CALLER ID SPOOFING

Analisi civilistica e interdisciplinarietà del fenomeno

GIORGIO GIANNONE CODIGLIONE

Sommario: 1. Introduzione – 2. Brevi cenni su un fenomeno globale. – 3. La *Federal Communications Commission* e il "*Truth in Caller* ID *Act of 2007*". – 3.1 La sentenza Martinez – 3.2 La commercializzazione in Europa e il brevetto *Spoofcard*. – 4. *Caller Id act of 2009*. – 4.1 *Penalties*. – 4.2 *Enforcement by states, Venue service or process*. – 4.3 *Caller* ID *information, Caller ID service*: definizioni. – 5. *The Federal Communications Commission's Notice of Proposed Rulemaking*: attuazione e implementazione del *Caller* ID *Act of 2009*. – 5.1 Responsabilità degli *spoofing providers,* diritti della personalità, privacy*:* I riferimenti impliciti della Commissione. – 6. Diritti della personalità e New Technologies in Europa e in Italia: L'identità digitale. – 7. Prospettive di tutela. –

1. – Con l'adozione del "*Caller ID Act of 2009*"[1], discusso e approvato tra il mese di febbraio e quello di dicembre 2010 dalla *House of Rapresentatives* e dal *Senate*[2] degli Stati Uniti d'America e definitivamente dotato di forza di legge dal presidente Barack Obama il 22 Dicembre del 2010, si pongono nell'ordinamento nordamericano dei limiti normativi al fenomeno dello "*spoofing*", tecnica di manipolazione dell'identità personale che può essere posta in essere attraverso l'uso di molteplici tecniche informatiche e di comunicazione: *hostname* fittizi, indirizzi *ethernet* falsi, invio di e-mail contenenti allegati apparentemente innocui.

Nel caso del "*caller* ID *spoofing*" si opererebbe un "mascheramento" del c.d. ID[3] chiamante, ovvero del numero di telefono che apparendo sul display di un qualunque apparecchio telefonico mobile (eccetto quando il soggetto si celi dietro un "anonimo"), permette di identificare il soggetto che sta effettuando la chiamata attraverso appunto l'associazione del numero all'utenza telefonica chiamante[4].

Da qualche anno a questa parte, grazie anche alla diffusione delle comunicazioni che fanno uso di servizi interconnessi attraverso il *voice over internet protocol* (VoIP), il multiforme universo di servizi offerto dalla rete telematica ha lanciato in vasta scala una massiccia campagna di *advertising* avente come oggetto alcuni *software* "*download and install"* che

---

[1] 111th Congress 2nd Session, S.30.

[2] Nello stesso periodo, la *House of Rapresentatives* e il *Senate* approvavano un "*Act*" dai contenuti analoghi, denominato "*Caller* ID *Act of 2010*". Vedi 111th Congress 2nd Session, Union Calendar No.264, H.R. 1258; Report No. 111-461.

[3] Per ID si intende in generale un *token* (blocco di testo) lessicale che denomina delle entità, in un concetto analogo a quello di "nome". Così l'enciclopedia *on-line* Wikipedia.

[4] Vedi lo schema riprodotto nell'appendice del presente articolo.

permettono di "celare", ma sopratutto creare, un effetto di "alterazione" del reale numero di telefono al quale dovrebbe essere associato la chiamata posta in essere e che in molti casi sarebbe strumentale a configurare fattispecie di illecito quali il furto d'identità, lo *stalking*, le molestie nonché permettere un accesso improprio alle *voicemail* di ignari utenti[5] o permettere di cambiare il proprio timbro di voce durante la telefonata stessa, traendo ulteriormente in inganno il ricevente.

2. – La nascita del *caller* ID *spoofing* è da fare coincidere con il medesimo segmento temporale in cui si ebbe la creazione del concetto di *caller ID number*[6].

Per oltre un decennio, lo *spoofing* del numero identificativo chiamante infatti veniva utilizzato dalle imprese quale strumento per poter fruire di linee telefoniche aventi tutte il medesimo numero di telefono (in certi casi si riusciva ad ottenerne sino a 23), a fronte però dell'accesso ad onerosi sistemi PRI (*Primary Rate Interface*)[7].

Intorno alla fine degli anni '90, questo fenomeno fu posto al centro di maggiori attenzioni dal punto di vista commerciale: molte agenzie di investigazione privata si garantivano infatti l'esclusiva d'uso delle già citate linee PRI al fine di rivenderle ad altre colleghi ed agenzie e ad un prezzo nettamente superiore, dando vita così alle c.d. "linee cieche".

Questo tipo di accordi nascevano dall'esigenza di rendere fruibili ai soggetti interessati servizi di linea che garantissero l'anonimato, facendo sì che il proprio ID chiamante reale non venisse palesato al soggetto ricevente.

Contestualmente al fenomeno delle "linee cieche" prese corpo l'attività dei primi *hackers* telefonici, i c.d *phreaks*[8], mirata a dar vita ai primi tentativi di utilizzo di questo strumento per scopi privati, illegali e fraudolenti, ma ancora di carattere "artigianale" e molto spesso di scarsa efficacia[9].

Partendo dai sopracitati primi tentativi si è innescata una repentina attività di sperimentazione (prima) e lancio commerciale (poi), di siti *web* e applicazioni dedicate che dal 2004 ad oggi hanno portato lo *spoofing* telefonico a divenire un *business* fiorente, oltre che a divenire un argomento molto dibattuto, in tema di *privacy* e difesa dell'identità personale,

---

[5] Vedi *Truth in Caller ID Act, Report of the Committee of Commerce, Science and Transportation* in S.30, S. REP. NO. 111-96, 1-2 (2009) e inoltre la relazione del Dipartimento di giustizia statunitense (DOJ) inviata alla *Federal Communications Commission* il 18.04.2011.

[6] Vedi sul tema S. SICA, *La riservatezza nelle telecomunicazioni: l'identificazione del chiamante nell'esperienza inglese e nella prospettiva comunitaria e italiana*, in *Dir. inf.*, 2, 1997, pp. 219-247.

[7] Linee fornite dagli operatori telefonici locali.

[8] *Phreaking* è un termine gergale coniato per descrivere l'attività di persone che studiano, sperimentano, o sfruttano, per *hobby* o utilità, i telefoni, le compagnie telefoniche, e i sistemi che compongono o sono connessi alla *Public Switched Telephone Network* (PSTN).

[9] Vedi sul tema AA.VV, *The internet: Laws and regulatory regimes*, II, a cura di D. CAMPBELL, Salisburgo, 2009.

in special modo all'interno degli ordinamenti giuridici dei paesi del nordamerica oltre che, in misura minore, degli stati europei.

3. –Negli Stati Uniti già nel 2006 la FCC (*Federal Communications Commision*)[10] aveva istruito sul tema alcuni procedimenti finalizzati a far luce su taluni servizi di comunicazione offerti da alcuni dei maggiori portali web del settore (*SpoofCard* e *Telespoof*)[11].

Queste indagini avevano però incontrato limiti di competenza territoriale collegati all'individuazione della reale ubicazione fisica delle sedi legali di queste società, che infatti si trovavano al di fuori della giurisdizione degli Stati Uniti (nello specifico, in Canada).

In contemporanea, nel 2006 la Camera dei Rappresentanti e il Senato intraprese una "battaglia" contro l'utilizzo dello *spoofing* per fini fraudolenti, dando vita al "*Truth in Caller* ID *Act of 2007*"[12], primo disegno di legge redatto a tal uopo, il quale recitava testualmente:

"It shall be unlawful for any person within the United States, in connection with any telecommunications service or VoIP service, to cause any caller identification service to transmit misleading or inaccurate caller identification information, with the intent to defraud or cause harm", (…) *"Nothing in this subsection may be construed to prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information"*.

Veniva così prevista l'illiceità degli atti posti in essere da qualsiasi persona all'interno degli Stati Uniti in relazione a tutti i servizi di telecomunicazione che rendevano possibile un servizio di identificazione del chiamante, la trasmissione di informazioni di identificazione del chiamante fuorvianti o inesatte utilizzati con l'intento di frodare o causare danni, facendo salvo il diritto di qualsiasi utente di bloccare o schermare la proiezione verso l'esterno del proprio ID chiamante.

Inoltre, il disegno di legge in analisi introdusse due definizioni fondamentali ai fini dell'inquadramento della fattispecie, quella di *caller* ID *information* e *caller* ID *service* (che analizzeremo approfonditamente *infra,* con riguardo all'*Act* del 2009 dotato recentemente di forza di legge), oltre che a fare espresso riferimento alle comunicazioni che avvengono attraverso l'utilizzo del VoIP*, voice over internet protocol.*

Il *Caller* ID *Act of* 2007 specificava che tale servizio "consente comunicazioni in tempo reale sfruttando il procollo TCP/IP o simili, gratuitamente o a pagamento", "viene offerto al pubblico", e "ha la capacità di originare traffico in uscita o in alternativa porre fine al traffico in entrata proveniente dai *networks* telefonici pubblici"[13].

