservatezza*, in *Dir. Internet*, 2008, 6, 545. Cfr. anche P. Menchetti, *Allocazione di* domain names, antitrust *ed autorità di regolazione: un approccio tradizionale*, in A. Sirotti Gaudenzi (a cura di), *Internet e diritto: problemi e soluzioni*, Bologna, 2001, p. 45 ss. e R. Bocchini, *La responsabilità extracontrattuale del* provider, in D. Valentino (a cura di), *Manuale di diritto dell'informatica*, Napoli, 2011 p. 146 s.

[4] Sul problema dell'identificazione dell'autore degli illeciti perpetrati « mediante internet » v. V. Zeno-Zencovich, *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su internet*, in questa *Rivista*, 1999, p. 103; G. Cassano, *Diritto dell'internet. Il sistema di tutele della persona*, Milano, 2005, p. 333 ss. e ancora G. Alpa (a cura di), *Computer e responsabilità civile*, Milano, 1985. Sulla contrapposizione tra diritto all'anonimato e principio di rintracciabilità del soggetto responsabile cfr. G.M. Riccio, *Anonimato e responsabilità in Internet*, in questa *Rivista*, 2000, p. 314; G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2008. Sul tema v. anche F. Di Ciommo, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line. *A proposito della sentenza Google/Vivi Down*, in questa *Rivista*, 2010, p. 829; B. Donato, *La responsabilità dell'operatore di sistemi telematici*, in questa *Rivista*, 1996, p. 135; S. Magni-M.S. Spolidoro, *La responsabilità degli operatori in « internet »: profili interni e internazionali*, in questa *Rivista*, 1997, p. 61.

Parallelamente a questo tema, si sviluppa l'ormai lampante problema delle connessioni *wireless* e della ancora più intricata questione etico-giuridica sul diritto di accesso ad internet.

Nell'ultimo decennio, i classici modem hanno lasciato il passo alla capillare diffusione della tecnologia *wireless*, capace di fornire connessione a più terminali e senza l'utilizzo di fili[5].

I *router wireless* vengono generalmente commercializzati forniti di sistemi di sicurezza basati su *password* numeriche modificabili dagli utenti che non dovrebbero, in teoria, permettere « intrusioni » per mano di sconosciuti non « autorizzati ».

Citando brevemente la pratica illecita del *wardriving*[6], che dimostra quanto « deboli » e facilmente penetrabili siano queste « barriere » di protezione, dall'altra parte è necessario segnalare come si stia diffondendo a macchia d'olio tra gli utenti della rete (soprattutto negli USA ma anche in Europa) una corrente « solidaristica », che sostiene la necessità di una condivisione « libera » della propria connessione internet a banda larga, non protetta da alcuna *password* e resa disponibile a chiunque ne fosse un interessato fruitore.

La corrente del « *free* Wi-Fi » trova il suo fondamento in quel pensiero che inquadra internet come un bene ormai indispensabile e imprescindibile per ogni uomo, considerato alla stregua di un diritto fondamentale[7]: quel « diritto di accesso ad internet'che anche in Italia è stato oggetto di autorevoli, rivoluzionarie e per certi versi provocatorie proposte, che hanno dato luogo ad interessanti dibattiti in dottrina e tra gli addetti ai lavori[8].

Il mettere a disposizione la propria connessione di tutti coloro che si trovano nel raggio di copertura del proprio *router* Wi-Fi, senza fini di lucro, diventa così il fulcro di un altro quesito e di un'altra importante riflessione di diritto attuale.

— Può l'intestatario di una connessione internet essere reputato responsabile per gli illeciti commessi da terzi che hanno fruito dell'accesso

[5] Si veda, ad esempio il quadro, seppur risalente, tracciato da L. ALBERTINI, *I contratti di accesso ad internet*, in *Giust. civ.*, 1997, 2, p. 95, il quale segnalava i primi fenomeni di *routing* legati alla diffusione delle linee LAN (*local area networks*) interaziendali.

[6] Il *wardriving* è un'attività con finalità tipicamente illecite che consiste nell'intercettare reti Wi-Fi, in automobile, in bicicletta o a piedi, con un laptop, solitamente abbinato ad un ricevitore GPS per individuare l'esatta posizione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un apposito sito web. Fonte: *http://www.wikipedia.it/*.

[7] Su questo argomento si rimanda ad alcune interessanti decisioni registratesi in Francia e in Germania, citate *infra sub* par. 3.

[8] Il riferimento primario è alla proposta, sollevata da Stefano Rodotà nel corso della terza edizione dell'Internet *Governance* Forum tenutosi a Roma presso la sede del CNR il 30 Novembre 2010, di apportare una modifica alla Carta Costituzionale italiana che riconosca ad ogni cittadino il diritto all'accesso ad internet, con l'introduzione dell'art. 21-*bis* per cui « tutti hanno eguale diritto di accedere alla Rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale ». Sul tema si veda ancora T.E. FROSINI, *Il diritto costituzionale di accesso a internet*, in *Riv. Aic.*, 1, 2011; P. PASSAGLIA, *Diritto di accesso a internet e giustizia costituzionale. Una (preliminare) indagine comparata*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad internet - Atti della tavola rotonda svolta nell'ambito dell'IGF Italia 2010* (Roma, 30 novembre 2010), Napoli, 2011 pp. 59-88; M. CUNIBERTI, *Nuove tecnologie e libertà della comunicazione, profili costituzionali e pubblicistici*, Milano, 2008, p. 20 ss. e ancora S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012.

alla rete, poiché non ha protetto il suo *router* con alcuna *password*, in violazione di un presunto dovere di diligenza e sorveglianza?

Seguendo queste direttrici, indirizzi IP e reti Wi-Fi diventano i protagonisti di alcune decisioni di diverso segno recentemente registratesi in tribunali di merito e Supreme Corti di diversi paesi, (dall'Italia alla Germania, dal Regno Unito agli Stati Uniti), fondendosi in un articolato percorso di riflessione sulla responsabilità per illecito commesso in internet da terzi.

2. Reti *wireless* e responsabilità dei terzi in Germania: *Störerhaftung*, doveri di vigilanza e violazione del *copyright*.

In Germania la questione ha catalizzato l'attenzione degli interpreti principalmente in relazione a due pronunce, per certi versi connesse tra loro.

Nella più recente, la Corte Costituzionale tedesca, con sentenza del Marzo 2012[9], ha richiamato l'attenzione sul tema della responsabilità per violazione di *copyright* in relazione al fenomeno del *file-sharing*.

Nel curioso caso di specie una *major* discografica aveva citato per violazione del diritto d'autore un agente di polizia membro di un nucleo di indagine contro la pirateria telematica, intestatario di una linea di accesso internet domestica.

Ritenuto responsabile dal *Landgericht* di Colonia[10], in realtà il materiale autore dell'illecito era un familiare adulto (il figlio ventenne della convivente), il quale, utilizzato l'accesso alla connessione internet domestica, aveva reso disponibili per il *download* circa 3749 *files*. Chiarito questo aspetto davanti ai giudici, la richiesta di risarcimento dei danni veniva ritirata dall'attore, ma restava ancora irrisolta la questione riguardante il pagamento delle spese legali, al quale in sede di appello era stato condannato il convenuto.

Il *Bundesverfassungsgericht* ha revocato la condanna nei confronti dell'agente di polizia, rinviandola all'*Oberlandesgericht* di Colonia[11], rilevando come i giudici di *Kalsruhe* abbiano illegittimamente respinto la richiesta formulata dall'imputato di proporre ricorso per « *Revision* » al *Bundesgerichtshof* (BGH), la Corte di ultima istanza nel sistema della giustizia ordinaria, al fine di favorire una pronuncia che affermasse un principio di diritto omogeneo.

Secondo la Corte Costituzionale l'accoglimento di detta richiesta, infatti, avrebbe dovuto operare obbligatoriamente, poiché la decisione del tribunale di revisione era necessaria nel caso di specie « ai fini dell'evoluzione del diritto o della garanzia dell'uniformità della giurisprudenza », conformemente al disposto del § 543, Abs. 2, Satz 2 del ZPO (*Zivilprozessordnung*).

Con questa illegittimo rifiuto inoltre, la Corte d'appello ha violato il § 101, Abs. 1, Satz 2 del *Grundgesetz*, sul diritto a un equo processo.

[9] BVerfG, 21 marzo 2012 - 1 BvR 2365/11, in *www.comparazionedirittocivile.it*, a cura di P. Stanzione.

[10] LG Köln, 24 novembre 2010 - 28 O 202/10.

[11] OLG Köln, 22 luglio 2011 - 6 U 208/10.

Apertis verbis, i giudici costituzionali hanno ribadito come la fattispecie descritta appaia ancora poco nitida nei suoi contorni e necessiterebbe pertanto, come legittimamente richiesto in sede di appello dall'intestatario della connessione « incriminata », di un rinvio al *Bundesgerichtshof* ai fini della pronuncia di un'auspicata sentenza « chiarificatrice ».

Infatti, ancora secondo la Corte, l'unica pronuncia da prendere in considerazione sul tema (una sentenza del BGH del 2010), affronta una fattispecie per certi versi diversa da quella in oggetto e pertanto non può essere in alcun modo generalizzata ed eretta a *leading case* attorno al quale far giostrare l'intera disciplina.

Nella pronuncia del 12 maggio 2010, « *Sommer unseres Lebens* »[12], si disponeva, nei confronti del titolare di una connessione internet W-Lan in uso nel proprio ufficio, l'emissione di un'ingiunzione a cessare le violazioni del diritto d'autore: l'8 settembre 2006 alle ore 18.38 un'utente con uno specifico indirizzo IP condivideva sulla piattaforma di *file-sharing* « *Emule* » la canzone « *Sommer unseres Lebens* ».

La già menzionata connessione W-Lan privata, associata all'indirizzo IP e intestata al convenuto era però stata utilizzata a sua insaputa da un terzo, ad ufficio chiuso e durante un periodo di ferie.

Il BGH, nel motivare la propria decisione, ha primariamente affermato che sussiste una presunzione di colpa a carico dell'intestatario della connessione internet la cui identità è associata all'indirizzo IP tracciato al momento della commissione dell'illecito, superabile però soddisfacendo un onere della prova secondario che dimostri come l'autore della violazione in questione sia stato una terza persona[13].

Tale presunzione dunque non è assoluta: confrontando la fattispecie in oggetto con un'altra pronuncia riguardante l'utilizzo improprio da parte di un terzo di un *account* eBay[14], i giudici del BGH hanno affermato che « un indirizzo IP non è paragonabile ad una funzione identificativa di un conto eBay », giungendo alla conclusione che l'indirizzo IP non fornisce informazioni attendibili sulla persona che in un particolare momento ha avuto accesso alla rete[15].

Rilevato come nel caso di specie le prove prodotte dal convenuto avessero ampiamente raggiunto tal fine, i giudici, esclusa a suo carico ogni ipotesi di intenzionalità e dunque il risarcimento del danno, hanno però in se-

[12] BGH, 12 maggio 2010 - I ZR 121/08, in *MIR*, 6, 2010.

[13] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Posto che un'opera protetta è stata resa accessibile al pubblico da un indirizzo IP assegnato al momento dei fatti ad una determinata persona, sussiste una presunzione semplice per cui egli venga reputato responsabile della violazione. Ciò si traduce in un onere della prova secondario a carico dell'intestatario che dovrà dimostrare che un altro soggetto ha realmente commesso la violazione (cfr. OLG Köln MMR 2010, 44, 45; GRUR-RR 2010, 173, 174). Tale onere secondario della prova è stato comunque soddisfatto dall'imputato avendo egli sostenuto — non contestato dal ricorrente — di trovarsi in vacanza al momento della violazione e ancora che il proprio PC sarebbe stato inaccessibile ai terzi poiché chiuso nella propria stanza d'ufficio ».

[14] BGH, 11 marzo 2009 - I ZR 114/06, in *MIR*, 5, 2009. Sul tema v. anche BGH, 11 maggio 2011 - VIII ZR 289/09, in *www.comparazionedirittocivile.it*, a cura di P. STANZIONE.

[15] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Gli indirizzi IP non forniscono quindi informazioni attendibili sulla persona che, in un particolare momento ha accesso ad una determinata connessione Internet ».

condo luogo fatto riferimento all'esistenza di un « ragionevole dovere di controllo » posto in capo all'intestatario della rete W-Lan[16].

In questo caso esso non sarebbe stato adempiuto correttamente, in collegamento alla circostanza di aver lasciato tale connessione accessibile ai terzi, integrando così un tipo di condotta volontaria e adeguatamente causale (*willentlich und adäquat kausal*), consistente nell'« omissione di misure di sicurezza sufficienti »[17] e idonea ad integrare un ipotesi di *Störerhaftung* (letteralmente responsabilità, o corresponsabilità del disturbatore/interferente[18]), punita con l'emissione di un'ingiunzione a « cessare e desistere » e la condanna al pagamento delle spese legali di notifica dell'avviso.

Nello specifico il *router wireless* non era stato lasciato completamente sprovvisto di *password*, ma la connessione era protetta dalla c.d. sequenza « madre », stabilita dal produttore (e in questo caso mai modificata dall'utente), consistente in una combinazione libera di sedici numeri stampata sul *router* stesso. Il grado di « sicurezza » celato dietro il mantenimento della *password* madre è molto basso: spesso le stesse case produttrici utilizzano medesime combinazioni applicandole a tutti i modelli di modem *wireless* della stessa serie o, ancora, le combinazioni possono essere dissimulate a distanza dal reale responsabile dell'illecito attraverso l'uso di alcuni *software* (facilmente reperibili in rete) che permettono di trovare le chiavi preimpostate di alcune marche di *router*.

Un altro importante dato che emerge dalla sentenza in analisi è il fatto che i proprietari di *router wireless* non potrebbero giovarsi delle eccezioni previste dal § 10, Satz 1 del TMG (*Telemediengesetz*) per gli « *host provider* »[19]: questa interpretazione, se confermata in futuro, senza dubbio potrebbe creare non pochi problemi a titolari di connessioni Wi-Fi private ma anche ad esercenti e titolari di internet-*cafè* e connessioni Wi-Fi *hotspot* gratuiti. L'unico limite prospettato in questa sede dai giudici del Bgh è connesso alla circostanza che tale tipo di attività di controllo preventivo possa gravare in termini negativi a livello economico, minacciando un modello di *business*[20].

[16] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Anche con riguardo ai privati che fanno uso di una connessione Internet WLAN non pare irragionevole il fatto che essi si sincerino che la connessione sia stata sufficientemente protetta con adeguate misure di sicurezza tali da salvaguardare la stessa da abusi e violazioni da parte di terzi. La ragionevolezza deriva dal fatto che molto spesso è nel miglior interesse del sottoscrittore mettere al sicuro i propri dati da interferenze non autorizzate provenienti dall'esterno. Adottare misure di sicurezza per la propria connessione WLAN al fine di evitare violazioni del diritto d'autore commesse da terzi non autorizzati può allo stesso modo essere considerato nell'interesse del sottoscrittore ».

[17] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Unterlassung ausreichender Sicherungsmaßnahmen ».

[18] Il principio di *Störerhaftung*, applicato di recente anche al mondo di Internet in numerose pronunce, trae origine da un concetto di responsabilità largamente diffuso e radicato nell'ordinamento tedesco, posto a protezione dei diritti assoluti ai sensi dei paragrafi 823 e 1004 del BGB. Secondo tali principi chiunque, senza esserne l'autore o un complice, abbia in qualche modo contribuito deliberatamente ed in maniera adeguatamente causale alla violazione di un diritto riconosciuto e protetto dall'ordinamento può essere soggetto ad un provvedimento ingiuntivo. V. A. HARTMANN, *Unterlassungsansprüche im Internet. Störerhaftung für nutzergenerierte Inhalte*, München 2009.

[19] L'art. 10 comma 1 rappresenta una fedele riproduzione dell'art. 14, lettera a) della direttiva 2000/31/CE sul commercio elettronico.

