Prima relazione annuale in tema di Internet tra libertà e diritti: privacy, diffamazione online e cybercrime in particolare.

di avv. Giuseppe Siniscalchi*

L'utilizzo di Internet è oggi sempre più frequente, per molti necessario, sia per lavoro sia per svago ecc. poiché la rete offre la possibilità di operare nei modi più svariati.

Conseguentemente vi è un crescente numero di illeciti e reati commessi attraverso la rete.

Il secondo rapporto della Symantec, pubblicato nel maggio 2012 e relativo all'anno 2011, descrive un quadro allarmante di oltre 5,5 miliardi di attacchi a siti nel 2011, con una crescita dell'81%, con un tasso giornaliero cresciuto del 36% e un numero di varianti uniche di malware di 403 milioni (contro i 286 milioni del 2010).

Gli episodi di hacking, spesso attraverso l'utilizzo di social network, costituiscono grave minaccia, avendo esposto nel 2011 ben 187 milioni d'identità.

Come si legge nel recente comunicato della Commissione Europea con riferimento all'operatività, a partire dall'11 gennaio 2013, del nuovo Centro Europeo per la lotta alla criminalità informatica (EC3) "*secondo un recente sondaggio dell'Eurobarometro la sicurezza informatica desta ancora molta preoccupazione tra i cittadini europei. L'89% degli utenti di Internet non rivela informazioni personali online e il 12% è stato vittima di frode online.*

Circa un milione di persone nel mondo è vittima ogni giorno di varie forme di criminalità informatica. Secondo le stime le vittime perdono circa 290 miliardi di Eur ogni anno nel mondo a causa di attività criminali informatiche (Norton, 2011)"[1].

---

* Membro del Comitato Tecnico-Giuridico dell'Osservatorio sulla legalità e sui diritti Onlus, Coordinatore della Commissione cybercrime dell'Osservatorio stesso.

1 Cfr. comunicato della Commissione Europea, in *http://ec.europa.eu/cgi-bin/etal.pl*.

Sempre secondo il predetto rapporto Symantec Roma sarebbe la seconda città al mondo con il maggior numero di "bot" cioè di computer controllati da remoto da criminali informatici all'insaputa dei loro utilizzatori per lanciare attacchi informatici[2].

Come si legge in tale rapporto "*nel trattato del Consiglio d'Europa sulla criminalità informatica viene utilizzato il termine 'cybercrime' per definire reati che vanno dai crimini contro i dati riservati, alla violazione di contenuti e del diritto d'autore [Krone, 2005]. Tuttavia, altri [Zeviar-Geese, 1997-98] suggeriscono una definizione più ampia che comprende attività criminose come la frode, l'accesso non autorizzato, la pedopornografia e il 'cyberstalking' o pedinamento informatico. Il manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (The United Nations Manual on the Prevention and Control of Computer Related Crime) nella definizione di crimine informatico include frode, contraffazione e accesso non autorizzato [Nazioni Unite, 1995]*"[3].

2 F. Boneschi, *Symantec: spam in calo ma mobile Android e furto identità nel mirino*, in www.hwfiles.it del 5.5.2012; F. Tarissi, *Roma capitale dei virus informatici e i siti religiosi sono tra i più colpiti*, in www.larepubblica.it del 2.5.2012; v. l'articolo *Più infettati da virus siti religiosi che porno*, in www.ansa.it del 2.5.2012; G. Rusconi, *Symantec: i siti religiosi sono più pericolosi di quelli porno. Roma al top per computer infetti*, in www.ilsole24ore.com del 2.5.2012.

3 Norton by Symantec, *Che cosa è il crimine informatico?*, in *it.norton.com/cybercrime-definition/promo*.
Il prof. Ben Hayes (Statewatch-Monitoring the State and Civil Liberties in Europe, London, UK) - nel corso della Conferenza Internazionale "Cybercrime: globalità del fenomeno e sfide" promossa dal 2 al 4 dicembre 2011 in Courmayeur dall'ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme) nonché dal CNPDS (Centro Nazionale di Prevenzione e Difesa Sociale) in cooperazione con l'United Nations Office on Drugs and Crime-UNODC, Vienna e Korean Institute of Criminology-KIC, Seul - ha richiamato l'attenzione sull'ampiezza della definizione di cybercrime che coinvolge qualunque atto criminale commesso attraverso la rete, con fenomeni talvolta nuovi che mettono in difficoltà i legislatori di molti Paesi.
In sintesi il prof. Hayes ha rilevato che occorre la ricerca di soluzioni che superino i criteri e sistemi tradizionali puntando, il più possibile, sulla prevenzione ed armonizzazione.
Ciò al fine di rispettare diritti fondamentali che richiedono maggiori tutele, pur mantenendo l'idea di libertà come base importante di Internet, ma sempre nel rispetto dei diritti inviolabili dell'individuo e della collettività.