---

[10] Agenzia Indipendente del Governo degli Stati Uniti d'America per le Comunicazioni.

[11] http://www.spoofcard.com; http://www.telespoof.com.

[12] Il testo integrale del *Truth in Caller ID Act of 2007* è rintracciabile all'indirizzo: http://www.govtrack.us/congress/billtext.xpd?bill=h110-251.

[13] H. R. 251 (Report No. 110-188): *"(i) provides real-time voice communications transmitted through end user equipment using TCP/IP protocol, or a successor protocol, for a fee or without a fee;*

In conclusione, con riguardo al sopracitato "*Act*" bisogna aggiungere che esso non ha mai superato l'esame del Senato americano, a causa di caratteri connotati da vaghezza e imprecisione, ma può comunque considerarsi, analizzato in un quadro complessivo, un primo e importante esperimento, o tentativo legislativo sul tema.

Mentre gli organi legislativi discutevano e rigettavano il *Caller* ID *Act of* 2007 i casi di *spoofing* dilagavano nella vita quotidiana dei cittadini statunitensi, come dimostrò la polemica di carattere nazionale sorta per una moltitudine di telefonate di *telemarketing*[14], ricevute da alcuni utenti e provenienti da un ID chiamante che oltre a non essere quello reale, tradiva il consumatore facendo apparire sul display del proprio dispositivo telefonico il titolo di una famosa canzone degli anni 80, "867-5309/Jenny"[15].

3.1 – In contemporanea al clamore mediatico suscitato dalla vicenda di cui sopra, si rileva in giurisprudenza la prima condanna per *spoofing* posto in essere per fini fraudolenti, pronunciata dopo circa 10 anni dall'avvento di questo fenomeno in scala commerciale e mondiale[16] .

Nel 2007 infatti il tribunale di Dallas condannò il signor Guadalupe Santana Martinez e altri soggetti a 5 anni di carcere e al pagamento della somma di 24.000 dollari come risarcimento per essersi macchiati di crimini di *swatting* e *spoofing*.

Per *swatting* nello specifico si intese l'aver segnalato una falsa emergenza ad una squadra SWAT[17] indicando un indirizzo fisico presso il quale non si necessitava un intervento delle suddette forze speciali, o l'avere ricevuto una risposta da parte di unità di primo intervento a fronte di una chiamata di emergenza fatta provenire da un indirizzo fisico specifico, come ad esempio accade nei servizi di protezione civile.

I soggetti condannati infatti posero in essere delle chiamate al "911", il numero di pronto intervento per emergenza in uso negli Stati Uniti, sfruttando l'ID chiamante

---

(ii) is offered to the public, or such classes of users as to be effectively available to the public (whether part of a bundle of services or separately);

(iii)has the capability to originate traffic to, or terminate traffic from, the public switched telephone network".

[14] Contatto telefonico diretto, svolto mediante operatori commerciali, fra una o più aziende consociate e la clientela, attuale o potenziale, di tali aziende.

[15] "867–5309/Jenny", canzone scritta da Alex Call e Jim Keller ,interpretata da Tommy Tutone dall'album *Tommy Tutone 2*, edito dalla *Columbia Records*. Raggiunse il quarto posto nella classifica *Billboard Hot 100* e il primo nella *Billboard Top Tracks* nel 1982.

[16]Riguardo i crimini di *swatting* e *spoofing* commessi da Guadalupe Santana Martinez vedi: http://dallas.fbi.gov/dojpressrel/pressrel08/swattersentenced031208.htm.

Vedi anche sul tema il caso di Stuart Rosoff, Jason Trowbridge and Chad Ward, considerato dal dipartimento di giustizia degli Stati Uniti "uno dei più importanti casi di *swatting* mai registratosi, con più di 100 vittime": http://www.justice.gov/usao/txn/PressRel08/rosoff_trowbridge_ward_sen_pr.html.

[17] *Special Weapons And Tactics*, reparti scelti presenti in molti dipartimenti di polizia statunitensi.

"spoofato" di una persona ignara, con lo scopo di esercitare delle molestie, delle intimidazioni o per fini estorsivi.

Le chiamate al "911" vennero effettuate utilizzando "*spoofcards*"[18] facilmente reperibili e acquistabili sul Web e riuscirono a creare la falsa convinzione nelle unità di primo intervento che la chiamata provenisse realmente dalla residenza della vittima dello *spoofing*.

In quello stesso periodo, la FCC sviluppò all'interno della propria pagina *Web* una sezione apposita dedicata allo *spoofing*, col fine di informare in maniera adeguata i consumatori del rischio che correvano ignaramente[19].

3.2 – Infine, con riferimento alle prime iniziative riguardanti lo *spoofing*, bisogna aggiungere che anche in Europa a partire dal 2007 iniziarono a proliferare siti *web* che promuovevano servizi di *caller* ID *spoofing*: i primi casi si ebbero in Germania e in Gran Bretagna, dove un'azienda venne però costretta a chiudere il proprio dominio, a causa dell'intervento di carattere inibitorio dell' OFcom britannica *(Office of Communications)* e per il collegato timore dei possibili oneri di carattere legale che avrebbe potuto investire l'impresa stessa.

In parallelo temporale, negli Stati Uniti una serie di controversie legali si risolsero in favore di alcune *companies* della Florida, le quali poterono così tornare a commercializzare i servizi di *spoofing*[20].

Inoltre il portale web *Spoofcard* depositò e vide riconosciuto il suo brevetto da parte dell'USPTO (*United States Patent and Trademark Office*), rubricato sotto la dicitura di "Sistema e metodo per comunicazione telefonica anonima"[21].

4. – Con l'adozione del *Caller* ID *Act* o 2009, approvato e dotato di forza di legge con la ratifica presidenziale del 23 Dicembre del 2010, è stato emendato il "*Communications Act of 1934*" al fine di determinare la contrarietà a norme di legge del comportamento dei soggetti che, all'interno del territorio degli Stati Uniti, sfrutti la connessione con qualunque tipo di servizio di telecomunicazione o servizio voce IP per causare qualunque tipo di servizio di *caller identification* al fine di trasmettere consapevolmente dati dell'ID chiamante

---

[18] Per "*spoofcard*" la FCC intende "carte prepagate" acquistabili presso negozi autorizzati che permettono di avere accesso ai servizi di *spoofing*. FCC 11-100, WC Docket No.11-39, p.4.

[19] La pagina web è ancora attiva all'indirizzo: http://www.fcc.gov/cib/consumerfacts/callerid.html.

[20] Nello stato della Florida nel 2008 era stata introdotto un "*caller* ID *anti-spoofing Act*", il quale è stato però dopo pochi mesi reputato incostituzionale dalla corte distrettuale di Miami per violazione della "U.S. Constitution's Commerce Clause"(U.S. Constitution, Article I, Section 8, Clause 3).

[21] Il brevetto può essere consultato presso il sito del USPTO all'indirizzo:
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=7664242.PN.&OS=PN/7664242&RS=PN/7664242.

manipolati o non corretti, con l'intento di ingannare, danneggiare o ottenere illegalmente un vantaggio economico[22] .

Nella legge di recente approvazione è stato altresì previsto un sistema ibrido di "*penalties*", anche di carattere pecuniario[23] in aggiunta al regime della *General Penalty* disposto alla sezione 501 del *Communication Act*.

Come già era avvenuto nella stesura del 2007, è stato previsto che nessuna misura dovrà essere disposta con l'intento di ledere il diritto all'anonimato degli utenti che decidessero di avvalersene rendendo invisibile il proprio ID chiamante (il c.d. *caller* ID *blocking*[24]), al fine di tutelare la propria *privacy*[25]:

La legge ha ritagliato inoltre il medesimo trattamento di protezione con riguardo a tutte le "*authorized activity of a law enforcement agency or a court order that specifically authorizes the use of caller identification manipulation*", ovvero alle attività di tipo investigativo, di protezione o di intelligence di un agenzia di stato, una suddivisione politica di uno stato o di agenzie investigative degli Stati Uniti autorizzate per legge, oltre a tutte le attività che prevedono l'utilizzo della manipolazione del *Caller Id* che abbiano una specifica autorizzazione governativa.