[20] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Questo non è un modello di business che potrebbe essere compromesso dall'imposizione di un obbligo preventivo di

Affermata pertanto l'esistenza di un ragionevole obbligo di protezione della propria connessione privata dall'uso da parte di terzi, il BGH ha indicato — ma con esclusivo riferimento al caso di specie — attraverso quale comportamento si dovrebbe configurare la condotta omissiva giuridicamente rilevante ai fini dell'imputazione della responsabilità in oggetto: non tanto il fatto di avere protetto (come quasi tutti gli utenti fanno d'altronde) il proprio *router* con una *password* a sedici numeri combinati casuahnente, ma piuttosto la circostanza di aver mantenuto la combinazione « madre » originaria e riportata fisicamente sopra il *router* stesso, non sostituendola con « una *password* sufficientemente lunga e sicura » al momento dell'acquisto e dell'avviamento dell'apparecchio; non munendolo in altre parole degli strumenti di sicurezza necessari[21].

Anche nella sentenza della Corte d'Appello di Colonia i giudici hanno condannato l'agente di polizia facendo riferimento ad un generico dovere di controllo[22], senza però specificare di quali adempimenti e misure esso possa constare e soprattutto se tali obblighi di controllo e monitoraggio siano altresì applicabili quando è un soggetto adulto a fruire della connessione domestica.

Inquadrati in un'ottica più ampia, i due casi descritti sembrano indirizzarsi verso l'affermazione di un generale dovere di ragionevole vigilanza e controllo in capo all'intestatario della connessione e dunque sull'esistenza di una presunzione di colpa a suo carico.

Ciò che non appare chiaro, anche alla luce della pronuncia in analisi del *Bundesverfassungsgericht*, è in che modo l'intestatario sia tenuto ad agire al fine di non incorrere in tale regime di responsabilità, sia con riguardo all'accesso di terzi « non autorizzato » alla propria connessione W-Lan, sia nel caso si tratti di un familiare « autorizzato » ad avere accesso alla connessione internet domestica: se è vero che nel caso di connessioni *wireless* potrebbe essere sufficiente crittografare il proprio *router* per impedire l'accesso a terzi non autorizzati (anche se come sottolineato sussistono anche su questo punto dubbi interpretativi di non poco conto[23]), parrebbe irrealizzabile e non « ragionevole » l'imposizione di un dovere di « con-

controllo (cfr. BGHZ 158, 236, 251 f. - Internet-Versteigerung I). Non sono inoltre valide le esenzioni da responsabilità di cui al § 10 TMG e all'Art. 14 f. della direttiva 2000/31/CE sul commercio elettronico, che nel caso dei prestatori di servizi *ex* § 10, Satz 1 TMG (Host Provider) escludono ogni ulteriore azione inibitoria. Il legittimo interesse di fruire di un accesso WLAN ad internet facile e flessibile, non è messo in discussione dal fatto di estendere anche ai privati uno standard di diligenza da attuare al momento dell'installazione del *router* WLAN al fine di contrastare l'uso non autorizzato da parte di terzi ».

[21] BGH, 12 maggio 2010 - I ZR 121/08, cit.: « Questo obbligo è stato contravvenuto dal convenuto. Egli infatti ha lasciato il collegamento del router WLAN con le impostazioni di sicurezza predefinite non assegnando per l'accesso al *router* una password personale, sufficientemente lunga e sicura ».

[22] Secondo i giudici della Corte d'Appello di Colonia infatti il proprietario della connessione internet non avrebbe soddisfatto l'onere probatorio previsto dallo *Störerhaftung*, in connessione alla violazione di un obbligo di vigilanza. Non sarebbe infatti stata ritenuta sufficiente la circostanza che l'intestatario avesse parlato in famiglia rimarcando il carattere illecito di condotte quali il *filesharing*. Cfr. OLG Köln, 22 luglio 2011 - 6 U 208/10.

[23] Si pensi, ad esempio, ad un utente non particolarmente esperto rispetto a tali procedure o, ancora a dei router che non permettano, durante la « prima installazione » una procedura (*wizard*) di modifica della *password* facile ed intuitiva.

trollo » diffuso o ancora di un « divieto » di accesso « autorizzato » ad internet nei confronti dei propri familiari[24].

2.1. *Indirizzi IP dinamici, attendibilità e memorizzazione.*

Nel dibattito sulla « natura » dell'indirizzo IP si sono invece inserite, succedendosi a pochi mesi di distanza le une dalle altre, alcune pronunce dei giudici del *Bundesgerichtshof* e ancora del *Bundesverfassungsgericht*.

Nel gennaio del 2011 il BGH[25] si è pronunciato affermando che agli ISP è consentito di memorizzare, ai sensi del § 100, Abs. 1 del TKG, l'indirizzo IP dinamico attribuito ad una connessione internet *flat*, anche se non sussiste nessun sospetto legato alla commissione di un illecito a carico dell'utente: è infatti sufficiente che sia in atto un guasto o un difetto che colpisca i sistemi di comunicazione, a patto che tale attività di *data retention* venga effettuata in maniera adeguata, necessaria e proporzionata e che non vada oltre un periodo massimo di sette giorni[26].

Secondo i giudici della Suprema Corte tedesca, infatti, la semplice memorizzazione di un indirizzo IP per un breve periodo di tempo non provoca nessun grave impatto sui diritti fondamentali degli utenti ed è compatibile con la normativa europea[27]; inoltre per risalire all'identità di ciascun utente sarebbe comunque necessario collegare l'indirizzo IP ad altri dati[28].

[24] Con specifico riferimento alla responsabilità dei genitori per violazione del *copyright* commessa dal figlio minore si è recentemente pronunciato ancora il *Bundesgerichtshof*. I giudici di Kalsruhe hanno affermato come i genitori non possano ritenersi responsabili indirettamente per gli illeciti in violazione del diritto d'autore commessi dal figlio minore in collegamento alla mancata osservanza del dovere di diligenza, controllo e supervisione sancito dal § 832 del BGB. Il BGH ha infatti osservato come il dovere di supervisione previsto dal Codice civile tedesco fosse stato ampiamente adempiuto, ritenendo sufficiente che gli stessi genitori avessero avvertito e istruito il « normalmente sviluppato » figlio tredicenne riguardo all'illiceità e ai rischi connessi a condotte quali il *downloading* di *files* musicali « pirata » o il *file-sharing* degli stessi. BGH, 12 novembre 2012, I ZR 74/12, « *Morpheus* ». Per un primo commento della vicenda, sia consentito rimandare a G. Giannone Codiglione, Copyright, *genitori e doveri di controllo sul figlio minore che naviga su internet*, in *Diritto Mercato Tecnologia*, a cura di A.M. Gambino (*www.dimt.it*).

[25] BGH, 13 gennaio 2011 - III ZR 146/10, in *JZ*, 13, 2011, pp. 691-696, con nota di T. Hoeren.

[26] Sul tema v. E. Falletti, *I diritti fondamentali su internet. Libertà di espressione*, privacy, copyright, Padova, 2011, pp. 78-82.

[27] Art. 15, par. 1, direttiva 2002/58/CE: « Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea ». Sul tema v. anche S. Sica-V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione*, 3ª ed., Padova, 2012.

[28] BGH, 13 gennaio 2011 - III ZR 146/10, cit.: « L'identità di ciascun utente non è deducibile unicamente dall'Indirizzo IP ma soltanto dal collegamento con altre informazioni ».

Alla luce di quanto *supra* appare però fuori di dubbio che qualora nel futuro non venissero rispettati i rigidi principi di proporzionalità ed adeguatezza sanciti in sede comunitaria il rischio di incorrere in « abusi » di vario genere potrebbe aumentare sensibilmente.

Alle conclusioni dei giudici del *Bundesgerichtshof* non sono invece pervenuti i giudici dell'OLG di Colonia[29], che hanno infatti dichiarato inammissibili le informazioni collegate a degli indirizzi IP di tipo dinamico, evidenziando le difficoltà di corretta identificazione connesse alla valutazione di dati di tale genere, soprattutto rispetto alla facilità e alla velocità con cui gli ISP assegnano nuovi indirizzi dinamici ai terminali, secondo la disponibilità di codici « liberi ».

Qualche mese dopo, il *Bundesverfassungsgericht*[30] ha affrontato nuovamente il problema dell'attendibilità dei dati connessi agli indirizzi IP dinamici ma sotto un altro punto di vista, concernente il giudizio di presunta incostituzionalità di alcune disposizioni di legge presenti nel TKG dedicate alla sicurezza e inerenti ai dati che possono essere richiesti dalle autorità di pubblica sicurezza e alle procedure di comunicazione dei dati raccolti.

In particolare, è stato considerato non conforme ai principi di segretezza delle comunicazioni e tutela della dignità umana (§ 1, Abs. 1 del *Grundgesetz*) il § 113, Abs. 1, Satz 2 del TKG: in applicazione della disposizione in oggetto infatti, a seguito di una prassi interpretativa « estensiva » della norma, venivano annoverati nell'insieme dei dati resi accessibili alle autorità giudiziarie per fini di sicurezza pubblica — oltre ai codici PIN e PUK, alle *password* e ai codici di accesso — anche gli indirizzi IP dinamici.

Con la sentenza citata la Corte ha richiamato l'attenzione del legislatore, ribadendo l'esigenza di apportare un ulteriore modifica che chiarisca la normativa in questione, invitandolo altresì a contemplare l'obbligatorietà dell'autorizzazione del giudice ai fini dell'ottenimento dei dati personali collegati all'intestatario della connessione corrispondente all'indirizzo IP dinamico, anche con riguardo ai procedimenti di carattere penale. Nell'attesa di questo intervento legislativo e alla luce di quanto disposto dalla Corte Costituzionale, non sarebbe pertanto consentita l'identificazione dell'utente associato ad un indirizzo IP « dinamico ».

3. La Francia e la legge HADOPI: l'intervento del *Conseil Constitutionnel*. Il principio di *négligence caractérisée*.

In Francia, un'importante apporto sul tema è stato offerto dal *Conseil Constitutionnel* con la decisione n. 580 del 10 giugno 2009[31], il quale, a se-

[29] OLG Köln, 10 febbraio 2011 - 6 W 5/11, in *MIR*, 2011, 022.

[30] BVerfG, 24 gennaio 2012 - 1 BvR 1299/05. La sentenza è rintracciabile all'url: *http://www.bverfg.de/*. Per un primo commento della pronuncia si rimanda a O. Pollicino, *Il Tribunale costituzionale tedesco alle prese con l'indirizzo IP*, in *www.diritto24.ilsole24ore.com* e A. Di Martino, *Dati relativi alle telecomunicazioni e sicurezza in una nuova pronuncia del BVerfG*, in *www.medialaws.eu*.

[31] Il testo della decisione è rintracciabile all'url: *http://www.conseil-constitutionnel.fr/decision. 42666.html/*. Per un commento si rimanda a V. Franceschelli, *Libertà in internet: per fortuna c'è la Corte Costituzionale francese!*, in *Riv. dir. ind.*, 2009, II, p. 404 ss..; P. Passaglia, *L'accesso ad internet è un diritto (il Conseil constitutionnel francese dichiara l'incostituzionalità di parte della c.d. « legge anti* file-sharing *»)*, in *Foro it.*, 2009, IV, 472 *m*); G. Votano, *Internet fra diritto*

guito delle censure di costituzionalità operate in quella sede, ha « obbligato » il legislatore francese a dover modificare la dibattuta legge HADOPI[32] che introduceva nuove disposizioni in tema di tutela proprietà intellettuale.

Ciò che rileva ai fini della presente trattazione sono due aspetti fondamentali: in primo luogo il Consiglio ha reputato incostituzionale il dettato normativo della legge in oggetto, nella parte in cui prevedeva un obbligo di vigilanza a carico dell'abbonato ad internet affinché la stessa connessione non venisse utilizzata per attività illecite, quali il *downloading* di *files* protetti da diritti di privativa[33]. Inoltre, la norma in oggetto prevedeva una sorta di inversione dell'onere della prova e dunque una presunzione di colpa a carico dello stesso abbonato, basato sull'equiparazione dell'indirizzo IP all'identificazione del reale responsabile dell'abuso[34].

Secondo i giudici del Consiglio, infatti, tale inversione della presunzione di innocenza a carico dell'abbonato avrebbe violato in primo luogo l'art. 9 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789[35].

L'indirizzo IP non è stato pertanto reputato strumento efficace e sicuro per l'identificazione del soggetto responsabile dell'illecito per cui « *è incostituzionale la previsione secondo cui il mero fatto che, utilizzando un indirizzo IP, siano stati posti in essere atti di contraffazione dà luogo ad una*

d'autore e libertà di comunicazione: il modello francese, in questa *Rivista*, 2009, p. 524 ss.

[32] La legge istituisce l'Alta Autorità per la diffusione delle opere e la protezione dei diritti su Internet (*Haute Autorité pour la Diffusion des OEuvres et la Protection des droits sur Internet*), per l'appunto HADOPI. Per un breve ma interessante commento della vicenda si rimanda a O. POLLICINO, *Tutela del diritto d'autore e protezione della libertà di espressione in chiave comparata*, in F. PIZZETTI (a cura di), *I diritti nella « rete » della rete*, Torino, 2012, pp. 110-113.

[33] L'art. 331-21 disponeva che, in seguito alla ricezione della segnalazione da parte dell'avente diritto sul contenuto scaricato illegalmente, l'Autorità amministrativa, dopo aver proceduto ad un accertamento dell'esistenza meramente fattuale dell'abuso, ne avrebbe attribuito la responsabilità al soggetto titolare della connessione corrispondente all'indirizzo IP utilizzato per il download illegale. Dopo l'invio di una e-mail di avvertimento successiva alla prima infrazione e una raccomandata dopo la seconda, alla terza infrazione riscontrata avrebbe operato il blocco della connessione internet per un periodo compreso tra i 3 e i 12 mesi. La presunzione di colpa a carico dell'abbonato era superabile: *a*) dimostrando di avere installato sul proprio computer, in data anteriore alla segnalazione dell'abuso, uno dei programmi contenuti in una lista citata al secondo comma dell'art. 331-32 della legge Hadopi; *b*) dimostrando che un uso fraudolento della propria connessione; *c*) dimostrando la forza maggiore.

[34] *Conseil Constitutionnel*, decisione n. 580 del 10 giugno 2009, par. 16: « Considerando che i poteri sanzionatori introdotti dalle eccepite disposizioni investono la Commissione per la protezione dei diritti, che non è organo giurisdizionale, del potere di limitare o impedire l'accesso ad internet nei confronti dei titolari di abbonamento, così come delle persone da questi autorizzate a beneficiarne; che la competenza riconosciuta a questa autorità amministrativa non è limitata ad una categoria particolare di persone, ma si estende alla totalità della popolazione; che i suoi poteri possono condurre a restringere l'esercizio del diritto di ogni persona di esprimersi e comunicare liberamente, in special modo dal proprio domicilio; che, in queste condizioni, avuto riguardo alla natura della libertà garantita dall'articolo 11 della Dichiarazione del 1789, il legislatore non avrebbe potuto, quali che siano le garanzie poste alla irrogazione di sanzioni, investire di simili potestà una autorità amministrativa con lo scopo di tutelare i diritti dei titolari del diritto d'autore e dei diritti connessi ».

[35] « Presumendosi innocente ogni uomo sino a quando non sia stato colpevole, se si ritiene indispensabile arrestarlo, ogni rigore non necessario per assicurarsi della sua persona deve essere severamente represso dalla legge ».

sanzione per omessa vigilanza a carico del titolare dell'indirizzo, esclusa solo subordinatamente alla prova della sussistenza di una causa di esonero da responsabilità ».

Un secondo aspetto di lampante interesse è l'implicito riconoscimento del diritto di accesso alla rete quale diritto fondamentale[36] accostato al diritto di libertà di espressione ed opinione e sollevato contestualmente alla censura effettuata nella parte in cui la legge HADOPI prevedeva il blocco della connessione internet a carico degli utenti rei di aver commesso delle violazioni *on-line* del diritto d'autore[37].

A seguito dell'intervento del *Conseil Constitutionnel* la legge è stata rimodellata, ribattezzata HADOPI2 e privata delle parti reputate non conformi alla costituzione: inoltre lo strumento della sospensione della connessione internet è stato subordinato all'intervento dell'autorità giurisdizionale e non di quella amministrativa, delegando pertanto tale compito all'attività valutativa e di bilanciamento degli interessi in gioco svolta caso per caso dal giudice.