L'interesse per tali materie è crescente. Basti considerare, a titolo esemplificativo: i numeri di aumento esponenziale dei c.d. "internauti" (e cioè di soggetti, sparsi in tutto il mondo, che utilizzano internet); l'aumento significativo nell'invio e ricezione di email nonché nell'uso di social network[4].

Così come aumentano le possibilità di contatti esterni attraverso la rete aumentano altresì significativamente gli illeciti e reati commessi attraverso la rete stessa: diventa infatti sempre più diffusa la possibilità per i criminali informatici di entrare in possesso dei nostri dati personali, password e codici segreti attraverso i crimeware, i bot, i trojan horse, gli spyware, il phishing ed il pharming[5].

La violazione dei predetti dati dipenderebbe, nella maggior parte dei casi, dal furto o dallo smarrimento dei computer, degli smartphone e chiavette Usb.

Oggetto di attenzione da parte degli hacker non sarebbero solo le grandi aziende, ma anche organizzazioni con meno di 2.500 dipendenti e circa il 17% delle imprese con meno di 250 dipendenti[6].

Una notizia che interessa da vicino anche l'Italia è quella secondo cui i siti web religiosi e ideologici superano quelli pornografici per numero di minacce medie presenti per sito infetto[7].

---

4 Cfr. i dati riportati alla nota n. 8 di cui *infra*.

5 Come affermato da Viviane Reding, Commissaria Ue per la giustizia, "*I cyber attack sono uno strumento nelle mani della criminalità organizzata, ma anche una minaccia per la democrazia e l'economia*", in www.sysadmin.it del 29.4.2009; rinvio per ulteriori riferimenti ai miei scritti, *Le sfide della rete e la necessità di una normativa globale in materia (relazione alla conferenza internazionale "Internet fra libertà e diritti"*, in www.aaalegalitadiritti.it e *Cybercrime: globalità del fenomeno e sfide*, in www.osservatoriosullalegalita.org/11/acom/12dic1/0505giusinternet.htm; cfr. altresì R. Guma, *Internet: quale limite alla tutela delle libertà? (relazione alla conferenza internazionale "Internet fra libertà e diritti"*, in *www.aaalegalitadiritti.it*.)

6 V. il rapporto Symantec cit. alla nota n. 2.

7 G. Rusconi, *Symantec: i siti religiosi sono più pericolosi di quelli porno. Roma al top per computer infetti*, in www.ilsole24ore.com del 2.5.2012, cit.

Secondo gli analisti di Pingdom – esperti di siti web – gli internauti di tutto il mondo sarebbero nel complesso 2,4 miliardi con la possibilità di navigare in 634 milioni di pagine web di cui 50 milioni messe online solo nel 2012; in quest'ultimo anno sarebbero state inviate 144 miliardi di email e sarebbero state effettuate attraverso Google 1,2 trilioni di ricerche[8].

Riporto qui di seguito, in breve, alcune significative notizie, senza alcuna presunzione di completezza in considerazione della vastità e continua evoluzione delle fonti al fine di dare un quadro sintetico di informative e spunti a conferma del profondo e rapido cambiamento dei tempi e delle relative problematiche che la rete pone quotidianamente[9].

Google maps su iPhone e dati personali.

Un'associazione tedesca per la difesa della privacy ha posto il problema dell'asserito mancato rispetto, da parte del noto motore di ricerca, delle regole europee sui dati personali.

"*Quando gli utenti installano Google maps sul proprio iPhone, infatti, la possibilità di condividere dati di posizione con Google sarebbe attivata come impostazione predefinita.*

E proprio questo dettaglio renderebbe l'app incompatibile con le regole del vecchio continente"[10].

8 v. l'articolo *I numeri di Internet nel 2012*, in www.mrwebmaster.it del 18.1.2013.