4.1 – Come già anticipato *supra*, le misure sanzionatorie previste dal legislatore statunitense all'interno del *Caller Id Act of 2009* si dividono in due sezioni: una che prevede il pagamento di una sanzione di tipo pecuniario (*Forfeiture penalty*), l'altra che punisce le condotte volontarie e intenzionali (*Criminal fine*).

a) *Civil Forfeiture*

"Any person that is determined by the Commission, in accordance with paragraphs (3) and (4) of section 503(b), to have violated this subsection shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this paragraph shall be in addition to any other penalty provided for by this Act. The amount of the forfeiture penalty determined under this paragraph shall not exceed $10,000 for each violation, or 3 times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act".

---

[22] 111th Congress 2nd Session, S.30: "*It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value*".

[23] Vedi in merito il paragrafo 2.1, "*Civil Forfeiture*" e "*Criminal Fine*".

[24] Vedi sul tema 47 C.F.R. § 64.1601 (b) (2010).

[25] 111th Congress 2nd Session, S.30. *:"for prevent or restrict any person from blocking the capability of any caller Id service to transmit caller Identification information".*

Sul tema vedi anche il Decreto Legislativo 30 Giugno 2003, n.196 o "Codice in materia di protezione dei dati personali" che all' art.125 comma 1 e ss. prevede misure analoghe.

Come riportato testualmente *supra* la sanzione civile, o confisca, di stampo prettamente pecuniario che verrà applicata nei casi di *Caller* ID *manipulation* non potrà eccedere la somma di 10.000 *Us Dollars* per ogni violazione, o tre volte la somma citata per ogni giorno di violazione continuata, eccetto nei casi in cui l'ammontare fissato per ogni violazione protratta nel tempo non ecceda un totale di un milione di dollari per ogni singolo atto o tentativo, senza però oltrepassare la soglia limite di 1.000,000 di dollari.

b) *Criminal Fine*

"*Any person who willfully and knowingly violates this subsection shall upon conviction thereof be fined not more than $10,000 for each violation, or 3 times that amount for each day of a continuing violation, in lieu of the fine provided by section 501 for such a violation. This subparagraph does not supersede the provisions of section 501 relating to imprisonment or the imposition of a penalty of both fine and imprisonment*".

Anche nei confronti di coloro che volontariamente e intenzionalmente dovessero violare le prescrizioni poste dal *Caller* ID *Act* sono state previste sanzioni pecuniarie analoghe a quelle *supra* rubricate sotto la dicitura di "*Civil Forfeiture*" , senza escludere le misure previste dalla sezione 501 del *Communications Act* in tema di reclusione e pena coercitiva, imposizione di una penalty o la combinazione delle due pene[26].

4.2 – Riguardo ai profili applicativi, è stata posta, in capo ai "*Chief Legal officer*" di Stato (o ad ogni altro funzionario statale autorizzato), la facoltà di poter intraprendere iniziative e azioni civili (come la *parens patriae action* nella disciplina *antitrust*[27]) al fine di far osservare il disposto della legge in esame e applicare le sanzioni civili, ogni qualvolta essi abbiano ragione di credere che gli interessi dei residenti dello stato in questione possano essere stati minati o attaccati dalla violazione dell'*Act* in oggetto[28].

---

[26] 111th Congress 2nd Session, S.30.: *"Any person who willfully and knowingly does or causes or suffers to be done any act, matter, or thing, in this Act prohibited or declared to be unlawful, or who willfully and knowingly omits or fails to do any act, matter, or thing, in this Act required to be done, or willfully and knowingly causes or suffers such omission or failure, shall, upon conviction thereof, be punished for such offense, for which no penalty (other than a forfeiture) is provided herein, by a fine of not more than $10,000 or by imprisonment for a term of not more than two years, or both.".*

[27] Nella c.d. *parens patriae action* è lo stesso stato, o un suo organismo, a farsi carico di azionare la tutela per i suoi cittadini-consumatori, i cui interessi sono stati lesi dall'intesa anti concorrenziale. Vedi *The Clayton Antitrust Act, Section* 4C, nel quale si prevede che in alternativa ai rimedi generici (*damages and injiunctions*) i procuratori degli Stati Federali possano azionare delle *class actions* risarcitorie per l'ottenimento dei *treble damages* per conto dei consumatori.

[28] 111th Congress 2nd Session, S.30.: *"The chief legal officer of a State, or any other State officer authorized by law to bring actions on behalf of the residents of a State, may bring a civil action, as parens patriae, on behalf of the residents of that State in*

I funzionari legali di Stato dovranno altresì rendere notizia scritta alla *Federal Communications Commission* prima di poter intraprendere qualunque tipo di azione civile riguardante il *caller ID spoofing*, allegando altresì alla relazione una copia dell'azione stessa.

La Commissione stessa potrà avvalersi del diritto di costituirsi parte civile nell'azione, essere ascoltata e proporre richieste per l'appello. Il processo verrà tenuto in qualunque corte distrettuale degli Stati Uniti d'America che incontra i requisiti previsti nella sezione 1391, titolo 28 del USC (*United States Code*)[29].

Il processo inoltre dovrà essere condotto senza tener conto dei limiti territoriali del distretto o dello Stato nel quale è stata proposta l'azione, anche con riferimento alla residenza di tutti coloro che vogliano prendere parte ad un azione civile collettiva che abbia ad oggetto gli illeciti di cui *supra*.

4.3 – Nella redazione finale della legge statunitense sullo *spoofing* vengono inoltre riportate, come anticipato in precedenza, alcune sintetiche definizioni riguardanti l'oggetto della legge stessa: *caller* ID *information* e *caller* ID *service*.

"The term'caller ID information' means information provided by a caller ID service regarding the telephone number of, or other information regarding the origination of a call made using a telecommunications service, or Ip-enhabled voice service".

Per "*caller* ID *information*" il Congresso intende dunque le informazioni fornite ad un utente finale da un servizio di "*Caller* ID" riguardante il numero dell'utente chiamante o ancora altre informazioni sempre concernenti la "nascita" di una chiamata effettuata

---

an appropriate district court of the United States to enforce this subsection or to impose the civil penalties for violation of this subsection, whenever the chief legal officer or other State officer has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected by a violation of this subsection or a regulation under this subsection".

[29] 111th Congress 2nd Session, S.30: "*The chief legal officer or other State officer shall serve written notice on the Commission of any civil action under subparagraph (A) prior to initiating such civil action. The notice shall include a copy of the complaint to be filed to initiate such civil action, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such civil action. Upon receiving the notice required by subparagraph (B), the Commission shall have the right: '(i) to intervene in the action;'(ii) upon so intervening, to be heard on all matters arising therein; and (iii) to file petitions for appeal.*" E ancora: "*An action brought under subparagraph (A) shall be brought in a district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code*".

utilizzando qualunque tipo di "*telecommunication service*"[30] o servizio vocale IP, (primi tra tutti i già citati *supra* servizi VoIP).

Dall'altra parte, in tema di *caller ID service*, la legge[31] specifica che il termine si riferirebbe a qualunque tipo di servizio o "*device*"[32] designato per fornire all'utente il nome o il numero di telefono del chiamante o altre informazioni riguardanti l'origine di una chiamata fatta usando qualunque tipo di "*telecommunication service*" o servizi vocali IP, compresi gli "*automatic number identifications services*"[33].

Infine, nell'ultimo paragrafo della legge in questione è presente uno specifico rinvio ad una definizione tecnica di "IP-*Enabled Voice Service*" previsto dal "*Code of federal Regulations*"[34] .

5. – All'interno della legge in oggetto, approvata negli Stati Uniti nel dicembre del 2010, è inoltre stata prevista un'importante disposizione che ha investito la FCC (*Federal Communications Commission*) di pieni poteri volti al potenziamento dell'efficacia della legge in oggetto attraverso l' adozione di provvedimenti entro il termine di sei mesi dall'entrata in vigore del *Truth in Caller* ID *Act* of 2009[35].

Nel marzo del 2011 la Commissione stessa, nell'intento di porre in essere delle iniziative valide ed efficaci senza trascurare il contraddittorio ha diramato una *Notice of Proposed rulemaking* (NPRM), con la quale ha sollecitato e successivamente raccolto importanti relazioni sul tema da parte di organismi e associazioni quali il Dipartimento di Stato della Giustizia (DOJ), la ATIS (*Alliance for Telecommunications Industry Solutions*), la *National Cable and Telecommunications Association* e ancora la *Privacy rights Clearinghouse* (PRC) e la *National Network to End Domestic Violence* (NNEDV).

A seguito di questo periodo di "dialogo" tra commissione ed organismi interessati è stato emanato, nel Giugno del 2011, un "*Report and Order*" in tema di implementazione delle regole, strumentali all'attuazione del *Truth in Caller* ID *Act of 2009*[36], anche attraverso la

---

30 "Servizi di comunicazione vocale in tempo reale".