Il primo (e ad oggi) ultimo caso di condanna per violazione della legge dei « tre avvertimenti » è stata pronunciata dal *Tribunal de police* di Belfort a carico dell'intestatario di una connessione internet, reo di non aver protetto adeguatamente il proprio *account*[38]. L'uomo infatti, condannato al pagamento di un'ammenda, aveva ammesso di non aver protetto con alcuna *password* il proprio *router* Wi-Fi, permettendo alla ex moglie di « scaricare » *files* protetti da diritti di privativa. Nonostante le espresse ammissioni della ex moglie, comparsa in aula insieme al marito e reale autrice dell'illecito, il soggetto ad essere condannato è stato l'intestatario della connessione, in applicazione della nozione di « *négligence caractérisée* » introdotta dalla legge HADOPI[39].

[36] Così O. POLLICINO, *Tutela del diritto d'autore e protezione della libertà di espressione in chiave comparata*, cit., p. 112. Recentemente anche in Germania, seppur in seno ad una diverse vicenda, è stato affermato dal Bundesgerichtshof la sussistenza di un « diritto » a poter fruire di una connessione ad internet senza interruzioni, inquadrato quale « servizio primario » — alla stregua di acqua e luce — poiché considerato un « media essenziale per la vita della società tedesca ». V. BGH, 24 gennaio 2013 - III ZR 98/12.

[37] *Conseil Constitutionnel*, decisione n. 580 del 10 giugno 2009, par. 12: « Considerando che in conformità all'articolo 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789: "La libera comunicazione dei pensieri e delle opinioni è uno dei diritti più preziosi dell'uomo: tutti i cittadini possono dunque parlare, scrivere, stampare liberamente, salvo a rispondere dell'abuso di questa libertà nei casi determinati dalla Legge"; che con riferimento allo stato attuale dei mezzi di comunicazione e posto il generale sviluppo dei servizi di comunicazione *on-line* al pubblico e l'importanza che questi ultimi ricoprono nella partecipazione alla vita democratica e della libera espressione delle proprie idee ed opinioni, questo diritto presuppone la libertà di accedere a tali servizi ».

[38] Il caso è richiamato da M.C. GOUPIL, *Un réseau Wi-Fi sécurisé l'est-il vraiment?*, in *www.medialaws.eu*.

[39] V. M. IMBERT-QUARETTA-J.Y. MONFORT-J.B. CARPENTIER, *La contravention de négligence caractérisée à la lumière de la mise en oeuvre de la procédure de réponse graduée*, in *La Semaine Juridique*, Edition Générale n. 19, 7 Mai 2012, p. 591. Secondo gli Autori, membri della « *Commission de la protection des droits* », tale forma di negligenza si concreterebbe nella colpa omissiva, consistente nel non aver rispettato l'obbligo di protezione del proprio accesso ad internet, quando tale omissione porta al raggiungimento di un preciso fine, ovvero l'utilizzo di quel punto di accesso per commettere violazioni del diritto d'autore ». V. anche TUNC, *La responsabilité civile*, Parigi, 1989.

Secondo questo principio, nel caso di difficoltà nella reale individuazione dell'autore della violazione di *copyright*, verrebbe reputato responsabile colui che, venendo meno all'obbligo di proteggere la propria connessione internet, permetterebbe in questo modo lo sfruttamento del proprio punto di accesso al fine di raggiungere uno specifico risultato, ovvero la commissione di illeciti in violazione del diritto d'autore: in altri termini, il riferimento sarebbe ad una ipotesi di c.d. «*faute d'omission*», colpa omissiva[40].

A distanza di tre anni dalla sua entrata in vigore, la legge HADOPI pare essere giunta già al tramonto: reputata troppo costosa e poco efficiente dal nuovo governo francese, potrebbe essere presto abolita, con annessa chiusura dell'omonima Autorità, come dichiarato dal Presidente della Repubblica François Hollande[41]. A conferma degli scarsi risultati ottenuti dall'applicazione di tale normativa, giungono i dati contenuti nel rapporto sull'attività svolta negli ultimi due anni, reso recentemente pubblico dalla stessa Alta autorità per la diffusione delle opere e la protezione dei diritti su internet[42].

4. IP *addresses* and Wi-Fi *networks*: l'ir-responsabilità dell'intestatario nell'esperienza statunitense.

Negli Stati Uniti, il problema delle reti Wi-Fi libere è esploso negli ultimi anni in maniera prorompente. Da un lato, numerosi studi legali attuano una strategia di «aggressione» con l'invio di migliaia di lettere d'ingiunzione ad intestatari («presunti pirati») di connessioni internet, contenenti la «minaccia» di adire le vie legali, o ancora implicitamente di arrecare agli stessi pubbliche umiliazioni (ad esempio attraverso la divulgazione di *files* pornografici scaricati illegalmente dagli utenti «incriminati») qualora non venissero accettate le richieste di pagamento di somme di danaro ai fini della composizione bonaria della lite[43].

Dall'altra parte, parallelamente all'evidente e consapevole diffusione delle connessioni Wi-Fi «aperte», altri addetti ai lavori affermano che non si possa in alcun modo sostenere l'esistenza di un principio di responsabilità presunta in capo agli intestatari legata alla mancata o inadeguata protezione del proprio *hotspot*[44]: a sostegno di questa affermazione, non sarebbe applicabile un principio di negligenza[45] (sostenuto *a contrario* da al-

[40] Sul tema si rimanda a G. Alpa (a cura di), *La responsabilità civile. Parte generale*, Torino, 2010, pp. 66-77.

[41] V. ad esempio all'articolo apparso qualche mese fa su «Le Figaro»: *http://www.lefigaro.fr/politique/2012/01/19/01002-20120119ARTFIG00610-francois-hollande-veut-supprimer-hadopi.php/*.

[42] La sintesi della relazione, tenutasi il 5 settembre 2012, è reperibile all'url: *http://www.hadopi.fr/sites/default/files/page/pdf/Point_presse.pdf/*.

[43] In merito si rimanda alla azione civile avente ad oggetto la violazione del copyright che si sta svolgendo presso la Corte distrettuale di New York, in cui la parte attrice è la *Liberty Media Holdings*, un'azienda che opera nell'ambito della pornografia e i convenuti sono 50 utenti del *Massachusetts* individuati soltanto attraverso il loro indirizzo IP, molti dei quali accusati di non aver protetto, integrando una condotta negligente, la propria connessione *wireless*. La cronistoria aggiornata del caso, corredata degli atti giudiziari, è rintracciabile all'url: http:// *www.citmedialaw.org/threats/liberty-media-holdings-v-john-does/*.

[44] Interessante a questo proposito è l'analisi dell'avvocato statunitense N. Ranalla, *Are You Guilty If Pirates Use Your Internet? Lawyer Says NO*, in *torrentfreak.com*.

[45] Sulla figura in generale del *tort of ne-*

tri[46]) all'interno del sistema di imputazione del *copyright*, fondato essenzialmente sulla tripartizione in *direct*, *contributory* e *vicarious liability*[47].

Con riferimento alla « teoria della negligenza », per cui se « Tizio è a conoscenza del fatto che Caio sta commettendo un crimine con il suo *account* internet e continua a permetterne l'uso, Tizio è negligente »[48], il giudice Lewis A. Kaplan della Corte distrettuale di New York, in una « *memorandum opinion* »[49] sul caso « *Liberty Media Holdings* » (citato *supra* in nota) ha manifestato tutti i suoi dubbi, reputando non convincente il postulato della negligenza formulato dalla parte attrice.

A sostegno di questa posizione, egli ha inoltre ricordato come sia già valida e operativa, a tal uopo, all'interno della legislazione sul *copyright*, la figura della responsabilità indiretta per *contributory infringment*, per cui un soggetto viene reputato responsabile per concorso in violazione delle norme sul diritto d'autore qualora, essendo a conoscenza dell'attività illecita, induca, causi o contribuisca materialmente alla condotta illecita di un altro soggetto[50].

Tornando alle teorie sull'irresponsabilità dell'intestatario, si sostiene invece che i proprietari di *networks* « *open* Wi-Fi » andrebbero considerati alla stregua di ISP « *mere conduit* »[51] e dovrebbero fruire pertanto del « *safe harbor* » previsto dall'art. 512 *a*) del DMCA (*Digital Millenium Copyright Act*)[52] in favore di tutti quegli intermediari che sono meri trasmet-

gligence e sui suoi elementi costitutivi si rimanda a P. GALLO, *Negligence*, in *Dig. disc. priv.*, sez. civ., XII, Torino, 1995, p. 23.

[46] V. M. RANDAZZA, *Are You Guilty If Pirates Use Your Internet? Lawyer Says YES*, in *torrentfreak.com*.

[47] Cfr. J.G. FLEMING, *The Law of Torts*, 7th ed., Sidney, 1987, p. 339, S.M. SPEISER-C.F. KRAUSE-A.W. GANS, *The American Law of Torts*, New York - San Francisco, 1983, p. 532; P.S. ATIYAH, *Accidents, Compensation and the Law*, London, 1970, p. 43 e s.

[48] Tale postulato si baserebbe su una pronuncia del 1932, il « *Tugboat Case* »: *Eastern Transportation Co. (The T.J. Hooper)*, 60 F.2d 737 (2d Cir. 1932), in cui si fa riferimento all'affermata negligenza degli operatori di alcune chiatte per trasporto merci che, secondo i giudici dell'epoca, non si erano muniti di apparecchi radio per comunicare con l'equipaggio dei rimorchiatori che li trainavano, circostanza che avrebbe permesso di tenerli informati sulle cattive condizioni metereologiche. Sul tema si veda I.J. LLOYD, *Information Technology Law*, cit., pp. 524-528 e C. TAPPER, *Computer Law*, London, 1989.

[49] Il documento è reperibile all'url: *https://www.eff.org/sites/default/files/Tabora%20Dismissal%20Order.pdf*.

[50] Cfr. *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2001); *Universal Pictures Co. v. Harold Lloyd Corp.*, 162 F.2d 354, 366 (9th Cir. 1947); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936-37 (2005). Sul tema si rimanda anche a G.M. RICCIO, *La responsabilità civile degli internet* providers, Torino, 2002, p. 57 ss.; L. NIVARRA, *Dolo colpa e buona fede nel sistema delle « Sanzioni » a tutela della proprietà intellettuale*, in *Quaderni di AIDA*, 6, 2001, p. 137 ss., o ancora L. NIVARRA-V. RICCIUTO, *Internet e il diritto dei privati*, Torino, 2002.

[51] Sulla categoria di ISP investiti dell'attività del « semplice trasporto » di dati si rimanda anche a S. SICA, *Le responsabilità civili*, in E. TOSI (a cura di), *Commercio elettronico e servizi della società dell'informazione*, Milano, 2003, p. 127 ss.; G.M. RICCIO, *La responsabilità degli internet* service provider. *Situazione legislativa e problemi aperti*, in V. D'ANTONIO-S. VIGLIAR (a cura di), *Studi di Diritto della comunicazione*, Padova, 2009, p. 157 ss.; P. SANNA, *Il regime di responsabilità dei* providers *intermediari di servizi della società dell'informazione*, in *Resp. civ. prev.*, 2004, I, p. 279.

[52] 17 USC § 512, (Limitations on liability relating to material online): « *a*) A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmit-

titori di informazioni fornite da un destinatario del servizio su una rete di comunicazione o forniscono un accesso alla rete di comunicazione, a condizione che le informazioni trasmesse rimangano inunutate: dando seguito a questa ipotesi non sarebbe pertanto prospettabile a carico degli stessi, poiché « meri vettori » di segnale, alcun obbligo preventivo di controllo e monitoraggio della propria connessione internet.

In giurisprudenza, si registra una tendenza attuale la quale nega che il solo indirizzo IP possa costituire una prova sufficiente ai fini di reputare colpevole l'intestatario per illeciti commessi su internet[53].

In *K-Beech Inc. v. John Does*[54], il giudice Gary Brown ha affermato che l'indirizzo IP non identifica il responsabile della condotta illecita poiché esso « fornisce soltanto l'esatta localizzazione del computer, così come un numero di telefono può essere utilizzato contemporaneamente da una serie di terminali »[55].

Tale paragone calza a pennello anche nel caso dei *routers* Wi-Fi: come affermato dallo stesso giudice, il 61% per cento degli americani utilizza le reti *wireless* e se queste non sono state rese sufficientemente sicure (o a volte anche qualora esse lo siano) « vicini o passanti possono accedere ad internet utilizzando l'indirizzo IP assegnato ad un preciso abbonato »[56].

ting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if:

1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content ».

[53] Tra i primi casi sul tema si segnala il procedimento *Viacom c. Youtube*, nel quale un giudice distrettuale ha affermato che nella maggior parte dei casi un indirizzo IP, non collegato ad informazioni addizionali, non permette in alcun modo di identificare un individuo. S.D.N.Y, *Viacom International, Inc. v. YouTube, Inc.*, No. 07 Civ. 2103. Per una prima analisi del caso v. R. VERSTEEG, *Viacom v. YouTube: Preliminary Observations*, in *North Carolina Journal of Law and Technology*, Volume 9, Issue 1, Fall 2007, p. 43 ss.

[54] *K-Beech, Inc. v. John Does*, 1-37 CV 11-3995 (E.D.N.Y 2012), in *Diritto mercato e tecnologia*.

[55] *K-Beech, Inc. v. John Does*, cit.: « The Use of IP Address to Identify the Alleged Infringers The complaints assert that the defendants — identified only by IP address — were the individuals who downloaded the subject "work" and participated in the BitTorrent swarm. However, the assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time. An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones. As one introductory guide states ».

[56] *K-Beech, Inc. v. John Does*, cit.: « Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular

Ancora di recente, un giudice federale dell'Illinois ha stabilito che non sussiste *a priori* una connessione diretta tra gli autori della violazione del *copyright* e l'indirizzo IP: « se l'indirizzo IP può identificare il nome dell'abbonato e il suo indirizzo, la correlazione è comunque lontana dalla perfezione », « l'autore potrebbe essere l'abbonato, qualcuno presente nella sua casa, un ospite col suo computer portatile, un vicino, o qualcuno parcheggiato sulla strada in qualunque momento »[57].

Un'altra pronuncia contraria alla teoria della *negligence*, in questo caso accostata al profilo della responsabilità dei possessori di router Wi-Fi non protetti si è invece registrata nel *Northern District of California*. Il giudice ha escluso la sussistenza di una presunzione di responsabilità a carico dell'intestatario di una connessione *wireless* non protetta, né un generale dovere di protezione e prevenzione da fattispecie di *copyright infringement*, insomma alcun *duty of care* posto in capo al soggetto titolare della connessione, come previsto nei casi di « *non-feaseance* »[58] ed escluso che tra le due parti sussista un « legame speciale » che giustifichi la validità di un tale obbligo agendo come eccezione alla regola principale[59].

Infine, dalla lettura di un'altra pronuncia del 2009, si evincerebbe un implicito riferimento all'utilizzo di un *router wireless* quale potenziale « difesa » utilizzabile dall'utente al fine di non incorrere in ipotesi di responsabilità per illecito commesso in rete. Essa si basa sull'assunto che solo adoperando tali tecnologie si potrebbe addurre a propria discolpa la circo-

subscriber and download the plaintiff's film ».