9 Per un quadro relativo alle diverse fattispecie di danni alla persona e d'ipotesi risarcitorie connesse all'uso della rete v., per qualche esempio, D. Bianchi, *Internet e il danno alla persona*, TO, 2012, Collana diretta da P. Cendon.

10 C. Leonardi, *Google maps parte forte su iPhone: rischio inciampo nella privacy*, in *www.lastampa.it* del 17.12.2012 ove viene ripreso anche il pensiero di Marit Hansen, vice Commissario privacy e informazioni presso il Centro Indipendente per la Tutela della Privacy di Schleswing-Holstein in Germania; v. l'articolo *Google maps torna su iOS ma è polemica sulla privacy*, in *www.datamanager.it*;

Garante privacy e cookie.

Con provvedimento pubblicato sulla Gazzetta Ufficiale n. 295 del 19.12.2012 l'Autorità Garante per la Protezione dei Dati Personali ha avviato "*una consultazione pubblica ai sensi dell'art. 122 volta ad individuare le modalità semplificate per l'informativa di cui all'art. 13, comma 3, del codice in materia di protezione dei dati personali*".

La stessa Autorità ha altresì pubblicato in data 18.12.12 sul proprio sito un documento contenente chiarimenti su alcune questioni in materia di cookie (FAQ).

In tale documento si legge che "*I cookie sono piccoli file di testo che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente. Nel corso della navigazione su un sito, l'utente può ricevere sul suo terminale anche cookie di siti o di web server diversi (c.d. cookie di 'terze parti'); ciò accade perché sul sito web visitato possono essere presenti elementi come, ad esempio, immagini, mappe, suoni, specifici link a pagine web di altri domini che risiedono su server diversi da quello sul quale si trova la pagina richiesta. In altre parole, sono quei cookie che vengono impostati da un sito web diverso da quello che si sta attualmente visitando.*

I cookie sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni specifiche riguardanti gli utenti che accedono al server e di norma sono presenti nel browser di ciascun utente in numero molto elevato.

Alcune operazioni non potrebbero essere compiute senza l'uso dei cookie, che in alcuni casi sono quindi tecnicamente necessari: a titolo esemplificativo, l'accesso all'home banking e le attività che possono essere svolte sul proprio conto corrente online (visualizzazione dell'estratto conto, bonifici, pagamento di bollette, ecc.) sarebbero molto più complesse da svolgere e meno sicure senza la presenza di cookie che consentono di identificare l'utente e mantenerne l'identificazione

nell'ambito della sessione.

I cookie possono rimanere nel sistema anche per lunghi periodi e possono contenere anche un codice identificativo unico. Ciò consente ai siti che li utilizzano di tenere traccia della navigazione dell'utente all'interno del sito stesso, per finalità statistiche o pubblicitarie, per creare cioè un profilo personalizzato dell'utente a partire dalle pagine che lo stesso ha visitato e mostrargli quindi pubblicità mirate (c.d. Behavioural Advertising)"[11].

Internet e privacy negli USA.

Con riferimento alle ispezioni di contenuti di email o di dispositivi informatici, si sta tentando, negli Stati Uniti, di rafforzare la tutela della privacy.

A fine novembre 2012 "*la competente Commissione del Senato ha approvato … un provvedimento che impone alle forze dell'ordine di ottenere un mandato di perquisizione da parte di un magistrato prima di ispezionare qualsiasi contenuto email o altro dispositivo informatico*"[12].

Il tema di un corretto bilanciamento tra privacy e security è molto problematico e ben lungi da una soluzione univoca.

Il dibattito è tuttora acceso ed "*oggetto di polemiche crescenti in un momento in cui grandi quantità di email private sono regolarmente consegnate agli investigatori.*

Il problema è stato evidenziato dal caso dell'ex direttore della CIA David H. Petraeus, che si è visto costretto a rassegnare le dimissioni dopo che gli investigatori erano incappati in email inerenti ad una sua relazione extraconiugale"[13].

Facebook e privacy.

---

11 Cfr. anche l'articolo *Garante privacy: presto più trasparenza sui cookies*, in *Banca dati IPSOA* del 18.12.2012.
12 M. Pisano, *Internet: Stati Uniti verso il rafforzamento della privacy*, in *http://www.osservatoriosullalegalita.org/12/acom/12dic1/0101mipinternet.htm*.
13 M. Pisano, op. cit.