31 111th Congress 2nd Session, S.30: "*The term 'caller ID service' means any service or device designed to provide the user of the service or device with the telephone number of the caller or other information regarding the origination of a call made using a telecommunications service, or IP-enabled voice service. Such term includes automatic number identification services".*

32 "Dispositivo".

33 " Servizi di riconoscimento automatico del numero".

34 Vedi *Code of Federal Regulations*, 47 C.F.R. 9.3.

35 47 C.F.R. § 227 (e) (3): "*Not later than 6 months after the date of enactment of the Truth in Caller ID act of 2009, the Commission shall prescribe regulations to implements this subsection*". Secondo giurisprudenza affermata la FCC trarrebbe altresì legittimazione dal *Communications Act of* 1934, con il quale il Congresso dispose in favore della Commissione un ampia autorità sul tema della regolamentazione delle comunicazioni telefoniche interstatali (vedi *Global crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc.*, 550 U.S. 45,48 (2007)).

36 FCC 11-100, WC Docket No. 11-39.

modifica di alcune disposizioni, emanate nella metà degli anni '90, che disciplinano il CPN (*Calling Party Number*)[37].

La Commissione, con l'emanazione del seguente atto ha recepito all'interno del suo sistema la legge nazionale contro il *caller ID spoofing* ed ha introdotto altresì alcuni specifici "puntelli" che ampliano la portata della legge stessa e risolvono alcuni possibili dubbi interpretativi e applicativi.

In primo luogo con riferimento ai soggetti è stato introdotto, all'interno dei CPN *rules*, il termine entità (*entity*) a fianco del riferimento espresso al soggetto (*person*) previsto dall'*Act*, al fine di specificare che saranno perseguibili non soltanto le persone fisiche ma qualunque individuo, società, associazione, *joint-stock company*, consorzio monopolistico o ente privato, seguendo la consolidata definizione estensiva data dal *Communication Act*[38].

Altro tema discusso dalla commissione è stata la posizione all'interno della legge e l'adeguatezza dell' uso del termine "*knowingly*", il quale applica alla fattispecie il parametro della consapevolezza e che secondo la Commissione stessa, nel modo in cui è stato inserito all'interno del *Truth in Caller* ID *Act*, potrebbe indurre in errore l'interprete.

A seguito di un attenta analisi delle proposte, la Commissione ha rielaborato il dispositivo della legge che inquadra la fattispecie, posizionando il termine "*knowingly"* all'interno di una costruzione leggermente diversa rispetto all'originale, in modo tale da sottolineare che il soggetto (o entità) che consapevolmente causa una trasmissione, o l'apparizione sul display, di informazioni sul numero chiamante inaccurate o manipolate dovrà necessariamente essere lo stesso che sta operando con l'intento di frodare, causare un danno o ottenere un profitto indebitamente[39].

Nella nuova lettura del testo di legge si evince inoltre che la Commissione faccia espresso riferimento ad un'accezione globale dei servizi di *caller* ID ("*any caller identification service*") e dunque sottintenda l'inglobamento nella sopracitata categoria dei servizi voce IP e di tutti i servizi VoIP interconnessi.

5.1 – Sul tema della responsabilità degli *Internet Service Providers* (ISP) la Commissione, nella fase ricognitiva che ha preceduto l'emanazione del documento 11-39, ha ricevuto delle proposte da parte degli organismi interessati che hanno risposto attivamente all'input ricevuto, nel tentativo di disporre un rafforzamento degli obblighi previsti nei confronti dei c.d. *spoofing providers*.

Tra queste si ritiene degna di una breve analisi la proposta formulata dal Dipartimento di Giustizia, supportato dal procuratore generale del Minnesota, che auspicava l'adozione di una misura che obbligasse i *providers* pubblici che offrono servizi di

---

[37] Vedi 47 C.F.R § 64 (CC Docket No. 91-281, FCC 95-187).

[38] 47 U.S.C. §153(32).

[39] FCC 11-100, WC Docket No. 11-39, p.8: "*No person or entity in the United States shall, with intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information*".

caller ID *spoofing* ad operare un "*good faith effort*"[40] volto a verificare se l'utente possedesse o meno l'autorizzazione per disporre del numero di telefono utilizzato in sostituzione di quello "reale", ad esempio sottoponendolo ad una verifica telefonica.

La Commissione, nel suo *Order and Report* ha però rigettato la proposta del Dipartimento di Giustizia, non disponendo ulteriori obblighi che gravino sugli *spoofing providers* e dando così seguito ad un interpretazione che non snaturi la linea guida percorsa dal Congresso nell'emanazione della legge sullo *spoofing*, in un'ottica di bilanciamento tra le istanze di lotta allo *spoofing* "illecito" e quelle che difendono i benefici dello *spoofing* "legittimo".

Alla luce di quanto specificato dalla Commissione si evincerebbe altresì che le indicazioni date in merito ai soggetti imputabili del reato di *spoofing* andrebbero in alcune situazioni a coinvolgere gli stessi *providers*, vista la volontà espressa di colpire le entità e non solo i soggetti che consapevolmente causino, direttamente o indirettamente, un servizio di *caller* ID che trasmetta, o permetta la comparsa sul display, di ingannevoli o inesatti numeri identificativi.

Nello specifico la Commissione, nonostante si riservi di analizzare in maniera ampia e prendere decisioni in altra sede sul merito, ha specificato con un breve richiamo che sarebbero da ritenere altresì responsabili tutti gli *spoofing providers* che abbiano promosso e pubblicizzato i propri servizi verso il pubblico offrendoli come strumenti utili a porre in essere le figure di illecito espressamente proibite dall'*Act*.

La Commissione ha anche specificato che il riferimento al concetto di "azione indiretta" è stato introdotto per rafforzare la portata della legge e rendere dunque ammissibile la responsabilità del soggetto che ottenga gli effetti *supra* menzionati attraverso l'azione di una terza parte che ponga in essere materialmente la fattispecie di illecito[41].

Nel proseguire in questa rassegna sugli aspetti di rilevanza civilistica presenti all'interno delle disposizioni di implementazione emesse dalla Commissione per le comunicazioni, è opportuno riportare anche come essa abbia indicato una linea

---

[40] Testualmente "tentativo o sforzo in buona fede". Nella fattispecie, l'accezione di "buona fede" utilizzata in questa sede è da ricondurre ad una visione della *good faith* quale clausola oggettiva mutuata dal diritto dei contratti, che, discostandosi dalla visione tipica della *common law* britannica e avvicinandosi altresì alla posizione della *civil law*, si riferirebbe allo sforzo che una persona ragionevole, nella medesima situazione o circostanza, avrebbe posto in essere con diligenza e onestà. Così in *Troutt v. City of Lawrence*, 2008 U.S. Dist., in LEXIS 61641 (S.D. Ind. Aug. 8, 2008).

V.anche sul tema C. CASTRONOVO – S. MAZZAMUTO, in AA.Vv., *Manuale di diritto privato Europeo,* Milano, 2007, II, p.515-516 e I. MUSIO, *Breve analisi comparata sulla clausola generale della buona fede,* in *Comparazione e diritto civile,* p.35 ss.

[41] FCC 11-100, WC Docket No. 11-39, p.9: "We include the concept of "indirect" action in our rules to foreclose those acting with the requisite harmful intent from arguing that they are not liable merely because they have engaged a third party to cause the transmission or display of inaccurance or misleading caller identification information".

interpretativa del termine "*harm*", presente all'interno dell'*Act*, contestualmente al rigetto di un appello prodotto dalla NNEDV che chiedeva una maggiore precisione dei termini utilizzati dal legislatore.

Con questa puntualizzazione infatti la Commissione sottolinea come il fenomeno "*spoofing*" possa essere capace di colpire la persona nella sua sfera pubblica e privata, in un'accezione globale che consideri non solo i danni di carattere economico e finanziario ma soprattutto quelli che coinvolgono il soggetto nella sua fisicità ed emotività, ponendo in essere dunque un richiamo a quei "nuovi" diritti della personalità il cui sviluppo e ramificazione può essere senza dubbio considerato uno delle principali conseguenze ascrivibili alla nascita della società delle *Information and Communication Technologies*[42].

Viene inoltre sottolineato dalla Commissione come il fenomeno dello *spoofing* abbia di recente fatto scaturire dal suo interno una fattispecie denominata *caller* ID *unmasking*, che viene in certi casi offerta dai *providers* ai propri utenti al fine di dissimulare le telefonate, ricevute sotto la dicitura di "anonimo", che vengono composte da altri utenti che esercitano legittimamente il proprio diritto a fruite del blocco del proprio numero chiamante (*Caller* ID *blocking*).

Nonostante la stessa Commissione abbia affermato in questa sede di riservarsi di trattare successivamente e in maniera più ampia l'argomento in questione, essa non ha mancato di sottolineare l'inviolabilità dell'obbligo posto in capo alle società erogatrici di servizi di comunicazione di onorare le istanze di *privacy* degli utenti.