[57] *VPR Internationale* v. *Does* 1-1017, CV 11-2068 (D. Illinois 2011)

[58] In *Common Law* si distingue tra *Nonfeasance* e *Misfeasace*: se nel primo caso non ci si trova di fronte ad ipotesi di responsabilità, poiché non vengono contemplate le ipotesi in cui il danno scaturisca da un omissione, un « non fare » (« non esiste alcun obbligo imposto dalla legge a comportarsi come un buon Samaritano »), eccetto qualora non sussista una « *special relationship* » tra il danneggiato e il danneggiante (ad es. un rapporto di parentela); dall'altra parte, si incorre in responsabilità se il danno nasce da un'azione posta in essere « uncaressely », imprudentemente e dunque senza la dovuta diligenza. Per la giurisprudenza Britannica cfr. Stovin v Wise [1996] 3 WLR 389 e per quella Statunitense Yania v. Bigan, 155 A.2d 343 (Penn. 1959). Sul tema v. anche P. BENSON, *Misfeasance as an organizing normative idea in Private Law*, in *University of Toronto Law Journal*, Volume 60, Number 3, Summer 2010; E.J. KIONKA, *Torts in a Nutshell*, 3d ed., St. Paul, Minn., 1999; J. E. ROWE-T. SILVER, *The Jurisprudence of Action and Inaction in the Law of Tort: Solving the Puzzle of Nonfeasance and Misfeasance from the Fifteenth Through the Twentieth Centuries*, in *Duquesne Law Review*, 33 (summer), 1995 e ancora B.S. MARKESINIS, *Tort Law*, Oxford, 1984, e J.G. FLEMING, *The Law of Torts*, Londra, 1983.

[59] *AF Holdings v. Josh Hatfield and J. Doe*, C 12-2049 PJH (N.D. California 2012): « A defendant has no duty in situations of "non-feasance" unless a "special relationship" exists which would give rise to such duty. [...] AF Holdings has not articulated any basis for imposing on Hatfield a legal duty to prevent the infringement of AF Holdings' copyrighted works, and the court is aware of none. Hatfield is not alleged to have any special relationship with AF Holdings that would give rise to a duty to protect AF Holdings' copyrights, and is also not alleged to have engaged in any misfeasance by which he created a risk of peril. The allegations in the complaint are general assertions that in failing to take action to "secure" access to his Internet connection, Hatfield failed to protect AF Holdings from harm. Thus, the complaint plainly alleges that Hatfield's supposed liability is based on his failure to take particular actions, and not on the taking of any affirmative actions. This allegation of non-feasance cannot support a claim of negligence in the absence of facts showing the existence of a special relationship ». Il testo integrale del provvedimento è rintracciabile all'URL: *https://www.eff.org/sites/default/files/Order%20Granting%20MOTD.pdf*.

stanza che qualcuno possa aver « violato » o « sdoppiato » il proprio *account* internet sfruttando un punto di accesso *wireless* non protetto[60].

5. Regno Unito: il caso *Media CAT*.

Nel Regno Unito molto scalpore hanno destato le azioni avviate da alcuni importanti studi legali dell'isola avverso i presunti autori di violazioni del *copyright*, perpetrate per mezzo di piattaforme di scambio di *files peer-to-peer*.

A questo proposito, in *Media CAT c. Adams & Ors*[61], i legali dei titolari di diritti di privativa avevano richiesto e ottenuto, in conformità alla *Norwich Pharmacal jurisdiction*[62], che venisse ingiunto agli ISP di fornire i nominativi di 26 utenti, da associare agli indirizzi IP precedentemente tracciati e raccolti.

Ottenuti quindi i nominativi degli abbonati, i legali della *Media CAT* recapitavano agli stessi mezzo posta delle lettere di avviso, con le quali si proponevano transazioni pecuniarie al fine di comporre bonariamente le controversie, non perseguendo giudizialmente le presunte condotte illecite. Per ogni singola infrazione registrata a carico dell'indirizzo IP collegato al nominativo dell'abbonato veniva richiesta una somma di 495 sterline a titolo di parziale risarcimento per il danno subito, nonché di rimborso delle spese legali.

La questione, poi giunta innanzi alla *Patents County Court* ha visto il giudice Birss in via preliminare stigmatizzare il possibile carattere ingannevole di siffatte procedure e rigettare inoltre la successiva richiesta di risarcimento formulata dalla *Media CAT* nei confronti dei titolari degli IP associati ai *files torrent* « incriminati » e consistente nel pagamento di una somma pari a 550 sterline per ogni singola infrazione riscontrata.

I motivi della decisione in oggetto traggono primariamente spunto dalla constatazione che un indirizzo IP non può in alcun modo essere utilizzato quale prova sufficiente per l'imputazione della responsabilità: non sussiste nessuna evidenza che gli intestatari di una connessione abbiano commesso l'illecito, anzi è molto probabile che esso sia stato perpetrato da un terzo

[60] *Capitol Records Inc. v. Thomas-Rasset* 2009 WL 1664468, 7 (D.Minn. 2009). Si vedano anche *Arista Records, Inc. v. Musemeci* 2007 WL 3124545, 5 (E.D.N.Y., 2007) e *Motown Record Co., LP v. DePietro* 2007 WL 576284, 2 (E.D.Pa., 2007).

[61] *Media CAT v. Adams* EWPCC 6, [2011] FSR 28: « Therefore, given the evidence that there is no wireless router involved in this case, the Court excludes Kim's opinion that it is possible that someone could have spoofed or hijacked Defendant's Internet account through an unprotected wireless access point. Similarly, because Kim explicitly testified that this case does not involve any "black IP space," or any "temporarily unused" IP space (Kim Dep. 110-11), he is not permitted to opine at trial that hijacking of black IP space or temporary unused IP is a possible explanation in this case ». Sul tema v. G. Moss, *Media CAT v Adams: the CAT that did not get the cream*, in *Journal of Intellectual Property Law & Practice*, 2011, pp. 1-8.

[62] *Norwich Pharmacal Co. & Others v Customs and Excise Commissioners* [1974] AC 133. In questo caso venne disposto un *disclosure order* nei confronti di terzi non responsabili, che permettesse alle parti lese di venire a conoscenza dei nomi e degli indirizzi dei soggetti che importavano nel Regno Unito medicinali violando un brevetto. V. T. Aplin-J. Davis, *Intellectual property law*, Oxford, 2011, p. 796 ss.

autorizzato o da un *hacker* che ha illegalmente fruito della connessione stessa[63].

Un altro punto della motivazione della sentenza confuta le tesi addotte dai legali della *Media CAT* riguardanti il contenuto delle missive di avviso spedite agli utenti. All'interno delle stesse, infatti, si faceva « velatamente » intendere che permettere ad un terzo di connettersi alla propria rete, o ancora lasciare « non sufficientemente protetto » il proprio *router wireless*, significava incorrere in una fattispecie di responsabilità, basata sull'assunto che permettere, « *allow* » equivarrebbe ad autorizzare, « *authorize* »[64].

Secondo il giudice Birss invece, « permettere » ad un terzo di fruire di una connessione internet non vorrebbe necessariamente dire « autorizzarlo » a commettere illeciti in rete: il tema della presente trattazione si arricchisce ancora di un altro piccolo tassello giuridico-terminologico, che svela le innumerevoli difficoltà di venire a capo di un problema così complicato e di difficile comprensione, nel quale spesso i « muscoli » e le risorse economiche di società e legali senza scrupoli sfruttano lo strumento legale per perseguire i propri fini, ai danni di ignari e poco consapevoli utenti « vittime » di lettere imprecise e fuorvianti e spesso costretti a pagare per il timore di vedere lesa e irrimediabilmente compromessa la propria reputazione.

6. Indirizzi IP e responsabilità dell'intestatario: il quadro normativo e l'orientamento della giurisprudenza italiana.

In Italia il dibattito sul *wireless* « libero » si è riacceso in seguito all'entrata in vigore, nel gennaio del 2011, del nuovo quadro normativo che ha parzialmente modificato la disciplina introdotta dal decreto legge 27 luglio 2005 n. 144 (c.d. « decreto Pisanu »).

63 *Media CAT v. Adams*, cit.: « This question of unsecured internet connections and infringing by "allowing others" is a critical one since Media CAT's monitoring exercise cannot and does not purport to identify the individual who actually did anything. All the IP address identifies is an internet connection, which is likely today to be a wireless home broadband router. All Media CAT's monitoring can identify is the person who has the contract with their ISP to have internet access. Assuming a case in Media CAT's favour that the IP address is indeed linked to wholesale infringements of the copyright in question (like the *Polydor* case (above)), Media CAT do not know who did it and know that they do not know who did it. The Particulars of Claim are pleaded in a way to address a problem which is very old and very well known in intellectual property cases (see e.g. *The Saccharin Corp v Haines* (1898) 15 RPC 344). There the patentee had patents on all known methods of making saccharin and so, even though the patentee did not know how it was made, the defendant's saccharin must be infringing one way or another. Such saccharin type points arise frequently when a claimant contends that despite a lack of information about some aspect of the matter, one way or another the defendant is liable for infringement ».

64 *Media CAT* v *Adams*, cit.: « (...) they plead that the software was used either by the named defendant who was identified by the ISP, or by someone they authorised to use the internet connection or someone who gained access to the internet connection "due to the router having no or no adequate security". Then in paragraph 5 the plea is that "in the premises" the defendant has by himself, or by allowing others to do so, infringed. So taken together these two paragraphs show that the Particulars of Claim is pleaded on the basis that one way or another the defendant must be liable for the infringement which is taking place ».

Con l'introduzione del c.d. « D.L. Milleproroghe 2010 » infatti è stato modificato l'art. 7 del decreto Pisanu, che prevedeva a carico di internet-*point* e altri servizi pubblici che avessero intenzione di offrire delle connessioni Wi-Fi libere l'obbligo di richiedere un'autorizzazione al questore e contestualmente quello più gravoso di identificare ogni utente che accedeva alla rete condivisa[65].

Il comma 19 del decreto Milleproroghe ha invece ristretto l'obbligo di richiedere la speciale « licenza » al questore solo per i gestori di pubblici esercizi o circoli privati che svolgano (come gli internet-*point*), quale attività principale, la messa a disposizione del pubblico, dei clienti o dei soci, di apparecchi per le comunicazioni telematiche. Sono quindi escluse le altre categorie di esercenti, che solo in via secondaria offrono ai propri avventori i servizi aggiuntivi di connessione internet. Inoltre, è caduto in via assoluta, insieme ai commi 4 e 5 del decreto Pisanu, l'obbligo di identificazione degli utenti fruitori della connessione alla rete.

Gli effetti del comma 1 dell'art. 7, con una successiva modifica apportata dal « Milleproroghe 2012 » sono stati infine prolungati sino al termine dell'anno corrente.

Rispetto a questa novità nella normativa, che dovrebbe in qualche modo supportare una crescita e una diffusione più rapida delle tecnologie di accesso *wireless* da rendere disponibili al pubblico negli esercizi commerciali, l'apporto che la giurisprudenza ha offerto negli ultimi anni con riguardo al

[65] Art. 7, D.Lgs. 27 luglio 2005, n. 144, « Misure urgenti per il contrasto del terrorismo internazionale », convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155:

« 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 è 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, nonché 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, nonché 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, è 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, nonché 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 ».

problema della responsabilità dei terzi negli illeciti su internet risulta essere di scarsa entità.

Il primo contributo degno di nota, si riconduce all'ormai celebre caso « *Peppermint* »[66], che è poi divenuto un importante punto di riferimento anche per la giurisprudenza comunitaria, pronunciatasi qualche anno dopo su analoghe questioni (delle decisioni indirettamente « influenzate » da tale orientamento si parlerà più diffusamente *infra*, *sub par.* 8).

La vicenda trae le proprie origini dalle attività di investigazione antipirateria *on-line* di svolte dalla *Logistep* AG, con sede in svizzera, su mandato della *Peppermint Jam Records* e della *Techland*, due società operanti rispettivamente nell'ambito della produzione musicale (segnatamente nel ramo della *house music*) e della produzione e commercializzazione di *videogames*.

Gli indirizzi IP dei presunti « pirati », monitorati e « tracciati » dalla *Techland*, necessitavano infine di essere collegati agli altri dati riferibili all'utenza « incriminata » e in possesso degli ISP. A seguito dei dinieghi alle reiterate richieste di fornire tali informazioni, gli ISP (alcuni dei principali operatori del mercato italiano) venivano chiamati a rispondere della propria condotta in sede cautelare dinanzi all'Autorità giudiziaria.

Gli esiti — scaturenti da un travagliato iter processuale e da una copiosa produzione del giudice di merito e del garante per la privacy[67] — hanno portato all'affermazione di un principio che nega l'autorizzazione all'accesso ai nominativi degli utenti (c.d. *discovery*) formulato sulla base di un'interpretazione in chiave estensiva dell'art. 156-*bis* della legge italiana sul diritto d'autore, per cui in assenza di idonea informativa all'interessato, acquisizione del consenso e notifica al Garante per il trattamento dei dati personali, la raccolta di indirizzi IP deve ritenersi illecita e, in ogni caso, il diritto alla privacy degli utenti prevalente sul diritto all'ostensione dei dati del titolare del diritto d'autore[68].

[66] Una completa e critica ricostruzione della vicenda è fornita da L. Ferola, *Diritto d'autore vs. diritto alla riservatezza: alla ricerca di un equo bilanciamento nella rete*, in F. Pizzetti, *I diritti nella rete della rete*, cit., pp. 67-73.

[67] Il riferimento è alla « pionieristica » decisione del Garante privacy italiano sul caso *Peppermint*: Peer-to-peer: *illecito "spiare" gli utenti che scambiano file musicali e giochi*, 28 febbraio 2008, reperibile online all'URL: *http://www.garanteprivacy.it/garante/doc.jsp?ID=1495246*. Cfr. anche le sentenze della giurisprudenza di merito richiamate *infra*. Per i commenti in dottrina si rimanda, *ex multis*, a C. Blengino-M.A. Senor, *Il caso « Peppermint »: il prevedibile contrasto tra protezione del diritto d'autore e tutela della privacy nelle reti peer-to-peer*, in questa *Rivista*, 4-5, 2007, p. 385; D. Mula, *La responsabilità e gli obblighi degli Internet provider per violazione del diritto d'autore*, in *Riv. dir. ind.*, 3, 2010, p. 252; G. Scorza, *Il conflitto tra copyright e privacy nelle reti peer to peer: in margine al caso Peppermint*, in *Dir. dell'internet*, 2007, 5, p. 465.

[68] Cfr. T. Roma, 14 Luglio 2007, (T. sp. Z. e altro c. W.T. spa e altro), in *Juris Data*: « Il titolare di diritti d'autore non ha diritto d'ottenere dal provider *ex* art. 156-*bis* L.d.A. 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 è precluso dalla vigente disciplina in materia di privacy e trattamento dei dati personali in base alla quale è illecita, in assenza di idonea informativa all'interessato, acquisizione del consenso e notifica al Garante per il trattamento dei dati personali, la raccolta di indirizzi IP. Conseguentemente, *ex* art. 11 codice Privacy, devono ritenersi inutilizzabili nel procedimento di ostensione i dati raccolti, senza che sia invocabile l'art. 24 del codice Privacy, inapplicabile alla fattispecie. In ogni caso sul diritto all'ostensione del titolare del diritto

Dalle decisioni citate si trae altresì una definizione, seppur indiretta, di indirizzo IP come dato personale, inteso in un accezione « protettiva » (cara all'orientamento comunitario), ma valida solo se ricondotta alla combinazione dei dati oggetto delle attività di monitoraggio operate dalla *Techland* (tra cui appunto l'indirizzo IP)[69] con le generalità degli abbonati detenute dagli ISP[70] e sempre con specifico riferimento agli scopi e alle finalità che tale « trattamento » presupponeva.

Nel solco tracciato dalla pronuncia di cui *supra*, rispetto però all'efficacia ai fini probatori dell'indirizzo IP, si collocano le motivazioni addotte da un giudice capitolino nell'istanza di archiviazione (poi accolta) di un procedimento avente ad oggetto la presunta condivisione di *files* protetti da diritto d'autore attraverso programmi *peer-to-peer*, nel quale ad essere accusata era una signora individuata tramite l'indirizzo IP del proprio computer casalingo[71].