Facebook ha chiesto agli utenti di esprimere un voto, con termine fino al 10 dicembre 2012, "*sulle modifiche annunciate alle policy in materia di dati personali oltre che allo Statement of Rights and Responsibilities (SRR) dello stesso sito in blu*"[14].

La circostanza ha suscitato perplessità, polemiche e proteste come, ad esempio, quelle di cui al sito "Europe versus Facebook" per l'asserito "*scarso rispetto del social network verso le leggi sulla riservatezza irlandesi (Paese da cui Facebook controlla le operazioni europee)*".[15]

Google e privacy: recente pronunzia della Corte d'Appello Penale di Milano.

La Corte d'Appello Penale di Milano, con dispositivo del 21.12.2012, ha assolto i dirigenti Google nell'ambito del caso Vividown "perché il fatto non sussiste"[16].

A differenza di quanto affermato dal Giudice di primo grado la predetta Corte non ha evidentemente ritenuto sussistenti i presupposti di responsabilità penale e di violazione della normativa privacy nel noto caso di cronaca.

Le motivazioni della sentenza non risultano allo stato pubblicate.

Google e privacy in Svizzera.

La Corte Suprema con sede a Losanna ha in parte riformato la sentenza impugnata che avrebbe obbligato Google a garantire l'anonimato completo alle persone che appaiono nel servizio street view pur ribadendo l'ordine a Google di interrompere la pubblicazione di foto di giardini privati scattate con macchine fotografiche posizionate ad altezza superiore a quella delle persone[17].

14 M. Vecchio, *Facebook, l'ultimo voto?*, in *punto-informatico.it*.

15 M. Munafò, *Facebook, l'ultimo voto degli utenti. Il social network cambia le regole*, 5.12.2012, in www.repubblica.it; per news su iniziative contro Facebook in Germania v. l'articolo *Privacy. Facebook contro Germania 0-1* in *www.leggioggi.it* del 18.9.2011.

16 La notizia è riportata in più fonti: cfr. ad esempio *Caso Google-Vividown, imputati tutti assolti in secondo grado* di D. Lepido in *danielelepido.blog.ilsole24ore.com*.

17 v. l'articolo *Privacy, la vittoria di Google in Svizzera capovolta sentenza*, in www.repubblica.it del 8.6.2012.

LinkedIn e password degli utenti.

Il social network ha dato notizia che su un forum russo erano stati pubblicati gli hash delle password di circa 6 milioni di utenti di LinkedIn con conseguente compromissione degli stessi account. Gli hash sono una versione crittografata delle password da cui è possibile risalire a queste ultime. LinkedIn ha, per queste ragioni, comunicato che gli utenti degli account compromessi sarebbero stai contattati per le istruzioni ed informazioni del caso[18].

Giudice australiano condanna Google per diffamazione.

Con sentenza del 12.11.2012 la Corte Suprema di Vittoria, in Australia, ha condannato direttamente per diffamazione Google al pagamento di 200.000 dollari a titolo di risarcimento del danno in favore di un promoter musicale poiché - tra i primi dieci risultati riportati dopo aver effettuato una ricerca digitando il suo nome - comparivano immagini che accostavano il predetto promoter alla criminalità[19].

Si tratta, per quanto mi consta, della prima pronunzia al mondo che ha affermato il principio di una diretta responsabilità di Google per diffamazione[20].

Il tema è di grande interesse ed attualità[21].

---

18 G. Garro, *LinkedIn: compromesse le password di oltre 6 milioni di utenti*, in www.pctuner.net del 7.6.2012.

19 G. M. Marq, *Internet: giudice australiano condanna Google per diffamazione*, in *http://www.osservatoriosullalegalita.org/12/acom/11nov2/2900gabgoogle.htm*.

20 I Giudici australiani hanno respinto le tesi, prospettate da Google, nel senso di asserita insussistenza di responsabilità per caratteristiche del motore di ricerca quale, in sintesi, mero canale in cui confluirebbero moltissimi dati e che offrirebbe la possibilità del reperimento di miliardi di fonti, senza possibilità di controllo. Cfr. in senso contrario alla pronunzia dei Giudici australiani la pronunzia dell'*High Court of Justice, Queen's Bench, [2012] EWHC 449 (QB), Tamiz v. Google, 2.3.12* menzionata nel sito http://elenafalletti.wordpress.com/2012/06/ secondo la quale secondo i principi del Common Law, Google non può essere considerato un editore.