6. – I diritti della personalità[43] ricoprono un ruolo preminente nell'ordinamento comunitario, soprattutto dopo la proclamazione nel 2000 a Nizza della Carta dei diritti fondamentali dell'Unione Europea, che "pone la persona al centro della sua azione" e sempre nel medesimo preambolo solleva la questione fondamentale del contrasto tra innovazione e tutela dei diritti sottolineando la necessità di "rafforzare la tutela dei diritti fondamentali alla luce della evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici" [44]: la società appunto delle *Information and Communication Technologies*[45].

---

[42] FCC 11-100, WC Docket No. 11-39, p.9, nota 49: "*the term "harm" is a broad concept that encompasses financial, phisycal and emotional harm*".

[43] Sul tema dell'evoluzione delle teorie sui diritti della personalità vedi G.PINO, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Materiali per una storia della cultura giuridica*, 2003/1, pp.237-274.

[44] Vedi Gazzetta ufficiale delle Comunità europee (2000/C 364/01).

[45] Vedi sul tema, AA.VV., *Commercio elettronico e categorie civilistiche*, a cura di S. SICA - P. STANZIONE, Milano,2002; AA.VV., *Codice in materia di protezione dei dati personali*, a cura di G.CASSANO – S. ADDA, Milano, 2004; AA.VV, *Innovazioni tecnologiche e privacy*, a cura di G.RASI, Roma, 2005; AA.VV., *La nuova disciplina della privacy*, a cura di S. SICA - P. STANZIONE, Bologna, 2005; AA.VV., *Manuale di Diritto dell'Informazione e della Comunicazione*, a cura di S. SICA – V. ZENO ZENCOVICH, Padova, 2007; AA.VV., *Manuale di diritto dell'informatica*, a cura di D. VALENTINO, Napoli, 2011; P. CARETTA, *Diritto della comunicazione e dell'informazione*, Bologna, 2004;

Per una prospettiva di sintesi giuridica del fenomeno bisogna fare riferimento alle due trattazioni che regolano il tema della riservatezza e quello delle c.d. "comunicazioni elettroniche": Il Decreto legislativo 30 giugno 2003, n. 196, più comunemente chiamato "Codice in materia di trattamento dei dati personali" e il decreto legislativo n. 259 del 1 agosto 2003, "Codice delle comunicazioni elettroniche".

Due codici (nati dal recepimento di alcune direttive comunitarie che erano confluite, soprattutto in tema di *privacy*, in innumerevoli leggi) che sanciscono l' inderogabilità dei diritti di libertà delle persone nell'uso dei mezzi di comunicazione elettronica (art.3 D.Lgs 259/2003), "tenute salve le limitazioni derivanti da esigenze di difesa e sicurezza dello Stato, di protezione civile, di salute pubblica, di tutela dell'ambiente e di riservatezza e protezione dei dati personali"[46].

Inoltre, il codice delle comunicazioni fa richiamo ad un più ampio "diritto di iniziativa economica ed il suo esercizio in regime di concorrenza nel settore considerato", oltre che "alla libertà di fornitura di reti e servizi, dei quali si afferma la natura di preminente interesse generale"[47].

Proprio il concetto di concorrenza però si contrappone a quello di liberta' di comunicazione, poiché cela, nel suo assunto, la c.d. "*consumer welfare*" o tutela o benessere del consumatore, fine imprescindibile per uno sviluppo sano ed equilibrato del principio di concorrenza e dunque dell'efficienza del mercato.

Un corretto sviluppo sociale dunque "non dovrà da un lato comprimere la libertà di iniziativa economica e di concorrenza dei mercati di beni e servizi né dall'altro pregiudicare quella della persona in tutte le sue forme"[48].

Secondo le indicazioni comunitarie quindi non sarebbero da contemplare le sopracitate istanze "iperliberistiche" che hanno contraddistinto i primi passi della giurisprudenza americana in tema di diffamazione *on line* e responsabilità dei *providers* poichè

G.V. CARDARELLI – V. ZENO ZENCOVICH, *Trattamento dei Dati e tutela della persona*, Milano, 1998; G.CASSANO, *Diritto dell'Internet. Il sistema di tutele della persona,* Milano, 2005*;* A.M. GAMBINO – A. STAZI, *Diritto dell'informatica e della comunicazione,* Torino, 2009*;* J. HAGEL III – M. SINGER, *Net Worth: the emerging role of the informediary in the race for customer information*, Harvard, 1999, p. 275 ss.; D. IELO – L. MUSSELLI, *Concorrenza e regolazione nel nuovo codice delle comunicazioni elettroniche* in *Foro Amministrativo*: TAR, 2004, p.1952 ss; G. PINO*, I codici di deontologia nella normativa sul trattamento dei dati personali*, in *Danno e responsabilità*, n.4/2002, p.363 ss.; G.M. RICCIO, *La responsabilità civile degli internet providers*, Torino, 2002; S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995; S. SICA, *Il consenso del trattamento dei dati personali, metodi e modelli di qualificazione giuridica,* in *Riv.dir.Civ.*, n.6/2001, p.625 ss.; S. SICA, Sicurezza *e riservatezza nelle telecomunicazioni: il d.lgs n.171/98 nel "sistema" della protezione dei dati personali*, in *Dir.Inf.*, n.4-5 1998, p.777 ss.; S. VIGLIAR, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Dir.Inf.*, n.2/2003, p.423 ss.; V. ZENO ZENCOVICH, Sistema *giuridico e "diritto delle telecomunicazioni*", in *Dir.Inf.*, 1996, p.551 ss.

[46] Vedi V. D'ANTONIO - S. VIGLIAR, *Studi di diritto della comunicazione*, Padova, 2009, p.92.

[47] Vedi V. D'ANTONIO - S. VIGLIAR, *ibidem*, cit., p.92.

[48] Vedi V. D'ANTONIO - S. VIGLIAR, *ibidem*, cit., p.97.

"con la facilità di accesso ai servizi si gioca una buona parte del successo di mercato dei *providers*"[49], né dall'altra parte operare nell'ottica di un soffocamento della tutela dei diritti fondamentali dell'uomo rispetto all'uso delle *new technologies*.

A sottolineare l'attenzione comunitaria sul tema della tutela della persona si configura l'intervento del legislatore italiano in materia di *privacy*[50], cronologicamente anteriore all'emanazione del codice di comunicazione.

Esso pone l'accento sulla tutela della dignità e della libertà dei consumatori e utenti di servizi di telecomunicazione: è un codice per mezzo del quale il legislatore ha palesemente "rincorso" , l'evoluzione frenetica e a volte irriverente di un progresso tecnologico inarrestabile, ma con il quale ha dato dall'altra parte una consistenza unitaria a tutte le disposizioni di recepimento della direttiva europea 95/46/CE[51].

Diritto alla *privacy* o alla riservatezza che, rispetto alle *new technologies* deve essere modulato con riferimento agli interessi di chi vuole comunicare in maniera veloce ma in contemporanea anche di chi, "essendo oggetto della comunicazione ha diritto a vedere la propria sfera privata difesa da ingiustificate invasioni altrui"[52], nell'ottica della tutela del diritto all'anonimato, o *right to be alone*[53].

La direttiva del 1995 venne concepita per dare rilievo ad una disciplina nuova, quella attinente al progresso tecnologico, che con la stessa velocità con la quale porta e ha portato innegabili vantaggi ai fini delle comunicazioni e all'abbattimento delle distanze, non permette "l'individuazione preventiva di un ambito territoriale delimitato ma, al contrario, si fonda sulla totale indifferenza rispetto all'ubicazione fisica degli utenti o dei fornitori di servizi", con il conseguente verificarsi della c.d "morte della distanza"[54].

Con riferimento al c.d. "ID chiamante", all'art. 4 del Codice sulla *privacy*, che ospita un elenco predeterminato di sintetiche e puntuali definizioni atte a far chiarezza terminologica e concettuale sulla fattispecie oggetto di regolamentazione, vengono chiariti i concetti di "dato personale" [55] e "dati identificativi" [56].

---

[49] Vedi R. NATOLI, *Profili di diffamazione on-line: spunti dall'esperienza statunitense*, in *Internet e il diritto dei* privati, a cura di L. NIVARRA – V.RICCIUTO, Torino, 2002, p.91.

[50] D.Lgs. n.196 del 30/6/2003.

[51] Gazzetta Ufficiale delle Comunità Europee, n. L 281/31 del 23.11.1995.