Il pubblico ministero ha osservato che la presunzione di responsabilità a carico della donna fosse esclusivamente collegata al « *fatto di essere costei la proprietaria della linea telefonica a servizio dei computer, mentre non vi è prova certa di chi ne abbia fatto uso, specie con le condotte di* download *che si vorrebbero criminalizzare* », concludendo pertanto che « *non appare possibile contestare in fatto all'indagata il reato per cui si procede che potrebbe essere attribuibile ad altri soggetti che facciano uso o abbiano fatto utilizzo anche saltuario del computer in sequ*estro ». Inoltre, puntualizza il

d'autore prevarrebbe il diritto alla privacy dell'utente »; T. Roma, 22 novembre 2007, (Wind telecomunicaz. c. Peppermint Jam Records GmbH), in *Foro it.*, 2008, I, 1329, secondo cui « posto che, alla luce della disciplina comunitaria, la tutela delle persone fisiche, con riguardo al trattamento dei dati personali, è prevalente rispetto alle esigenze probatorie di un giudizio civile teso all'accertamento della lesione del diritto di sfruttamento economico del diritto d'autore, deve escludersi l'applicabilità dell'art. 156-*bis* L. 633/41, in tema di identificazioni dei soggetti implicati nell'illecito, e dell'art. 24 d.leg. 196/03 al trattamento dei dati personali relativi alle comunicazioni elettroniche e telematiche tra privati, per finalità connesse alla tutela dei diritti soggettivi dei privati »; T. Roma, 19 Marzo 2008, n. 26121, in *Juris Data*: « che in conclusione nel caso di specie, in cui l'esecuzione dell'ordine di discovery si risolverebbe in una comunicazione dei dati personali dei consumatori senza alcun consenso dei medesimi, che operano sulla rete sulla presunzione di anonimato, la misura violerebbe il diritto alla riservatezza dei medesimi e pertanto ne difetta il requisito di ammissibilità ». o ancora la più recente pronuncia « FAPAV »: T. Roma, 15 aprile 2010, (Fapav c. Soc. Telecom Italia), in *Riv. dir. ind.*, 2010, II, 248, con nota di D. Mula.

Ancora, con riferimento alla stessa vicenda il Tribunale Federale di Losanna Svizzero si è espressa in maniera conforme all'orientamento del giudice di merito capitolino: cfr. DTF, n. 136 II 508, del 8 settembre 2010, reperibile in lingua originale all'URL: *http://www.bger.ch/*. V. anche Tribunale amministrativo federale (TAF), I Corte, n. A-3144/2008, del 27 maggio 2009, in *www.bvger.ch*.

[69] « I nomi e le dimensioni dei *files* offerti, la data e l'ora del (o degli) *upload*, indirizzo IP dell'offerente, ed i relativi codici *hash* e GUID ».

[70] T. Roma, 22 novembre 2007, n. 39349, in *Juris data*: « la indicazione dei nominativi degli utenti ai quali sono attribuiti determinati indirizzi IP in una determinata data e ora (così come richiesta dalla parte ricorrente Peppermint) costituisce comunicazione di dati personali, ossia di informazioni concernenti una persona fisica identificata o identificabile; infatti attraverso tali dati, le azioni eseguite utilizzando l'indirizzo IP interessato possono essere ricondotte al titolare della linea ».

[71] Decreto di archiviazione, Sez. Penale, 7 aprile 2009, n. 5120 del GIP Roma, in *Quotidiano legale*, 7/2009, « *Condivisione illegale di file, l'IP non identifica l'autore* ». V. anche il commento di G. Scorza, *Non basta un IP per fare un pirata*, in *punto-informatico.it*.

p.m., « *gli accertamenti ulteriori per chiarire quest'ultimo aspetto appaiono impossibili in termini di significativa raccolta della prova* ».

Partendo da questo assunto centrale, che pare privare l'indirizzo IP — inquadrato come un singolo elemento[72] — di una qualsiasi efficacia di « prova assoluta » per l'identificazione del reale autore dell'illecito, si giunge ad un'altra pronuncia, questa volta della Corte di Cassazione Penale, che ha reputato il titolare di un *internet point* non responsabile per la diffamazione compiuta attraverso i terminali di connessione internet della propria attività, ad opera di terzi soggetti rimasti non identificati[73].

Secondo i giudici della Suprema Corte infatti, non sussiste « alcun obbligo di conoscenza né tantomeno di controllo da parte del gestore delle comunicazioni inviate »: esso violerebbe l'art. 617-*quater* del c.p., che vieta l'intercettazione fraudolenta di sistemi informatici e telematici.

Nel caso di specie il gestore non è stato reputato responsabile neppure sotto il profilo del dolo eventuale poiché « *non aveva alcun obbligo, anzi, in base alle norme sopra richiamate, gli era impedito di prendere contezza in alcun modo del contenuto della comunicazione inviata. Così che il reato ugualmente si sarebbe verificato anche se il gestore avesse annotato le generalità dell'utilizzatore del terminale per l'invio della posta elettronica* » (il riferimento è all'ormai abrogato obbligo di identificazione previsto all'interno del Decreto Pisanu).

Nella scarsa messe di pronunce sul tema, il Giudice di pace di Milano[74] si è espresso in maniera parzialmente difforme, affrontando di recente un caso di presunta responsabilità contrattuale del fornitore dei servizi internet, accusato da un abbonato di essere venuto meno ai doveri di assistenza e ancora a generali adempimenti contrattuali, che a detta dell'attore si ponevano alla base di episodi di traffico « anomalo » proveniente dalla propria connessione e, di conseguenza, alla ricezione di alcune fatture recanti importi dovuti esorbitanti rispetto al reale utilizzo dell'*account*.

Nel rigettare la domanda di parte attrice il giudice ha preso atto degli accertamenti operati dal C.T.U. che rilevavano come il traffico in oggetto, transitato attraverso un punto d'accesso di proprietà dell'attore e installato dallo stesso, era interamente addebitabile all'utenza dell'istante.

Ponendo l'ipotesi di una possibile fruizione indebita del collegamento internet da parte di soggetti estranei, nella pronuncia si sostiene che l'attore, installando il *router wireless* aveva omesso di proteggere la propria connessione mediante la programmazione di una apposita password, con il risultato che l'installazione, operata in modo non conforme, non proteggeva in alcun modo la rete locale da accessi di terzi non autorizzati: pertanto, il

[72] Sulla « natura » dell'indirizzo IP, in particolare rispetto alla associazione tra la funzione « numerica » di individuazione univoca di un computer tra i computer dell'indirizzo IP e quella di identificazione in « senso sociale » del *domain name*, si rimanda all'analisi svolta da G. FINOCCHIARO, *Arbitrato e* domain name, in *AIDA*, XV, 2006, p. 62 ss., soprattutto con riguardo a T. Firenze, ord. del 29 giugno 2000, in *Dir. inf*, 2000, p. 672 ss. e T. Salerno, 25 febbraio 2003, in questa *Rivista*, 2003, p. 832 ss. Sul tema v. anche P. SAMMARCO, *Nome, nome a dominio e marchio per la stessa denominazione: una coesistenza difficile*, in questa *Rivista*, 2003, p. 848.

[73] Cass. pen., sez. V, 11 novembre 2008, n. 6046. in *Foro it.*, 2009, II, 562 e in *Danno resp.*, 2009, 1049, con nota di M. CHIAROLLA.

[74] Giudice di pace Milano Sez. IX, Sent., 24 maggio 2011, in *Pluris*, Internet/Contratto in genere. Sul tema si veda T. Roma, 13 dicembre 2006, in *Dir. Internet*, fasc. 4, pp. 363-367, con nota di V. FRANCESCHELLI.

traffico in entrata e in uscita del router era nel caso di specie da considerarsi sotto la responsabilità del possessore del *router*.

In un altro caso, l'assenza di una preventiva responsabilità per *culpa in vigilando* in capo all'intestatario è stata di recente, seppur indirettamente, avallata dalla Cassazione Penale: due soggetti sono stati ritenuti responsabili del reato di diffamazione compiuto attraverso l'utilizzo di due apparecchi identificati attraverso il numero IP[75]. All'apparenza questo dato si porrebbe in contrasto rispetto a quanto precedentemente asserito.

Da un'attenta lettura della motivazione però si evince come la presunzione di colpa a carico degli imputati sia stata prima ampiamente valutata dagli inquirenti sia a livello tecnico che a livello logico-causale, con riferimento a precisi riscontri sul tempo e il luogo dell'illecito nonché con riguardo ad altre condizioni (*nickname*, uso del personal computer in famiglia, componenti dell'azienda, dissidi tra diffamante e diffamato) che hanno permesso di accantonare le tesi difensive basate su una presunta non appartenenza agli imputati dei contenuti lesivi dei messaggi, concludendo infine per la condanna degli stessi.

Questa pronuncia indica ad ogni modo che l'indirizzo IP, seppur non decisivo elemento probatorio, può avere un'importante valenza, accostato ad un attenta e precisa disamina degli elementi che concorrono a congiungere causalmente con un nesso tale identificativo numerico al nome del reale autore dell'illecito, che non sempre sarà corrispondente al nome dell'intestatario della connessione internet, in un'ottica che da un lato non crei una sorta di « immunità diffusa » ma che dall'altro non configuri un « ingiusto accanimento ».

6.1. *Ipotesi ricostruttive: Codice della privacy e misure di sicurezza.*

Con riferimento alle connessioni Wi-Fi private (o « casalinghe ») — e alla ricerca di un « contenuto minimo » del presunto dovere di « protezione diligente » posto in capo al titolare — il tentativo di operare una ricollocazione sistematica di tale fattispecie entro la disciplina legislativa vigente e nei canoni « classici » della responsabilità civile fornisce diversi spunti di interesse, sintetizzabili in tre differenti ipotesi.

Nel primo caso (simile, nei tratti, alla vicenda « *Sommer unseres Lebens* » affrontata *infra*, *sub par.* 2) sarebbe da escludere ogni tipo di responsabilità in capo all'intestatario di connessione senza fili se: *a*) il punto di accesso viene commercializzato dal produttore sprovvisto di *password*, *b*) la *password* « madre » preimpostata è facilmente eludibile; *c*) non è fornita all'« utente medio », al momento dell'installazione (ad esempio con un *wizard* all'avvio), la possibilità di inserire o modificare agevolmente la sequenza.

In questi termini infatti la protezione del proprio *router* sarebbe da considerare inesigibile, poiché non consentita dal produttore (o ancora non

[75] Cass. pen., sez. V., 1 dicembre 2010-7 marzo 2011, n. 8824. Per un commento si rimanda a G. NEGRI, *Condannato chi utilizza un nickname su un forum online*, in *Il sole 24 ore*, 8 marzo 2011 e G. CORRIAS LUCENTE, *L'indirizzo IP quale strumento d'identificazione dell'autore di reati in Internet*, in *www.medialaws.eu*.

garantita in maniera efficace), per cui l'accesso ai terzi sarebbe « *invito domino* », dato che avvenuto senza il consenso dell'intestatario[76].

Nell'ipotesi in cui invece fosse lo stesso proprietario del *router* a mantenere volontariamente « aperto » l'accesso lasciandolo privo di una sequenza di sicurezza, le prospettive da valutare sarebbero due.

Il primo spunto ci viene fornito dalla lettura degli artt. 31 e 33 del D.Lgs. 196/2003 (c.d. Codice privacy)[77], che regolamentano le « misure e obblighi di sicurezza » e, ancora la sottocategoria delle « misure minime di sicurezza » a carico del titolare del trattamento dei dati personali, da cui discenderebbero ipotesi di responsabilità da illecito trattamento dei dati personali o ancora, nel caso di violazione dell'art. 33 cit., in aggiunta alle responsabilità civili, anche misure contravvenzionali di carattere penale *ex* art. 169 cit.[78].

Se con l'articolo 31 cit. il legislatore ha voluto imporre una generale obbligazione di diligenza[79] quanto più estesa ed « elastica » possibile[80], con l'art. 33 cit. si è introdotto il concetto di « misure minime », intese come « il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 »[81].

[76] Nell'ambito della responsabilità civile e dei danni da sinistro stradale la giurisprudenza ha operato una distinzione tra circolazione del veicolo *invito domino* o *prohibente domino*. Secondo questi principi, al fine di andare esente da responsabilità *ex* art. 2054 c.c., il proprietario dell'autoveicolo dovrà fornire la prova non già che il mezzo abbia circolato senza il suo consenso *invito domino*, ma consistente « in un concreto comportamento, specificamente idoneo a vietare ed impedire la circolazione del veicolo ». Nel caso affrontato però, si discorre di un punto di accesso *wireless* sfornito « a monte » di una sequenza di protezione efficace, per cui sarebbe come parlare di un autoveicolo prodotto senza un sistema di chiusura e/o privo di un sistema di accensione « protetto » da una chiave. V. Cass., 17 ottobre 1994, n. 8461, in *Arch. circolaz.*, 1995, 394.

[77] *Ex multis*, si rimanda a S. Sica-P. Stanzione (a cura di), *La nuova disciplina sulla* privacy, Bologna, 2004. Per un commento della « vecchia » legge 675/96 v. V. Cuffaro-V. Ricciuto-V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998.

[78] « Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili ».

[79] V. S. Sica, *Commento agli artt. 1-6*, in S. Sica-P. Stanzione (a cura di), *La nuova disciplina sulla* privacy, cit.

[80] « I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta ».

[81] V. G.M. Riccio, *Commento agli artt. 33-36*, in S. Sica-P. Stanzione (a cura di), *La nuova disciplina sulla* privacy, cit.

Tale norma, in un'ipotetica estensione all'ambito delle reti *wireless*, potrebbe anche fornire un'indicazione tecnica specifica con l'art. 34, lett. *e*) cit., in cui si impone il dovere di proteggere gli strumenti elettronici e i dati per prevenire trattamenti illeciti di dati, con riferimento a determinati programmi informatici e, sopratutto, allo scopo di evitare « accessi non consentiti ».

L'interpretazione « estensiva » delle norme operata *supra* rivela, dall'altra parte, alcuni dubbi legati alla « portata » delle norme in analisi e, sopratutto, delle sanzioni previste. La figura del « titolare del trattamento », seppur pacificamente individuabile anche in una persona fisica, andrebbe pur sempre rapportata all'entità e alle dimensioni del trattamento effettuato.

Tale « limite » pare però essere — quantomeno a livello teorico-normativo — superato nelle intenzioni del legislatore.

L'art. 5 del Codice, delinea la generale esenzione per le persone fisiche che trattano i dati ai fini esclusivamente personali, per cui in queste ipotesi il codice andrebbe applicato solo qualora i dati venissero « destinati ad una comunicazione sistematica o alla diffusione ». Al terzo comma si è voluto puntualizzare che « in ogni caso » si applicano le disposizioni in tema di responsabilità e sicurezza dei dati di cui agli articoli 15 e 31.

L'obbligazione generale di sicurezza estenderebbe pertanto i propri effetti preventivi nei confronti di tutti i titolari persone fisiche e, qualora dalla violazione scaturisse una fattispecie di trattamento illecito di dati non di carattere « personale » — e pertanto non « esente » — si applicherebbero le regole di responsabilità *ex* art. 2050 c.c. contemplate dall'art. 15 del Codice privacy.

6.2. (Segue) *Art. 2051 c.c. e rapporto di custodia.*

L'ultima ambito d'indagine da esplorare attinente alla posizione del proprietario di accesso *wireless* « volutamente non protetto » conduce a forme di responsabilità « speciali » come quella rappresentata dall'art. 2051 c.c. (responsabilità da cose in custodia), secondo cui « ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito »[82].

La responsabilità da cose in custodia è stata (ed è ancora) oggetto di un lungo e altalenante dibattito giurisprudenziale e dottrinale avente per oggetto la sua natura, che ha « fluttuato » da tesi a sostegno di un criterio di

[82] Cfr. *ex multis* G. ALPA (a cura di), *La responsabilità civile. Parte generale*, cit.; G. ALPA-M. BESSONE-V. ZENO-ZENCOVICH, *I fatti illeciti*, in *Tratt. Rescigno*, 14, Torino, 1995, p. 342; D. APICELLA, *Responsabilità da cose in custodia*, in *Trattato sulla responsabilità civile*, a cura di P. STANZIONE, II, Padova, 2010, pp. 833-894; M. COMPORTI, *Artt. 2049-2053*, in *Il Codice Civile. Commentario*, dir. da F.D. Busnelli, Milano, 2009; L. BIGLIAZZI GERI, *Responsabilità civile per danni da cose ed animali*, 2ª ed., Milano, 1967, p. 240 ss.; ID., *Responsabilità civile da cose in custodia, animali e rovine di edificio*, Milano, 1974, p. 96 ss.; L. CORSARO, *Responsabilità da cose*, in *Dig. disc. priv.*, 1998 S. RODOTÀ, *Il problema della responsabilità civile*, Milano, 1964; C. SALVI, *La Responsabilità civile*, in *Trattato di dir.priv.*, a cura di G. Iudica-P. Zatti, Milano, 1998; P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961;. G. VISINTINI, *Trattato breve della responsabilità civile*, Padova, 1996, p. 647.

imputazione soggettivo e colposo a un'altra — considerata maggioritaria — che in essa ravvede i caratteri pregnanti di una forma di responsabilità « oggettiva ».