21 Con riferimento, in generale, alla responsabilità dell' "hoster attivo" definito quale "motore della net economy, il territorio in cui libertà d'impresa, esigenze di mercato e diritti della persona si incontrano e si scontrano" v. A. Fiorenzi in *Internet e il danno alla persona*, cit., pag. 367 ed ivi a pag. 368 ove si legge che "*i prestatori di servizi non sono più sparute imprese che si lanciano nel mondo dell'economia digitale fidando unicamente sulla forza di un'idea.*
I prestatori di servizi sono oggi colossi spesso non stabiliti nell'area UE che contrappongono le loro policy al mondo intero incuranti dei diritti professati nei vari Paesi. Si tratta di imprenditori che hanno fatto i soldi e che

C.d. diritto all'oblìo.

La Corte di Cassazione, con la sentenza del 5.4.2012, n. 5525 ha affermato il principio dell'obbligo, per gli editori, di aggiornare gli archivi storici delle notizie online[22].

Si tratta di pronunzia importante nell'ottica del dibattito tuttora acceso e su tema di grande attualità anche in considerazione delle iniziative dell'UE per l'affermazione del c.d. "diritto all'oblìo"[23].

La Suprema Corte ha affermato che "*anche in caso di memorizzazione in Internet, deve riconoscersi, al soggetto cui pertengono i dati personali oggetto di trattamento, il diritto all'oblio come controllo a tutela della propria immagine sociale, idoneo a tradursi nella pretesa alla contestualizzazione e aggiornamento dei medesimi e, se del caso (avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende), alla relativa cancellazione*"[24].

Centro europeo per la lotta alla criminalità informatica.

Come si legge nel sito http://ec.europa.eu/cgi-bin/etal.pl a partire dall'11 gennaio 2013 "*è pienamente operativo*" il nuovo Centro europeo per la lotta alla criminalità informatica (EC3).

---

spesso si trovano in stato di quasi monopolio o di oligopolio. Corrispondentemente certa parte della dottrina (Rossello, 2010, Zeno Zencovich, 2010) ritiene che i tempi siano maturi per avviare una nuova era della responsabilità dell'hoster declinata sulla relativa potenzialità di manipolare il materiale elettronico.
L'hoster passivo rimarrà sottoposto al regime di deresponsabilizzazione previsto dalla direttiva 2000/31/CE.
L'hoster attivo invece dovrebbe inquadrarsi in schemi di responsabilità adeguati all'evoluzione tecnologica ed economica.
Autorevoli voci indicano quale modello-guida lo schema della responsabilità per rischio d'impresa fondata sulla presunzione di colpa".

22 G. Negri, *Diritto di oblìo anche sul web*, in *Il Sole 24 Ore-Norme e tributi* del 6.4.2012, 25.

23 Cfr. R. Mastrolonardo, *Diritto all'oblio e multe, la UE ridisegna la privacy online*, in http://tg24sky.it del 25.1.2012; D. D'Elia, *Riforma UE della privacy: 1 milione di multa agli scocciatori*, in www.tomshw.it del 25.1.2012.

24 Cass. civ. 5.4.2012, n. 5525, in *Danno e Resp.*, 2012, 7, 747.

La Commissaria UE per gli affari interni, Cecilia Malmström, ha dichiarato che "*il Centro per la lotta alla criminalità informatica darà un forte impulso alla capacità dell'UE di combattere la criminalità informatica e proteggere una rete internet libera, aperta e sicura. I criminali informatici sono intelligenti e veloci nell'utilizzare le nuove tecnologie per scopi criminali; il Centro EC3 ci aiuterà a diventare ancora più intelligenti e veloci al fine di contribuire a prevenire e combattere i reati informatici*".

Come affermato da Troels Oerting, Capo del predetto Centro, "*nella lotta alla criminalità informatica, priva di confini per natura e caratterizzata da una grande abilità dei criminali a nascondersi, è necessaria una risposta flessibile e adeguata. Il Centro europeo per la lotta alla criminalità informatica è stato istituito per fornire queste competenze in qualità di Centro di fusione e di centro di sostegno operativo, investigativo e forense, ma anche grazie alla propria capacità di mobilitare tutte le risorse degli Stati membri dell'UE necessarie a mitigare e ridurre le minacce provenienti dai criminali informatici, ovunque essi operino*"[25].