[52] S. RODOTÀ, *Libertà, opportunità, democrazia e informazione*, testo della relazione introduttiva svolta dall'autore in occasione del Convegno promosso dal Garante per la protezione dei dati personali sul tema "Internet e privacy:quali regole?", tenutosi a Roma l'8 e 9 Maggio 1998, atti pubblicati nel supplemento n.1 al Bollettino n.5 dell'Autorità garante.

[53] Sul tema dell'anonimato vedi, tra glia altri la breve rassegna comparatistica di G.M RICCIO, *Diritto all'anonimato e responsabilità civile del provider,* in *Internet e il diritto dei privati*, cit., pp. 32 – 40.

[54] Vedi F. CAIRNCROSS, *The death of distance: how the communication revolution is changing our lives,* Boston, 2002.

[55] "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" Art 4, comma 1, lett. b), D.Lgs. n.196/2003.

Con la previsione dell'art.125 invece, analogamente a come è avvenuto nell'ordinamento statunitense, si assicura all'utente chiamante il "*Caller* ID *blocking*" (già citato *supra*), ovvero la facoltà di "impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea".

Ecco dunque configurarsi l'obbligo in capo all'operatore di rendere l'utente "padrone" del proprio diritto di apparire o meno col proprio numero sul display della persona chiamata, che si accosta al diritto di non rispondere o respingere la chiamata per il ricevente[57] e ancora nei confronti della compagnia telefonica al dovere di fornire, in maniera semplice e chiara i tabulati telefonici, o meglio "la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti addebitati per ciascuna conversazione"[58].

In questa maniera si contemplerebbe la tutela del c.d "anonimato parziale", che permetterebbe dunque di "risalire alla reale identità del soggetto agente, che sarà chiamato a rispondere direttamente dei danni eventualmente derivanti dal suo operato"[59], in analogia con quanto disposto per la responsabilità dell'intermediario, nella disciplina vigente del d.lgs 9 aprile 2003 n.70, il quale all'art.17 comma 2 prevedrebbe, nei casi di c.d. "*hosting*" un dovere in capo ai providers "di collaborazione, qualora richiesta dalle pubblica autorità competenti e, comunque, in presenza di illecito penale o amministrativo, specialmente mirata a fornire i dati di identificazione dei clienti"[60].

Posto il caso di un'utente che riceva una telefonata in entrata nella quale il chiamante abbia volutamente modificato (e non nascosto) i propri reali dati identificativi, o ancora li abbia sostituiti, sempre grazie all'uso di servizi di *spoofing*, con l'ID di un altro ignaro soggetto, ci si chiede quali conseguenze potrebbero scaturire da tale comportamento ma soprattutto quali diritti verrebbero violati da tale figura di illecito.

Sono innumerevoli i casi di soggetti che hanno sporto querela contro ignoti per casi di vero e proprio furto d'identità[61] o che abbiano comunque subito gravi danni economici o d'immagine, per aver ricevuto una "*spoofing incoming call*": affari perduti, salde relazioni sentimentali crollate per una chiamata o brutte ore trascorse dentro la propria casa circondati da un commando di unità speciali SWAT.

---

[56] "i dati personali che permettono l'identificazione diretta dell'interessato" Art 4, comma 1, lett. c), D.lgs. 196/2003.

[57] Art 125,comma 3, D.Lgs. n.196/2003.

[58] Art.124 comma 1 e ss., D.Lgs. n.196/2003.

[59] Così G.M RICCIO, *Diritto all'anonimato e responsabilità civile del provider,* in *Internet e il diritto dei privati*, cit., p.40.

[60] Così R. BOCCHINI, in *Manuale di diritto dell'informatica,* cit., p.145.

[61] Il c.d. furto d'identità in Italia è un reato punito con la reclusione fino a un anno ex art.494 c.p.. Vedi inoltre Cass.pen. Sez. V, 08.11.2007, n.46674.

Le compagnie che promuovono la vendita degli "*spoofing software"* si appellano al buon gusto dei propri utenti e raccomandano prudenza nell'azzardare chiamate di questo genere, a meno che non si facciano per fini semplicemente "goliardici" previo avvertimento della persona oggetto dello "scherzo": si giustificherebbe così l'uso dei servizi di *spoofing* celandoli dietro la c.d. fase ludica dell'utilizzo della rete, inquadrata dunque come vettore di intrattenimento piuttosto che come vettore economico[62].
Ma quante volte accade il contrario e soprattutto, cosa dovrebbe fare l'ordinamento giuridico per evitare o limitare il configurarsi di tali spiacevoli inconvenienti?

Sarebbe necessario appellarsi ai principi generali di tutela della dignità e libertà di ogni persona, libertà di espressione ma anche di veder riconosciuta in maniera chiara e indissolubile il diritto all'integrità della propria "identità digitale": per poter produrre effetti reali e durevoli nel tempo tale diritto dovrebbe essere accostato ad un senso di responsabilità maggiore da parte di tutti gli utenti e fruitori dei servizi telematici in genere, oltre che dai *providers* stessi.

Il consolidamento di un' "etica della responsabilità"[63] collettiva e condivisa da utenti e intermediari, visto non soltanto in rapporto con lo sviluppo di strumenti di *soft law* quali i codici di autoregolamentazione, renderebbe senz'altro più consapevoli i soggetti dei rischi che implica una partecipazione attiva, passiva o sporadica al mondo telematico e alla conseguente "frammentazione" del proprio "Io" tra *social network* e profili virtuali (corpo quindi visto nella sua integralità/duplicità, come corpo fisico ed elettronico[64]) e quindi anche del pericolo che si correrebbe in pochi attimi nel vedere distrutto, violato o "inquinato" il proprio diritto ad avere un nome, un cognome, un indirizzo, un recapito telefonico che sia realmente stato "voluto" e utilizzato non per fini "fraudolenti" o addirittura nel vedere infangata la propria reputazione e immagine[65].

Contestualmente a queste dinamiche insite nel rapporto tra reale e virtuale, persona e macchina, si configurerebbe, parallelamente alla sussistenza della propria identità personale, l'esistenza di una identità digitale[66], speculare alla prima ma al contempo multiforme e in alcuni casi "incontrollabile" da parte del soggetto a cui è legata.

---

62 Così E. TOSI, *Diritto privato dell'informatica e di internet*, Milano, 2006, p.56.

63 Sul tema vedi P. SAVONA, *Il terzo capitalismo e la società aperta*, Milano, 1993 e A. SCHIAVONE, *La sinistra del terzo capitalismo*, Bari, 1989.

64 Vedi P. MELL, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as property in the Electronic Wilderness*, in *Berkeley Technology Law Journal*, 11, 1996, p. 81 ss.

65 Vedi sul tema S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, II ed., Roma – Bari, p. 139 ss.

66 Vedi sul tema dello sviluppo diritto all'identità personale G. PINO, L'identità personale, in *Trattato di biodiritto*, diretto da S.RODOTÀ – P.ZATTI, I, a cura di S.RODOTÀ – M.TALLACCHINI, Milano, 2010, pp. 297-321; ID., *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali, in Libera circolazione e protezione dei dati personali*, a cura di R. PANETTA, Milano, 2006, I, pp. 257-321.

Nonostante il termine "identità digitale" pare non venga espressamente citato in nessuna normativa vigente, esso configurerebbe l'insieme "delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto"[67], in un'ottica che dovrebbe necessariamente contemplare l'aspetto "della tutela dell'identità personale in rete (specie nei suoi profili reputazionali) e quello delle tecniche di identificazione del soggetto a mezzo di strumenti informatici"[68].

Una figura dunque non statica ma "fluida" e "dinamica", che non viene più vista come dato preesistente, (ossia come proiezione esterna di un patrimonio individuale già delineato nelle sue caratteristiche distintive), bensì come processo, costantemente in atto, aperto ad una pluralità di esiti e continuamente esposto all'interferenza, capillare e pervasiva, delle varie forme di potere sociale"[69].

7. – Cosi' come si manifesta adesso in Europa, il fenomeno del *caller* ID *spoofing* analizzato *supra* potrebbe dunque arrecare ampi danni ai soggetti che fruiscono, abitualmente e non, di Internet e comunicazione cellulare.

Facile reperibilità, universalità d'uso e, una volta innescato il meccanismo di dissimulazione dell'ID, impatto visivo immediato e chiaro ne fanno una fattispecie difficile a prima vista da riconoscere e dalla quale difendersi.

La recente legge approvata negli Stati Uniti d'America riconosce e delinea il *caller* ID *spoofing* e predispone delle pene di tipo pecuniario e afflittivo di una certa consistenza che sottolineano la pericolosità del fenomeno in questione.