L'art. 2051 c.c. opera, come è noto, su un piano di « specialità » rispetto all'art. 2043 c.c., ma abbraccia un bacino casistico che può considerarsi, rispetto ad altre fattispecie di responsabilità « speciali » ampio e quasi « infinito ». Anche per questo motivo forse la giurisprudenza ha spesso optato per soluzioni non sempre coerenti l'una con l'altra.

Trascendendo dai meri esercizi classificatori la fattispecie in oggetto trova la sua principale direttrice nel rapporto di custodia, che potremmo definire quel legame intercorrente tra un soggetto e una cosa, che si esplicita nell'effettivo esercizio di un potere fisico consistente nel controllo delle modalità d'uso e di conservazione della cosa stessa: tale legame a sua volta si connota per la sussistenza di un dovere di custodia, o meglio di un vincolo di responsabile vigilanza[83].

Se, infatti, nel sistema descritto dall'art. 2050 c.c.[84] l'esercente l'attività pericolosa dovrà provare, in alternativa al fortuito o al fatto del terzo, di avere « adottato tutte le misure idonee ad evitare il danno » — posto il grado di pericolosità dell'attività stessa — nel caso di responsabilità *ex* art. 2051 c.c. è la relazione tra custode e cosa ad imporre uno standard che è pertanto parametro di sussistenza del rapporto stesso per cui, se correttamente atteso dal custode, « il fatto della cosa » non avrebbe modo di esistere perché non ci sarebbe danno se non quello collegato al caso fortuito, mentre, in caso contrario, il prodursi del danno ricondurrebbe automaticamente al vincolo gravante sul custode, per cui egli andrebbe ritenuto responsabile[85].

[83] V. G. ALPA, *La responsabilità civile. Parte generale*, cit., p. 739, secondo cui all'effettivo potere fisico di un soggetto sulla cosa « inerisce il dovere di custodire la cosa stessa, cioè di vigilarla e mantenerne il controllo, in modo da impedire che produca danni a terzi ». In giurisprudenza cfr. Corte Cost., 10 maggio 1999, n. 156, in *Giust. civ.*, 7-8, 1999, p. 1927; Cass., 18 febbraio 2000, n. 1859, in *Danno e resp.*, 2000, 390, con nota di I. NASTI: « L'art. 2051 c.c. non si riferisce alla custodia nel senso contrattuale del termine, bensì ad un effettivo potere fisico, che implica il governo e l'uso della cosa ed a cui sono riconducibili l'esigenza e l'onere della vigilanza affinché dalla cosa stessa, per sua natura o per particolari contingenze, non derivi danno ad altri; nel contratto di trasporto l'effettivo potere fisico ed il connesso obbligo di vigilanza passano al vettore dal momento in cui gli viene consegnata la cosa, sicché lo stesso è responsabile a norma dell'art. 2051 c.c. dei danni che la cosa produce fino alla riconsegna ».

[84] Sul tema, oltre alla letteratura già richiamata si rimanda a M. FRANZONI, *Responsabilità per l'esercizio di attività pericolose*, in *La responsabilità civile. Una rassegna di dottrina e giurisprudenza*, dir. da G. Alpa-M. Bessone, II, Torino, 1987; P.G. MONATERI, *Le attività pericolose*, *in Illecito e Responsabilità civile*, II, coll. dir. da M. Bessone, Torino, 2002; P. RECANO, *La Responsabilità civile da attività pericolose*, Padova, 2001. Sia consentito inoltre rimandare a G.M. RICCIO-G. GIANNONE CODIGLIONE, *Responsabilità da attività pericolose*, in P. STANZIONE (dir. da) *Trattato della responsabilità civile*, II, cit., pp. 687-730.

[85] Cfr. G. ALPA, *La responsabilità civile. Parte generale*, cit., p. 738, secondo cui l'art. 2051 c.c. « disciplina sì l'ipotesi di un danno prodotto dalle cose, ma in quanto il soggetto che le ha in custodia ometta le misure necessarie affinché esso non si verifichi, ond'è che causa del danno in definitiva non è la cosa, ma il comportamento umano negativo ». Cfr. Cass., 29 novembre 2006, n. 25243, in *Arch. locazioni*, 2007, 286. Secondo autorevole dottrina la custodia consiste nel dovere di controllo sul rischio derivante dalla cosa ed il custode è colui che ha con questa un rapporto permanente tale da rendere prevedibili i rischi ad essa connaturati. Così sinteticamente A. NEGRO, *Art. 2051*, in *Commenta-*

Il rapporto di custodia, quindi, presuppone un dovere « minimo » di vigilanza — flessibile e variabile rispetto alla natura della cosa — che connota la « speciale » relazione intercorrente tra il custode e la cosa stessa; allo stesso tempo però tale assunto non equivale al riconoscimento di una presunzione di colpa, ma piuttosto di una presunzione *iuris tantum* di responsabilità[86].

Ci si trova di fronte ad una particolare forma « ibrida » di responsabilità — che potremmo più propriamente intendere come una responsabilità « mediata » e « indiretta », a cavallo tra la responsabilità aggravata[87] e quella semioggettiva[88], legata alla sussistenza di un rapporto di custodia[89].

Il danno prodotto dovrà scaturire dal dinamismo connaturato alla cosa — o ancora dallo sviluppo di un agente dannoso in capo ad essa — e, dunque dovrà essere eziologicamente collegato alla cosa stessa: questo perché si discute di rapporti nei quali il carattere « speciale » sancito dal vincolo di custodia è predisposto « a monte », con la previsione di un aggravio dell'onere probatorio — invertito e a carico del custode — e, in aggiunta, del restringimento del contenuto della prova stessa al caso fortuito[90].

rio al codice civile. I Fatti Illeciti, a cura di P. Cendon, Milano, 2009, p. 866 con riferimento a P. Trimarchi, *Rischio e responsabilità oggettiva*, cit., p. 244. In giurisprudenza v. Cass., 6 luglio 2004, n. 12329, in *Danno e resp.*, 2004, 1193.

[86] Così G. Alpa, *La responsabilità civile. Parte Generale*, cit., p. 740 ss. In giurisprudenza cfr. Cass., sez. un., 11 novembre 1991, n. 12019, in *Foro it.*, 1993, I, 922 e ancora Cass., 20 maggio 1998, n. 5031, in *Foro it.*, 1998, I, 2875, con nota di L. Lambo; Cass., 17 gennaio 2001, n. 584, in *Danno e resp.*, 2001, 722, con nota di R. Breda.

[87] Cass., 20 febbraio 2006, n. 3651, in *Foro it.*, 2006, I, 2801, con nota di P. Laghezza: « l'art. 2051 c.c. determina infatti un'ipotesi (non già di responsabilità oggettiva bensì) caratterizzata da un criterio di inversione dell'onere della prova, ponendo (al 2° comma) a carico del custode la possibilità di liberarsi dalla responsabilità presunta a suo carico mediante la prova liberatoria del fortuito (c.d. responsabilità aggravata), dando cioè, in ragione dei poteri che la particolare relazione con la cosa gli attribuisce cui fanno peraltro riscontro corrispondenti obblighi di vigilanza, controllo e diligenza (i quali impongono di adottare tutte le misure idonee a prevenire ed impedire la produzione di danni a terzi, con lo sforzo adeguato alla natura e alla funzione della cosa e alle circostanze del caso concreto) nonché in ossequio al principio di c.d. vicinanza alla prova, la dimostrazione che il danno si è verificato in modo non prevedibile né superabile con lo sforzo diligente adeguato alle concrete circostanze del caso ». Cfr. anche P. Laghezza, *Insidia e trabocchetto: un addio senza rimpianti*, in *Corr. giur.*, 2006, p. 1727 e A. Carrato, *Insidia stradale: amministrazione responsabile* ex *art. 2051 c.c.*, in *Dir. e giust.*, 2006, p. 52.

[88] L. Bigliazzi Geri-U. Breccia-F.D. Busnelli-U. Natoli, *Diritto civile, Obbligazioni e contratti*, Torino, 1989, p. 752 ss.; F.D. Busnelli, voce *Illecito civile*, in *Enc. Giur. Treccani*, XV, Roma, 1991, p. 25.

[89] Cass., 20 luglio 2002, n. 10641, in *Arch. civ.*, 2003, 571: « La custodia si concretizza, cioè, in un criterio di responsabilità, intendendo per tale quello che addossa a colui che ha la custodia della cosa la responsabilità per determinati eventi, indipendentemente dalla ricerca di un nesso causale tra il comportamento del custode e l'evento ».

[90] Cass. 26 febbraio 1994, n. 1947: « Poiché la responsabilità si fonda non su un comportamento o un'attività del custode, ma su una relazione (di custodia) intercorrente tra questi e la cosa dannosa, e poiché il limite della responsabilità risiede nell'intervento di un fattore (il caso fortuito) che attiene non ad un comportamento del responsabile (come nelle prove liberatorie degli artt. 2047, 2048, 2050 e 2054 c.c.), ma nelle modalità di causazione del danno, si deve ritenere che la rilevanza del fortuito attiene al profilo causale, in quanto suscettibile di una valutazione che consenta di ricondurre all'elemento esterno, anziché alla cosa che ne è fonte immediata, il danno concretamente verificatosi. Si intende, così, anche la ragione dell'inversione dell'onere della prova prevista dall'art. 2051, relativa alla ripartizione della prova sul nesso causale. All'attore compete provare

In altre parole, il danno dovrà scaturire dal « fatto della cosa custodita » o, per meglio dire, dal fatto della cosa oggetto di un rapporto di custodia violato. Il limite del fortuito pertanto, è posto ad evidenziare la sussistenza di un vincolo i cui caratteri pregnanti sono strettamente legati alla natura e alle peculiarità della cosa custodita.

Poste queste riflessioni, si potrebbe in via ipotetica ricondurre entro tali canoni il rapporto tra l'intestatario della connessione (il « custode ») e il *router wireless* (« la cosa »), per cui un accesso di terzi « indotto » da una custodia disattesa si potrebbe equiparare, ad esempio, al caso della violazione di un rapporto di custodia intercorrente tra il condominio e le impalcature montate per svolgere alcuni lavori di ristrutturazione del palazzo.

Nel caso di specie la giurisprudenza — seppur non pacificamente — ha reputato responsabile il condominio stesso (o quantomeno corresponsabile) per il danno patito da persona il cui appartamento è stato svaligiato da terzi introdottivi. Il danno sarebbe causalmente collegato alla cosa, poiché scaturito da un accesso alle impalcature metalliche comunque « favorito » dal venir meno degli standard minimi di sicurezza richiesti e intrinseci al rapporto[91].

Un altra situazione adattabile alla fattispecie dell'accesso *wireless* potrebbe essere quella contemplata recentemente da un giudice di merito nel reputare responsabile *ex* art. 2051 c.c. il custode di una condotta elettrica sovrastante un'abitazione, per i danni cagionati dalle eccessive ed intollerabili immissioni elettromagnetiche[92].

Ammessa — sempre in via ipotetica — la compatibilità con l'art. 2051 c.c. andrebbe ora valutato il contenuto dell'onere probatorio a cui sarebbe tenuto il custode per andare esente da responsabilità: nel caso di un *router* volutamente non protetto, nel senso di un dispositivo le cui caratteristiche e peculiarità sono state *de facto* rese accessibili a tutti a causa di una violazione del rapporto di custodia, l'onere probatorio andrebbe ricondotto ad una nozione di caso fortuito più severa ed « onerosa », strettamente aderente a quella contemplata dalla giurisprudenza maggioritaria, per cui il custode dovrà « *dimostrare l'esistenza di un fattore estraneo che, per il carattere dell'imprevedibilità e dell'eccezionalità, sia idoneo ad interrompere il nesso di causalità* »[93].

l'esistenza del rapporto eziologico tra la cosa e l'evento lesivo; il convenuto per liberarsi dovrà provare l'esistenza di un fattore, estraneo alla sua sfera soggettiva, idoneo ad interrompere quel nesso causale. Secondo l'orientamento giurisprudenziale prevalente tale idoneità sussiste solo se il fattore esterno (che può essere anche il fatto di un terzo o del danneggiato) presenti i caratteri del fortuito, e cioè dell'imprevedibilità e dell'assoluta eccezionalità ».

[91] V. Cass., 17 marzo 2009, n. 6435, in *Danno e resp.*, 2009, 620, con nota di A. Mastrolilli; Cass., 6 ottobre 1997, n. 9707, in *Foro it.*, 1998, I, 100; Cass., 9 febbraio 1980, n. 913, in *Giur. it.*, 1981, I, 1, 587 e in *Foro pad.*, 1982, I, 256, con nota di M. Bessone, *contra* Cass. 23 maggio 2006, n. 121111, in *Danno e resp.*, 2007, 163; Cass., 18 ottobre 2005, n. 20133, in *Danno e resp.*, 2006, 405, con nota di G. Guerreschi; Cass., n. 3722/1976 e 4643/1976, in *Giur. it.*, I, 1, 222, con nota di G. Alpa, o ancora, nel caso di responsabilità di un proprietario di appartamento disabitato utilizzato come « punto di passaggio » per un furto v. Cass., 6 aprile 1982, n. 2134, in *Resp. civ. prev.*, 1982, 745.

[92] T. Modena, 6 settembre 2004, in *www. personaedanno.it*, a cura di P. Cendon.

[93] Cass., 29 novembre 2006, n. 25243, cit. Per caso fortuito in questo caso, secondo autorevole dottrina e ampia parte della giurisprudenza, bisogna intendere anche,

Delle evidenti difficoltà interpretative sorgono però se si ribalta la prospettiva, applicando la medesima regola: data una connessione *wireless* protetta da una *password*, il proprietario del punto di accesso sarebbe ritenuto responsabile (o quantomeno corresponsabile) anche nei casi di accesso abusivo al sistema informatico posto in essere da un terzo, poiché non basterebbe provare un caso fortuito in termini « soggettivi », identificabile in questo caso nella vigilanza diligente della connessione[94]. Una soluzione — seppur quasi mai contemplata dalla giurisprudenza — potrebbe essere rappresentata dall'orientamento espresso da alcuna dottrina che, nel descrivere la figura della responsabilità semi-oggettiva, ha affermato che la prova della condotta diligente del custode, pur se insufficiente a « liberare » lo stesso, può costituire un elemento presuntivo *ex* art. 2729 c.c., atta pertanto ad identificare una causa estranea idonea ad escludere la responsabilità del custode[95].

La forma di responsabilità tratteggiata dall'art. 2051 c.c. potrebbe a ben vedersi divenire nel futuro uno strumento ancor di più utilizzato dalla giurisprudenza per « cristallizzare » regole di condotta non scritte al fine di prevenire (o risarcire) i danni collegati alla sussistenza e alla violazione di determinati rapporti — selezionati poiché meritevoli — intercorrenti tra soggetti e cose[96], inquadrati nel contesto di un progressivo mutamento degli usi, delle abitudini e, appunto, delle *res*[97].

in una vasta accezione, il fatto del terzo e del danneggiato, rimanendo però esclusa la causa ignota. Così G. ALPA, *La responsabilità civile. Parte generale*. cit., p. 739 s.

[94] Secondo la posizione della giurisprudenza e della dottrina più favorevoli alla tesi della natura soggettiva, il caso fortuito andrebbe concepito come la situazione in cui si dimostri di essere esenti da colpa o, in altre parole che « la prova del caso fortuito è data sul piano di ciò che il presunto responsabile avrebbe dovuto fare e ha fatto per evitare il danno ». Così C.M. BIANCA, *Diritto civile. La responsabilità*, Milano, 1994, p. 718.

[95] L. BIGLIAZZI GERI-U. BRECCIA-F.D. BUSNELLI-U. NATOLI, *Diritto civile, Obbligazioni e contratti*, cit., p. 752. In giurisprudenza una (isolata) eco di tale orientamento si rintraccia in Cass. 20 febbraio 2006, n. 3651, cit., per cui « Tale inversione dell'onere probatorio non fa peraltro venire meno la rilevanza del requisito della colpa, che concorre — seppure in via presuntiva — a costituire l'illecito, come reso palese dalla stessa possibilità di provarne la mancanza ».

[96] Sulla prospettiva di un'applicazione « estensiva » dell'art. 2051 c.c. ad altre fattispecie « selezionate » al fine di adattare la disciplina e le regole del rapporto di custodia all'evoluzione della società, si guardi, ad esempio, all'evoluzione giurisprudenziale in tema di responsabilità della pubblica amministrazione e al concetto di « effettivo esercente della custodia »: sul punto cfr. Cass. 6 luglio 2006, n. 15384, in *Foro it.*, 2006, I, 3358, con nota di P. LAGHEZZA: « La presunzione di responsabilità sancita dall'art. 2051 c.c. non si applica agli enti pubblici, per i danni subiti dagli utenti di beni demaniali, ogni qual volta sugli stessi, per le loro caratteristiche, non sia possibile esercitare la custodia; a tal fine, l'estensione del bene e la sua utilizzazione generale e diretta da parte di terzi costituiscono soltanto figure sintomatiche dell'impossibilità di custodia e, come tali, vanno sottoposte in concreto al vaglio del giudice di merito ». Secondo un più recente indirizzo a S.C. a puntualizzato che « la presunzione di responsabilità di cui all'art. 2051 c.c. è applicabile nei confronti della p.a. per le categorie di beni demaniali quali le strade pubbliche solamente quando, per le ridotte dimensioni, ne è possibile un efficace controllo ed una costante vigilanza da parte della p.a., tale da impedire l'insorgenza di cause di pericolo per gli utenti ». Così Cass., 26 settembre 2006, n. 20827, in *Arch. circolaz.*, 2007, 791.

[97] È indubbio che il già ampio concetto di « cosa » sia stato oggetto, negli ultimi 50 anni di un continuo processo di ridefinizione: si guardi ad esempio allo sviluppo delle tecnologie dell'informazione e della comunicazione per cui la cosa, da « oggetto che è in relazione con un soggetto che lo detiene » sia divenuta oggetto capace di « animarsi », di interagire con il mondo circo-

Dall'altra parte però, l'estensione di siffatte regole, cosi ampie e severe, alla disciplina di fattispecie come quella rappresentata *lato sensu* dall'accesso ad internet — inteso come un « diritto » non ancora del tutto « emerso » e riconosciuto, ma che è già fondamentale per lo sviluppo della società moderna — andrebbe sempre inserita in uno schema più ampio e articolato, in cui i « rischi » connessi alla violazione di rapporti di custodia e vigilanza devono essere sempre rapportati agli interessi contrapposti coinvolti e, soprattutto alla tutela di diritti e principi fondamentali della persona quali, ad esempio, la libertà di espressione e d'informazione o la solidarietà.

7. Reti Wi-Fi « aperte » e responsabilità: l'interessante opinione di un giudice di merito e la innovativa disciplina finlandese.

Nel quadro sino ad ora tracciato si colloca l'interessante esperienza normativa della Finlandia, suggellata da una recente pronuncia di una corte distrettuale[98].

La corte di Ylivieska ha reputato non responsabile l'intestatario di un *account* « *open* Wi-Fi » per i reati di violazione del diritto d'autore commessi da terzi soggetti nell'utilizzo di quel *network*.

Il « *Copyright Information and Anti-Piracy Center* » (CIAPC o TTVK, nell'acronimo in lingua finlandese), un'associazione di gestori di diritti d'autore aveva citato una donna finlandese, chiedendone la condanna al pagamento di una somma pecuniaria abbastanza cospicua quale risarcimento del danno subito.

Il presunto illecito si era verificato in un lasso temporale di circa 12 minuti nel luglio del 2010: utilizzando la connessione intestata alla donna infatti un utente aveva condiviso, attraverso una piattaforma *peer-to-peer*, alcuni *files* protetti da diritti di privativa. In quello stesso momento però un pubblico di circa cento persone era impegnato in un'attività ricreativa estiva (la visione di uno spettacolo teatrale) presso i locali della residenza della donna, una ex scuola.

Anche a causa di questa circostanza, la parte istante non è riuscita a produrre alcuna prova valida atta a dimostrare che la donna convenuta in giudizio avesse preso parte o fosse stata in qualche modo coinvolta nella commissione dell'illecito in oggetto.

I giudici finlandesi si sono pronunciati valutando se il mero atto di mettere a disposizione una rete di connessione internet Wi-Fi non protetta da *password* potesse o meno essere considerato fonte di responsabilità per l'intestatario nei casi di illeciti da parte di terzi.

Contestualmente alla richiesta di risarcimento l'istante aveva inoltre richiesto un'ingiunzione nei confronti della donna, al fine di prevenire ogni altra possibile e futura violazione: qualora tale richiesta fosse stata ac-

stante, prescindendo dalla signoria e dal « comando » dell'uomo.

98 *Ylivieskan käräjäoikeus*, 14 maggio 2012, *TTVK v. Toppinen*. Il testo integrale della pronuncia, in lingua originale, è reperibile all'url: *http://www.turre.com/2012/05/ylivieskan-ko-ei-vastuuta-wlanista/*.

colta, i titolari di diritti d'autore avrebbero avuto a loro disposizione un potente strumento di carattere inibitorio, suscettibile di essere utilizzato anche in maniera impropria e indiscriminata nei confronti dei fornitori di connessioni Wi-Fi « aperte ».

Alla luce della legislazione finlandese che ha recepito la normativa europea che regola tale fattispecie (su tutte le direttive 2000/31/CE e la 2001/29/CE), i giudici di primo grado si sono espressi rigettando la richiesta della CIAPC e affermando che l'intestatario di una connessione Wi-Fi non protetta da password non può essere considerato responsabile per gli illeciti commessi da terzi.

Con tutta probabilità verrà presentato appello presso la Corte d'appello di *Vaasa*, il che potrebbe innescare il meccanismo di rinvio pregiudiziale innanzi alla Corte di Giustizia europea, per un auspicabile chiarimento su tale controversa questione.

Nel 2010, il ministro della giustizia finlandese aveva espresso l'intenzione e la necessità di « de-criminalizzare » le connessioni « *open* Wi-Fi », modificando le disposizioni di legge precedenti (risalenti al 2005) che consideravano un reato l'accesso non autorizzato a reti wireless non protette da password. Inoltre, il 1° luglio del 2010 è entrata in vigore una legge che proclama l'accesso a internet quale « diritto legale » per tutti i cittadini finlandesi[99].

In questo scenario, la diffusione di reti *wireless* in Finlandia è cresciuto in maniera esponenziale, facendole lasciare rapidamente la posizione di fanalino di coda nella classifica dei paesi europei che utilizzano tale tecnologia.

8. L'INDIRIZZO IP NEL DIBATTITO COMUNITARIO.

In ambito comunitario, il dibattito attorno al ruolo e alla natura dell'indirizzo IP si è recentemente arricchito di ulteriori spunti, provenienti sia dal formante giurisprudenziale che dal dibattito avente per oggetto le imminenti modifiche del quadro normativo vigente.

Da un lato infatti, la giurisprudenza della Corte di Giustizia ha dato seguito alla celeberrima pronuncia « *Promusicae* »[100] con le pronunce

[99] V. C. T. MARSDEN, *Internet co-regulation. European law, Regulatory governance and Legitimacy in Cyberspace*, Cambridge, 2011, p. 4 ss.

[100] Nel 2005 *Promusicae* (*Productores de Mùsica España*) chiedeva al Tribunale commerciale di Madrid di ingiungere al gestore *Telefonica* di rivelare l'identità e l'indirizzo fisico di alcuni utenti, individuati attraverso il proprio indirizzo IP, che fruivano della connessione Internet offerta da quest'ultimo ISP. Secondo *Promusicae*, infatti, tali utenti avevano ripetutamente violato il diritto d'autore condividendo e scaricando *files* musicali attraverso piattaforme *peer to peer* (quali *KaZaa*). La stessa *Promusicae* aveva in precedenza provveduto a raccogliere gli indirizzi IP degli utenti « sospettati » e si era vista contestualmente rifiutare da *Telefonica* la richiesta di accesso ai dati dei titolari degli abbonamenti. Dopo una prima sentenza favorevole a *Promusicae* la questione, giunta in appello è divenuta oggetto di un rinvio pregiudiziale alla Corte di Giustizia UE, che si è pronunciata affermando che: « La direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, (...) la direttiva del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, (...) la direttiva del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, (...) e la direttiva del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE (...), non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per

« *Scarlet* c. *Sabam* » e « *Sabam* c. *Netlog* »[101], nelle quali partendo da una lettura in chiave « estensiva » dell'art. 2, lett. *a*) della direttiva 95/56/CE[102], si è voluta rimarcare la natura di « dato personale » degli indirizzi IP.

Proprio attorno a questo assunto centrale, i giudici della Corte del Lussemburgo hanno valutato il corretto bilanciamento tra le istanze di tutela del *copyright* rivendicate dall'istante società degli autori ed editori belga e gli interessi contrapposti dei convenuti, nello specifico un ISP (*Scarlet*) e un *social network site* (*Netlog*), nel caso di sospetta violazione del diritto d'autore da parte dei propri utenti abbonati o registrati.

Il verdetto finale, nel caso di specie ha visto affermare la preponderanza, sul « piatto » della « bilancia comunitaria », del diritto alla privacy (ma anche del diritto alla libertà d'impresa e di informazione), a scapito della necessità, sostenuta dalla *collecting society* belga, di imporre agli ISP misure di autotutela tecnologica che attraverso l'attività di filtraggio preventivo dei contenuti e delle azioni poste in essere dagli utenti — nonché la raccolta degli indirizzi IP — avrebbero garantito una maggiore tutela degli interessi dei titolari di diritti di privativa.

Secondo i giudici della Corte invece « *l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso suddetti utenti* »[103].

Qualche mese dopo la Corte ha indirettamente confermato la natura di « dato personale » dell'indirizzo IP reputando però legittima la richiesta di un singolo titolare di diritti d'autore residente in Svezia, di vedere applicata la disciplina sulla tutela del diritto d'autore vigente in quel Paese, nella parte in cui prevede che il titolare di opere protette possa ingiungere

garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile ». V. Corte di Giustizia UE, Sentenza C-275/06 del 29 gennaio 2008, *Promusicae c. Telefonica de Espana SAU*), in *Racc.*, 2008, pp. I-271 e ancora in questa *Rivista*, 2008, p. 182 ss.

[101] Corte di Giustizia UE, Cause C-70/10 del 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* e C-360/10 del 12 marzo 2012 *Belgische Vereniging van auteurs, componisten en uitgevers CVBA (SABAM) c. Netlog NV*, non ancora pubblicate ma entrambe reperibili all'URL: www.curia.europa.eu o, ancora, in questa *Rivista*, 2012, p. 303 ss., con nota di P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*. Sul punto, sia consentito rimandare a G. GIANNONE CODIGLIONE, *Corte di giustizia e diritto d'autore*, in *www.comparazionedirittocivile.it*, a cura di P. STANZIONE, pp. 1-7.

[102] Conformemente a quanto affermato nella direttiva 95/46/CE, per dato personale si intende « qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale ».

[103] Corte di Giustizia UE, Causa C-70/10 (*Scarlet c. Sabam*), cit., p. 303. Cfr. sul punto P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE*, cit., nel quale l'Autore, commentando in chiave critica le affermazioni della Corte sotto una prospettiva più precisa e tecnica, afferma come un indirizzo IP dinamico andrebbe in realtà considerato come un dato personale « incompleto » e « non pienamente formato », « proprio perché non vi sarebbe la corrispondenza tra indirizzo IP e la persona fisica ».

all'ISP di comunicare gli indirizzi IP e le generalità di soggetti anche solo « fortemente sospettati » di aver violato il diritto d'autore (e non dunque che abbiano commesso una violazione accertata), ai fini della loro identificazione e citazione in giudizio. Nella pronuncia in oggetto i giudici della Corte di Lussemburgo hanno reputato « equilibrato » e « proporzionato » il rapporto tra la normativa svedese e le leggi comunitarie sulla privacy e la *data retention* (con riferimento primario alle direttive CE 2006/24, 2002/58 e 2004/48/), confermando come il parametro dell'« adeguatezza » da applicare nell'attività valutativa di contemperamento tra tutele e diritti risulti estremamente flessibile e per certi versi « oscillante »[104].

La tendenza interpretativa affermata nelle pronunce *supra* citate pare inoltre trovare una conferma « *pro futuro* » negli esiti dei lavori condotti e prodotti, negli ultimi anni, dall'organo consultivo indipendente dell'Unione europea per la protezione dei dati denominato « *Article 29 working party* », inquadrati nell'ottica della riforma della disciplina « *data protection* » annunciata dalla Commissione europea nel gennaio del 2012[105].

I membri del gruppo, esponenti delle Autorità garanti della privacy delle varie nazioni UE, hanno modulato la loro opinione sul punto partendo da un'analisi delle nozioni complementari di *data subject* (interessato) e di *personal data* (dato personale) presenti nella proposta di Regolamento, al fine di definire e chiarirne ambito di applicazione e contenuti[106].

Per *data subject*, conformemente all'incipit dell'art. 4, punto 1 della proposta di regolamento andrebbe intesa « la persona fisica identificata o identificabile »: sul punto il gruppo specifica che per « identificabile » si dovrebbe intendere « quando, all'interno di un gruppo di persone, essa può essere distinta dagli altri membri del gruppo e di conseguenza essere trattata diversamente ».

[104] Corte di Giustizia UE, Causa C-461/10, 19 aprile 2012, *Bonnier Audio* c. *Perfect Communication*, non ancora pubblicata, ma reperibile all'URL: *www.curia.europa.eu* o in questa *Rivista*, 2012, pp. 283-297: « le direttive 2002/58 e 2004/48 devono essere interpretate nel senso che non ostano ad una normativa nazionale, come quella oggetto della causa principale, nella parte in cui tale normativa consente al giudice nazionale, dinanzi al quale sia stata proposta, da parte di un soggetto legittimato ad agire, domanda di ingiunzione di comunicare dati di carattere personale, di ponderare, in funzione delle circostanze della specie e tenuto debitamente conto delle esigenze risultanti dal principio di proporzionalità, i contrapposti interessi in gioco ».

[105] La riforma comprende una comunicazione strategica con la quale sono stati fissati dalla Commissione europea gli obiettivi da raggiungere e due proposte legislative, ovvero un regolamento che istituisce un quadro generale dell'Unione per la protezione dei dati e una direttiva sulla protezione delle persone fisiche con riguardo al trattamento dei dati a fini di prevenzione, indagine, accertamento o perseguimento dei reati e nell'ambito delle connesse attività giudiziarie.

[106] Cfr. Parere 1/2012 - WP 191, « *Sulle proposte di riforma in materia di protezione dei dati* », adottato il 23 marzo 2012; Parere 2/2008 - WP150, « Sul riesame della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, adottato il 15 maggio 2008; Parere 1/2008 - WP148, « *Sugli aspetti della protezione dei dati connessi ai motori di ricerca* », adottato il4 aprile 2008; Parere 4/2007 - WP 136, « *Sul concetto di dati personali* », adottato il 2 giugno 2007 e, ancora il Parere WP 37, « *Tutela della vita private su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line* », adottato il 21 novembre 2000. Tutti i pareri sono consultabili in lingua italiana presso la pagina web dell'Autorità garante per la protezione dei dati personali (*www.garanteprivacy.it*).