In Italia i principi cardine ai quali si dovrebbe far riferimento per regolare la fattispecie dovrebbero *prima facie* trovare appiglio nel disposto dell'articolo 15 del Codice sul trattamento dei dati personali che in tema di risarcimento dei danni per illecito trattamento dei dati prevede che "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento dei danni ai sensi dell'art.2050 del codice civile"[70] e ancora, al secondo comma specifica che il danno patrimoniale sarebbe risarcibile anche nei casi di trattamento attuato in dispregio delle regole sulle modalità del trattamento e sui requisiti dei dati.

Inoltre sempre all'interno del Codice si troverebbe un riscontro implicito della fattispecie all'art.130, nel quale il legislatore, in tema di vendita diretta stabilisce che è fatto divieto di utilizzare sistemi informatici che celino l'identità del mittente o camuffino la

---

[67] Così l'enciclopedia *on-line* Wikipedia definisce la figura in oggetto.

[68] Così G. RESTA, *Identità personale e Identità digitale*, in *Dir. inf.*, 3, 2007, p. 515.

[69] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, cit., p.141.

[70] La scelta del legislatore di far rientrare la disciplina del risarcimento da illecito trattamento di dati personali all'interno della previsione normativa della c.d. responsabilità da attività pericolose ex art.2050 c.c. ha l'importante valenza di prevedere un più stringente onere probatorio nei confronti del convenuto (c.d. prova liberatoria), oltre che a contemplare espressamente la risarcibilità del c.d. danno non patrimoniale, di cui parleremo brevemente *infra*.

stessa (art.130, comma 5) prevedendo altresì che il Garante, qualora tale divieto non venisse rispettato, possa disporre nei confronti dei fornitori dei servizi di comunicazione elettronica l'adozione "di procedure di filtraggio relativamente alle coordinate di posta elettronica da cui sono state inviate le comunicazioni"[71].

Altro principio affermato dal Garante, anche se in tema di *spamming* sarebbe la rilevanza che assumerebbe, per la libera costruzione della propria sfera privata, il tema del controllo sui dati in entrata.

Un'ulteriore accenno al problema della manipolazione dei dati personali si rintraccia in una delibera del 2006, riguardante il tema delle comunicazioni VoIP:

> "26. A livello generale gli operatori evidenziano l'importanza per le reti e i servizi "IP-based" di rispettare opportuni livelli di sicurezza, disponibilità ed integrità delle piattaforme di rete e di servizio. Per quanto riguarda i servizi che dovrebbero confluire nella categoria individuata dalla decade 5 alcuni di essi ritengono necessario avviare, nelle opportune sedi istituzionali, opportuni approfondimenti per individuare i requisiti di qualità che l'Autorità intende richiedere, in modo da valutarne congiuntamente la fattibilità e sostenibilità economica.
>
> 27. Inoltre uno dei rispondenti evidenzia che, considerato che il concetto di servizio nomadico fa perdere l'associazione rigida tra il punto di accesso alla rete e il cliente che utilizza il servizio di comunicazione elettronica, tali servizi sono maggiormente esposti a possibili utilizzi ingannevoli in cui un utente può presentarsi alla rete con una diversa identità (spoofing). Ne segue la necessità di adottare norme che consentano in ogni caso la identificazione dei clienti utilizzatori dei servizi VoIP"[72].

Al punto 27 viene dunque fatto un accenno allo "*spoofing*", con evidente riferimento alla palese difficoltà di controllare e identificare in maniera chiara i reali dati e le reali identità delle comunicazioni in entrata e in uscita che avvengono attraverso questo diffusissimo, economico ed elastico sistema di comunicazioni e alla conseguente necessità di veder controllato in maniera più chiara e severa il traffico che corre su questo *network*.

Gli strumenti di tutela dell'identità personale e più in generale dei diritti della personalità che si delineano nell'ordinamento italiano comprendono essenzialmente i tradizionale rimedi dell'azione inibitoria (di tipo preventivo) e del risarcimento del danno (di carattere successivo).

---

[71] Vedi S. SICA, in *Manuale di diritto dell'informatica,* cit., p.111.

[72] Delibera n.11/06/CIR, Allegato B (Disposizioni regolamentari per la fornitura di servizi VoIP e integrazione del piano nazionale di numerazione), 2.12 (Sicurezza,disponibilità ed integrità di reti/servizi).

Si sono riscontrati altresì dei limiti in seno all'applicazione dei seguenti rimedi alla fattispecie dei diritti della personalità che diminuirebbero sensibilmente la portata e l'effettività della tutela stessa.

Nel caso dell'azione inibitoria infatti l'applicabilità sarebbe da riferire esclusivamente in relazione alla violazione di singoli attributi della personalità: il seguente problema è stato ovviato in giurisprudenza dall'applicazione dei provvedimenti d'urgenza ex art.700 c.p.c. con la conseguente estensione del rimedio cautelare e dei conseguenti obblighi di *facere* o *non facere* al fine di porre un freno seppur provvisorio alla violazione degli interessi della persona.

Problema più rilevante si considera invece in tema di risarcimento del danno e in particolare riferito al vuoto normativo concernente i c.d. danni non patrimoniali nelle ipotesi di risarcibilità ex art. 2059 c.c..

In dottrina si era delineata una linea di pensiero, confortata anche da recenti pronunce giurisprudenziali[73], che sostiene l'ipotesi di risarcibilità dei cosiddetti "danni esistenziali"[74], (anch'essi poco considerati rispetto agli ordinamenti anglosassoni[75]) includendo cosi la sfera dei danni non patrimoniali da lesione di un diritto della personalità tra quelle ipotesi che si collocherebbero "fuori dalle strettoie poste dall'art.2059, al pari del danno biologico"[76].

Essi riguarderebbero danni di natura morale quali dolore, fastidio, imbarazzo, irritazione, ira e offesa seguenti alla lesione di diritti assoluti e indisponibili della persona e non sarebbero legati quindi alla sussistenza e all'inquadramento all'interno delle c.d.

---

[73] Cass. 31.05.2003, n.8827 in Foro it., 2003, I, 2273, con nota di E. NAVARRETTA,; Cass., 31.05.2003, n.8828; Cass. 12.05.2003, n. 7281; Cass. 12.05.2003, n.7283; Corte Cost., sent. 11.07.2003, n.233.

[74] Vedi sul tema A. JANNARELLI, *La responsabilità civile, in Istituzioni di Diritto Privato*, a cura di M. BESSONE, Torino, 2010 e in particolare sul danno esistenziale P. CENDON, *Essere o non esistere, in Trattato breve dei nuovi danni,* a cura di P. CENDON, *Padova, 2001;* ID., *Il risarcimento del danno esistenziale nel sistema di tutela della persona,* in *Studi in onore di Schlesinger, III, Milano, 2004;* ID., *L'itinerario del danno esistenziale,* in *Giur.It., 2009, pp.1047 ss.,* ID., *L'araba fenice. Più vivo che mai il danno esistenziale presso i giudici italiani,* in *Nuova giur.civ. comm.,* 2010.

[75] Così sinteticamente G. COMANDÈ in *La nuova Categoria del danno patrimoniale*, relazione dell'incontro tenutosi sul tema presso il Consiglio superiore della magistratura, Roma, 17-19 Giugno 2009: "É estremamente complesso ricostruire in termini generali la posizione dell'intera famiglia di *common law* rispetto alle perdite non pecuniarie, in quanto le soluzioni offerte variano spesso da paese a paese e nel tempo all'interno del medesimo. Ciò nonostante le voci base di danno comprese nelle *non pecuniary losses* sono comuni a tutti i paesi di *common law - pain and suffering, loss of amenity of life / loss of enjoyment of life, loss of expectation of life* - e per esse si registrano tendenze evolutive omologhe.
All'interno di quest'ampia categoria sono considerati tutti i danni che possono interessare la persona umana, prescindendo, però, dalla perdita di guadagno che la condotta illecita può avere provocato o dal danno emergente come le spese mediche".

[76] *Così* A. FUSARO, *La responsabilità: ipotesi e limiti,* in *Informazioni e conomiche e "reputazione d'impresa",* Torino, 2010, p. 259.

responsabilità da fatto che costituisce reato ex art. 185 c.p., il quale è condizione imprescindibile per l'ottenimento della risarcibilità del danno patrimoniale.

La sentenza delle Sezioni Unite della Cassazione n.26972 del 2008 ha però posto chiarezza sul tema, indicando che "il danno non patrimoniale (e il suo risarcimento) è categoria generale non suscettiva di suddivisione in sottocategorie variamente etichettate" e dunque non potrebbe "farsi riferimento ad una generica sottocategoria denominata "danno esistenziale", perché attraverso questa si finisce per portare anche il danno non patrimoniale nell'atipicità"[77].