Ancora, rispetto alla nozione di *personal data*, il parere adottato esprime orientamenti divergenti rispetto al contenuto del Considerando 24 della proposta di regolamento, per cui, numeri identificativi, dati localizzativi, identificativi *on-line* e altri specifici fattori non andrebbero necessariamente considerati, in ogni circostanza, alla stregua di dati personali.

Secondo le opinioni maturate e applicando un criterio « estensivo » e « di protezione » che fa seguito al significato di « individuabilità » *supra* descritto infatti, i dati personali, considerati quali « dati relativi ad una persona individuabile » andrebbero intesi nel senso di dati « che si riferiscono all'identità, al comportamento, alle caratteristiche di un individuo o ancora se gli stessi vengono utilizzati per determinare o influenzare il modo in cui un determinato soggetto è trattato e valutato »[107].

La proposta formulata dal gruppo *Article 29* rimarcherebbe pertanto la necessità di una modifica del Considerando in analisi, al fine di prevenire possibili interpretazioni « restrittive » della normativa e dando seguito ad una visione — già ampiamente condivisa negli anni passati dal gruppo[108] — che include l'indirizzo IP all'interno della categoria dei *personal data*, alla stregua dei *cookies*.

Quanto invece alla natura di « prova » dell'indirizzo IP, anche rispetto alle reti WLAN pubbliche, il gruppo di lavoro sostiene che gli IP *adresses* debbano essere considerati degli « identificatori » ovvero quelle particolari informazioni che hanno un rapporto stretto e privilegiato con la persona interessata e, nello specifico, che potrebbero concorrere all'identificazione o all'identificabilità « indiretta » della stessa (solo in possesso del nome si avrebbe un'identificazione « diretta »)[109].

Atteso che « per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona »[110], il gruppo *Article 29* ha argomentato ritenendo possibile, per i fornitori di accesso internet o i gestori delle reti, identificare « ragionevolmente » gli utenti internet poiché normalmente, essi « registrano » in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato: essi andrebbero intesi come dati personali[111] con-

[107] *Article 29 Working party*, parere WP136, cit., p. 10.

[108] V. F. LAH, *Are IP Adresseses « Personal Identifiable Information »?*, in *I/S: A Journal of Law and Policy*, 2008, pp. 676-703. e, ancora, J. HELMINK, *Article 29 Working Party: Protecting Consumer's Personal Data*, in *www.peterswire.net*.

[109] Sul tema dell'identificabilità il gruppo precisa che « Per quanto concerne le persone identificate o identificabili "indirettamente", questa categoria rimanda tipicamente al fenomeno delle "combinazioni uniche", siano esse ampie o ridotte. Nei casi in cui, a prima vista, gli identificatori disponibili non consentono di identificare una persona particolare, si può ancora considerare quella persona "identificabile" perché quelle informazioni combinate con altre (che siano o meno conservate dal responsabile del trattamento) consentiranno di distinguerla dalle altre ».

[110] Considerando 26 del preambolo della direttiva 95/46CE.

[111] *Article 29 Working party*, parere WP36, p. 22: « I fornitori di accesso Internet e i gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP, poiché, normalmente, essi "registrano" in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet. Lo stesso dicasi per i fornitori di servizi Internet, i quali detengono un registro sul server HTTP. In questi casi, non vi è dubbio sul fatto che si possa parlare di dati personali ai sensi dell'articolo 2 a) della direttiva ».

cernenti una persona identificabile e, quindi andrebbero ricompresi di diritto nell'ambito di protezione della direttiva privacy.

L'applicazione e l'utilizzo dell'« insieme dei mezzi » ai fini dell'identificazione dovrà pertanto basarsi su criteri di ragionevolezza, ovvero contemplare tutti i fattori in gioco, quali il costo, le modalità e sopratutto le finalità del trattamento, il vantaggio atteso dal responsabile del trattamento o, ancora, l'interesse dei singoli, come pure il rischio di disfunzioni organizzative (es. violazioni degli obblighi di riservatezza) e tecniche[112].

Nello specifico caso in cui il trattamento di indirizzi IP viene effettuato per identificare gli utenti di un computer, come per il perseguimento dell'autore di una violazione del *copyright* da parte del titolare, secondo l'opinione dei membri del gruppo il responsabile del trattamento avverte che « i mezzi che potrebbero essere ragionevohnente utilizzati » sono disponibili, ad esempio, su richiesta del giudice della Corte adita, « altrimenti la raccolta delle informazioni non avrebbe senso »: per questi motivi, anche nell'ambito della tutela del diritto d'autore nel mondo digitale, gli indirizzi IP andrebbero considerati dati personali ai sensi della direttiva privacy.

Infine, nell'ambito delle reti WLAN pubbliche (ad esempio gli *internet cafè*), il gruppo *Article 29* ha confermato la difficoltà di offrire una sicura identificazione dell'utente, operata « con mezzi ragionevoli », sopratutto vista la variabilità di alcuni parametri tecnici (il tempo di connessione o la mancata registrazione del fruitore occasionale), ribadendo dall'altra parte la necessità di imporre in capo agli ISP un obbligo generale di trattamento di tutti gli indirizzi IP quali dati personali, stante l'impossibilità per gli stessi gestori di operare *ex ante* una distinzione tra informazioni (o meglio identificatori) riguardanti « soggetti identificabili » o « non identificabili ».

Anche il Garante europeo per la protezione dei dati personali negli ultimi anni si è pronunciato numerose volte sull'argomento.

L'opinione rilevabile dalla lettura di alcuni pareri sul tema della conservazione dei dati relativi al traffico per fini investigativi e il dibattito sulla neutralità degli ISP nell'ambito delle tecniche di monitoraggio e filtraggio, pare contemplare in via generale l'assoggettabilità dell'indirizzo IP — inquadrato come « dato relativo al traffico » — al regime dei dati personali[113], con una premessa (o un « motivo di dubbio ») rappresentata dal fatto che « *i dati relativi al traffico e i dati relativi all'ubicazione non sono sempre legati a una determinata persona, pertanto la conoscenza di un numero telefonico (o di un indirizzo IP) non rileva necessariamente*

[112] *Article 29 Working party*, parere WP136, cit., p. 15.

[113] Cfr. il Parere del GEPD in merito ai negoziati attualmente condotti dall'Unione europea per il raggiungimento di un accordo commerciale anticontraffazione (ACTA), in GUUE n. c 147 del 5 giugno 2010: « se si considera la definizione dei dati personali contenuta nell'articolo 2 della direttiva 95/46/CE (...), non si può che concludere che gli indirizzi IP e le informazioni sulle attività collegate a questi indirizzi costituiscono dati personali in tutti i casiqui rilevati. Infatti, un indirizzo IP serve come numero identificativo che consente di scoprire il nome dell'abbonato al quale è stato assegnato tale indirizzo IP. Inoltre, le informazioni raccolte a proposito dell'abbonato che possiede quell'indirizzo IP (''ha caricato un determinato materiale sul sito web ZS alle 15.00 del 1 gennaio 2010'') si riferiscono e attengono chiaramente alle attività di una persona identificabile (il possessore dell'indirizzo P) e devono pertanto essere considerati dati personali ».

l'identità di una persona »[114]. Queste argomentazioni sono inoltre espresse nell'ottica dell'applicazione del principio di proporzionalità alle attività di controllo e monitoraggio del traffico in rete e nel rispetto dei parametri di adeguatezza e ragionevolezza richiamati dalla direttiva sulla protezione dei dati personali e dai pareri del gruppo *Article* 29.

Ciò che emerge dall'analisi delle prospettive *in fieri* della nuova regolamentazione sulla privacy è la volontà di affrontare la tematica di cui si discorre « virando » verso una nuova sintesi del concetto « comunitario » di dato personale — che potremmo definire « 2.0 » — certamente più flessibile, « dinamico » e protettivo.

L'auspicio è che tali strumenti normativi diventino il fulcro di una tutela più efficace e trasparente degli utenti rispetto alle nuove « insidie » rappresentate dall'esponenziale crescita del *web* 2.0 e di veri e propri fenomeni « economici » quali, ad esempio, le piattaforme di *social networking*[115], non sacrificando dall'altra parte prerogative fondamentali — valide nella rete come nel mondo reale — quali il diritto all'anonimato o, ancora, la necessità di garantire una tutela giurisdizionale dei diritti quanto più equa, proporzionale e « bilanciata »[116].

[114] Parere del GEPD sulla proposta di direttiva del Parlamento europeo e del consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE, in GUUE, n. c 298/1 del 29 novembre 2005, p. 4. In un altro parere il GEPD descrive il procedimento di invio e ricezione di dati divisi per « pacchetti » operato dagli ISP, costruendo un parallelo con il servizio postale: nel *payload* IP si rinverrebbe il contenuto delle comunicazioni, destinate esclusivamente al destinatario (ovvero la lettera custodita all'interno di una ideale busta); l'*header* IP rappresenta invece la busta, poiché contiene tra l'altro, gli indirizzi del destinatario e del mittente. Il Garante infine specifica come, in via generale, come questo processo sia contraddistinto dalla maggiore neutralità possibile, con un approccio « senza memoria », per cui tra un passaggio dei pacchetti di informazioni da un nodo ad un altro non vengono conservate ulteriori informazioni del router. V. Parere del GEPD « *Sulla neutralità della rete, la gestione del traffico e la protezione della vita privata e dei dati personali* », in GUUE n. c 34 del 8 febbraio 2012.

[115] Sul tema, v. tra gli altri S. Sica-G. Giannone Codiglione, *Social network sites e il « labirinto » delle responsabilità*, in *Giur. merito*, 12, 2012, pp. 2714-2733 e S. Vigliar, *Consenso, consapevolezza e responsabilità nei* social network sites, Padova, 2012.

[116] Cfr. Sul punto l'art. 1, par. 3-*bis*, direttiva 2009/140/CE, per cui « I provvedimenti adottati dagli Stati membri riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, devono rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario.

Qualunque provvedimento di questo tipo riguardante l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione dev'essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo. Tali provvedimenti possono di conseguenza essere adottati soltanto nel rispetto del principio della presunzione d'innocenza e del diritto alla privacy. Dev'essere garantita una procedura preliminare equa ed imparziale, compresi il diritto della persona o delle persone interessate di essere ascoltate, fatta salva la necessità di presupposti e regimi procedurali appropriati in casi di urgenza debitamente accertata conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Dev'essere garantito il diritto ad un controllo giurisdizionale efficace e tempestivo ».

9. Soluzioni diverse per un problema attuale: quale bilanciamento?

Gli elementi raccolti in questa breve e incompleta analisi si ricongiungono in un quadro difficile e per certi versi contraddittorio.

La necessità di garantire una sempre più capillare diffusione della « rete » deve ritenersi senz'altro un fondamentale obiettivo per qualunque società che punti al raggiungimento in tempi brevi di elevati standard di sviluppo e progresso sia tecnologico che culturale: a questo però si deve sempre accostare il dovere posto in capo ad ogni Stato di garantire che tale sviluppo si realizzi in modo equilibrato, formando primariamente la consapevolezza etica e sociale di ciascun utente e in secondo luogo approntando un sistema di rimedi che garantisca una risposta il più snella, imparziale e efficace possibile al fenomeno degli illeciti su internet[117].

In questo panorama, il problema della responsabilità degli intestatari di connessioni internet si scontra con la « paura » di incorrere nel vuoto normativo che si concretizzerebbe nei casi di « illecito commesso da persona non individuabile »[118].

Ad ogni modo, alla luce dell'indagine svolta, l'indirizzo IP, nella sua accezione statica o dinamica, non appare elemento inconfutabile ai fini dell'identificazione del soggetto che opera sul *web*: esso è infatti un mero dato tecnico, spesso « fluttuante », che conchiude la « traccia » della dinamica intercorsa in un dato lasso di tempo tra un utente, un terminale e la rete. Per tali motivi esso potrebbe essere al massimo considerato un dato personale « relativo », poiché solo rapportato ed accostato ad altri elementi

[117] A questo proposito si v. G.M. Riccio, *La responsabilità degli internet* service provider. *Situazione legislativa e problemi aperti*, cit., p. 170, il quale sottolinea come l'esigenza di perseguire i reali autori degli illeciti debba essere ritenuto un obiettivo primario da raggiungere, strumentale a « funzionalizzare » la regolamentazione della rete, soprattutto in rapporto al ruolo degli ISP e al rischio che essi, all'interno del rapporto « trilaterale » tra danneggiante, intermediario e danneggiato, siano tenuti a dover sempre rispondere delle condotte illecite poste in essere in internet, rimanendo l'unico terminale di « sfogo » di tale sistema di responsabilità. Sulla questione, ampiamente dibattuta in dottrina e giurisprudenza ma ancora non pacifica e in continua evoluzione cfr. Id., *La responsabilità civile degli internet* provider., cit., p. 36 s. e p. 65 ss.; G. Ponzanelli, *Verso un diritto uniforme per la responsabilità degli internet* service providers, in S. Sica-P. Stanzione (a cura di), *Commercio elettronico e categorie civilistiche*, Milano, 2002, p. 368 ss.; E. Montero, *La responsabilité des prestataires intermédiaires sur les réseaux*, in AA.VV., *Le commerce électronique européen sur les rails ? Analyse et propositions de mis en uvre de la directive sur le commerce électronique*, Bruxelles, 2001; A.C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringment, Enterprise Liability and the First Amendment*, in *88 Georgetown L.J., 2000*, p. 1833 ss.; D. Lichtman-E. Posner, *Holding Internet Service Providers Accountable*, in *John M. Olin & Economics working paper*, no. 217, Chicago, 2004. V. anche A. Mantelero, *La responsabilità on-line: il controllo nella prospettiva dell'impresa*, in questa *Rivista*, 2010, p. 405.

[118] V. L. Vignudelli, *Il gestore del forum: spunti su identificazione dell'utente, anonimato e (ir)responsabilità*, in questa *Rivista*, 2011, 1, p. 107. V. anche F. Di Ciommo, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line. *A proposito della sentenza Google/Vivi Down*, cit. Più in generale sul concetto di « danno anonimo » nel sistema della responsabilità civile cfr. J. Josserand, *La responsabilità du fait de choses inanimées*, Paris, 1897, p. 7 e S. Rodotà, *Il problema della responsabilità civile*, cit., p. 23 ss.

e circostanze può concorrere a fornire un'indicazione corretta e « piena » sulla reale identità dell'utente.

Pertanto, la raccolta dell'indirizzo IP, assunta a metodo di imputazione « assoluto » in una fattispecie di responsabilità di così difficile lettura, si rivela non equilibrata e poco corretta sul piano tecnico-giuridico, così come inutili e controproducenti ai fini della crescita del « tecno-diritto » appaiono le « crociate » anti-pirateria combattute a forza di lettere e carta bollata che continuano a perpetrarsi in danno di utenti e consumatori.

Dati gli spunti che emergono dalle più moderne tendenze giurisprudenziali, l'impressione è che tra gli interpreti si faccia strada la volontà di trovare una ragionevole stabilità del sistema, in primo luogo soppesando, caso per caso, la reale entità dell'illecito e del conseguente danno subito e mirando a garantire una sicurezza « minima » delle reti a banda larga (che favorisca una diffusione armoniosa della cultura del « *free* Wi-Fi ») oltre che un'adeguata attività istruttoria e probatoria ai fini dell'individuazione del reale autore dell'illecito: la speranza è che dall'altra parte non si trascenda nell'imposizione di eccessivi, gravosi e difficilmente verificabili obblighi di vigilanza o protezione e di insuperabili, « diaboliche » presunzioni di colpa (o improbabili fattispecie di « *negligence copyright infringement* ») a carico degli intestatari di *account* privati.

Abstract

The paper deals with the role of IP addresses in the general frame of internet liabilities and with the debate on « open Wi-Fi » networks. The Courts of several countries (from United States to Europe) recently hold on this aspect, with different views, often considering IP addresses as personal data.

Starting from an analysis of the relations between Courts decisions and national regulations, the paper will also take into account the debate on the new EU data protection regulation proposal.

The need of prosecuting the offenses, while ensuring net neutrality, is therefore one of the most important challenges for the future of ICT law, in the light of a difficult balance between solidarity and law effectiveness and with respect to the growth of a « new » fundamental right: the right to internet access.