Le Sezioni Unite hanno altresì puntualizzato che "il risarcimento del danno alla persona deve essere integrale, nel senso che deve ristorare interamente il pregiudizio, ma non oltre..." e che il giudice, nel considerare "gli aspetti relazionali" della persona dovrà tener fermo il concetto che "la risarcibilità del danno non patrimoniale postula, sul piano dell'ingiustizia del danno, la selezione degli interessi dalla cui lesione consegue il danno", la quale avverrà " a livello normativo, negli specifici casi determinati dalla legge, o in via di interpretazione da parte del giudice, chiamato ad individuare la sussistenza, alla stregua della Costituzione, di uno specifico diritto inviolabile della persona necessariamente presidiato dalla minima tutela risarcitoria".

Ad esempio, la fattispecie dell' illecito trattamento dei dati personali rientrerebbe tra le ipotesi nelle quali "la legge espressamente consente il ristoro del danno non patrimoniale anche al di fuori di una ipotesi di reato" e ancora che "in tal caso la vittima avrà diritto al risarcimento del danno non patrimoniale scaturente dalla lesione dei soli interessi della persona che il legislatore ha inteso tutelare attraverso la norma attributiva del diritto al risarcimento".

In questo modo la Cassazione non ha, come parrebbe da una prima lettura, "cancellato" l'esistenza delle fattispecie di danno biologico, morale ed esistenziale e le rispettive caratteristiche connotanti, ma ha invero specificato che il risarcimento del danno non patrimoniale sarebbe ammissibile soltanto qualora riconducibile a dei casi previsti dalla legge, operando in un ottica di interpretazione costituzionalmente orientata dell'art.2059 c.c..

Successivamente alla sopracitata sentenza, altre pronunce della Corte hanno ulteriormente analizzato i termini della questione, affermando che il danno non patrimoniale dovrà essere "liquidato in unica somma"[78], senza duplicazioni e facendo riferimento ove possibile, ai fini della valutazione equitativa ex art. 1226 c.c, alle "Tabelle per la liquidazione del danno non patrimoniale derivante da lesione all'integrità psicofisica del Tribunale di Milano" (c.d. tabelle di Milano)[79].

---

[77] Cass. Sez.un., 11.11.2008, n.26972, in *Rep. Foro It.*, 2008, Danni Civili, n.189.

[78] Così Cass., 17.09.2010, n.19816, in *Rep. Foro It.*, 2010, Danni Civili, n.318.

[79] Vedi Cass., 30.06.2011, n.14402, in *Rep. Foro it.*, 2011, Danni Civili, n.176: "Ai fini della liquidazione del danno non patrimoniale derivante da lesione dell'integrità psico-fisica, le tabelle all'uopo elaborate dal tribunale di Milano costituiscono necessario criterio di riferimento, laddove la fattispecie concreta non presenti

Dovranno altresì essere tenute in considerazione dal giudice tutte quelle sfaccettature e quegli aspetti che abbiano concorso a dare delle caratteristiche peculiari alla fattispecie nel caso concreto, condensando dunque la figura del danno non patrimoniale all'interno di un rapporto interconnesso tra unicità della forma e molteplicità dei contenuti[80].

Nel novero dei nuovi strumenti di tutela configuratisi negli altri ordinamenti comunitari sembra utile evidenziare come nella giurisprudenza tedesca, sulla falsariga dell'esperienza nordamericana dei *punitive damages*, si sia fatto avanti l'uso "di rimedi risarcitori o restitutori in funzione dissuasiva e sanzionatoria rispetto ad illeciti particolarmente gravi e lesivi dell'altrui sfera personale" e come dall'altra parte in Francia si applichino invece le c.d. *astreintes*, consistenti in una pena pecuniaria comminata dal giudice e rapportata progressivamente al protrarsi giornaliero dell'illecito giudizialmente accertato[81].

E' altresì necessario sottolineare come la nascita dell' Autorità Garante per le Comunicazioni (AGCOM)[82] e dell' Autorità Garante per la protezione dei dati personali è da ritenersi un'essenziale conquista, strumentale a garantire un intervento più strutturato e capillare nella regolamentazione e nella vigilanza della società delle *Information and Communication Technologies* oltre che atta a ricoprire un ruolo preminente nell'assistenza e lo sviluppo di una consapevole "etica della responsabilità", attraverso, ad esempio, interventi che, nel delineare altre fattispecie globali di illecito informatico quali l'*hacking*, lo *spamming*[83] o il *phishing*[84], rafforzino e amplino al contempo l'ambito preventivo della tutela da predisporre.

---

circostanze che richiedano una variazione, in aumento o in diminuzione, occorrendo in tal caso che la motivazione dia conto delle ragioni della preferenza assegnata ad una liquidazione che risulti sproporzionata rispetto a quella cui si perverrebbe mediante l'adozione dei parametri contenuti nelle predette tabelle".

[80] Vedi Cass., 26.05.2011, n.11069: "le distinzioni elaborate dalla dottrina e dalla prassi fra danno biologico, danno per morte, danno esistenziale, ecc, hanno funzione meramente descrittiva; dall'altro lato, ha precisato che, nel procedere alla quantificazione ed alla liquidazione dell'unica categoria "danno non patrimoniale", il giudice deve tenere conto di tutti gli aspetti di cui sopra; se, pertanto, debbono essere evitate duplicazioni risarcitorie, mediante l'attribuzione di somme separate e diverse in relazione alle diverse voci (sofferenza morale, danno alla salute, danno estetico, ecc), i danni non patrimoniali debbono comunque essere integralmente risarciti, nei casi in cui la legge ne ammette la riparazione: nel senso che il giudice, nel liquidare quanto spetta al danneggiato, deve tenere conto dei diversi aspetti in cui il danno si atteggia nel caso concreto".

[81] Vedi G. RESTA, *Diritti della personalità, problemi e prospettive*, in *Dir. inf.*, 6, 2007, p. 1068.

[82] Autorità amministrativa indipendente, istituita in Italia con la legge 31 Luglio 1997 n.249 (c.d. Legge Maccanico).

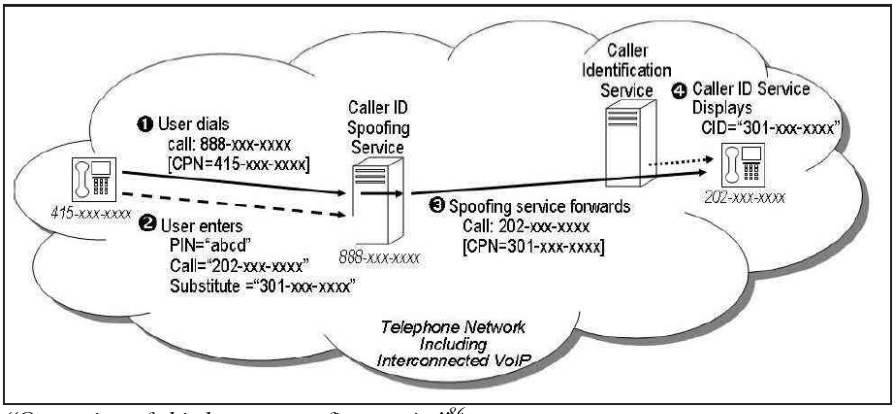
[83] Invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

[84] Spillaggio (di dati sensibili)", attività illegale che sfrutta una tecnica di ingegneria sociale, utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto d'identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

L'azione combinata tra rimedi tradizionali, possibili nuovi meccanismi di tutela da testare ed introdurre, strumenti di *soft law*, azioni ad iniziativa collettiva, unitamente alla funzione preminente del garante nell'esercizio dei suoi poteri di stampo privatistico e pubblicistico, potrebbe dunque dare vita ad un funzionale sistema di monitoraggio, controllo e intervento nei confronti di "vecchi" e "nuovi" fenomeni di illecito informatico.

Nel caso di specie essi concorrerebbero a limitare e combattere lo *spoofing* fraudolento posto in essere con lo scopo di minare il diritto alla protezione dei dati personali e la figura dell'identità in tutte le sue sfaccettature, nell'ottica di un rafforzamento imprescindibile della tutela di tipo general-preventivo in luogo di quella tipo risarcitorio e successivo, strumentale ad offrire ai soggetti la possibilità di costruire e definire liberamente la propria sfera privata e altresì a implementare gli effetti benefici anche sul piano collaborativo e della trasparenza alla quale sarebbe tenuta ad adeguarsi l'altra parte in causa, ovvero i *providers* che erogano tali servizi[85].

Appendice



"Operation of third party spoofing service"[86]

[85] Vedi inoltre sul tema la scelta di una figura di responsabilità "elastica", che valuta la condotta caso per caso, per gli Internet *providers*: Artt. 12 e 14 Dir. 2000/31/CE e artt. 14 e 16 del d.lgs n.70/03.

[86] Schema ricostruttivo del *caller ID spoofing* riportato sul "*Report and Order*" della *Federal Communications Commission*.