Il cybercrime in Italia.

Secondo una ricerca condotta da Kaspersky l'Italia sarebbe il Paese più colpito dal crimine informatico; i dati più diffusi, oggetto di attacchi informatici, sul 44% dei computer italiani, sarebbero le credenziali d'accesso all'home banking e i numeri di carta di credito. Sempre secondo tale ricerca, in futuro, l'obiettivo dei criminali informatici potrebbe essere il mobile banking[26].

25 Cfr. comunicato della Commissione Europea, in http://ec.europa.eu/cgi-bin/etal.pl, cit.
26 v. l'articolo *L'Italia è il paese più colpito dal cyber crimine*, in www.mrwebmaster.it del 15.9.2012.

Facebook e lotta alla criminalità.

Le chat attive sarebbero monitorate al fine di scovare indizi su eventuali cyber criminali. All'uopo sarebbe preposto un apposito algoritmo anche per rilevare pericoli per la pubblica sicurezza e per i minori[27].

Email ed sms: differenze rilevanti per la configurabilità o meno di reati.

La Corte di Cassazione, sezione feriale penale, con la recente sentenza n. 44855 del 2012 depositata il 16 novembre 2012 ha affermato che l'invio ripetuto di email non configura il reato di molestie[28].

Facebook e cyberstalking.

Con sentenza del 12 aprile 2012, n. 13878 la Corte di Cassazione ha respinto il ricorso di un uomo condannato dalla sentenza impugnata per il reato di stalking in considerazione di atti persecutori posti in essere anche attraverso messaggi offensivi su Facebook nei confronti delle vittime[29].

27 v. l'articolo *Sei in chat? Facebook ti spia (per combattere il crimine)*, in www.mrwebmaster.it del 17.7.2012.

28 Per qualche considerazione su tale pronunzia ed in tema di email richiamo il mio articolo *Email ed sms : quali differenze per la configurabilita' dei reati ?*, in *http://www.osservatoriosullalegalita.org/12/acom/12dic2/2200gsmolestiemail.htm.*

29 Cass. pen. 12.4.2012, n. 13878, in *Pluris IPSOA*; cfr. l'articolo di D. Bianchi, *Molestie, Facebook, Cyberstalking e risarcimento del danno esistenziale*, in *http://www.personaedanno.it/index.php?option=com_content&view=article&id=38623&catid=173&Itemid=420&mese=04&anno=2012.*

La virtualità: la rete.

È il titolo della relazione del Presidente del CNF, avv. prof. Guido Alpa, alla 25ª Conferenza Internazionale su "Fra individui e collettività. La proprietà nel secolo XXI"[30].

Nel corso della sua relazione il prof. Alpa ha posto il problema delle difficoltà di esecuzione nell'ambito di eventuali contenziosi in tema di rete[31].

Giurisprudenza di merito.

Segnalo la rassegna della prof. Elena Falletti[32] in tema di novità giuridiche sul web ed in particolare richiamo:

1) la pronuncia in data 12.4.2012 n. 14120/2012 del Tribunale di Milano in tema di sequestro preventivo e di differenze tra testata giornalistica web e stampa[33];

30 Conferenza organizzata dall'Osservatorio "Giordano Dell'Amore" sui rapporti tra diritto ed economia e dalla Fondazione Centro Nazionale di Prevenzione e Difesa Sociale (CNPDS) in cooperazione con la Scuola di Dottorato in Scienze giuridiche dell'Università degli Studi di Milano Associazione Di Studi su Diritto ed Economia, l'8 e 9 novembre 2012 i cui atti dovrebbero essere pubblicati prossimamente.

31 In quell'occasione ho avuto modo di porre ai relatori alcuni quesiti (pure in corso di pubblicazione) in tema di giurisdizione e competenza ed eventuali profili di responsabilità dei motori di ricerca.

32 E. Falletti, *Internet: le novità giuridiche sul web*, in *http://dottrinaediritto.ipsoa.it*.

33 In proposito cfr. anche Cass. pen. 24.2.2011, n. 7155 in *CED Cassazione*, 2011, in tema di ammissibilità del sequestro preventivo di articolo pubblicato su un sito Internet; cfr. anche Trib. Milano ord. 28.5.2002, in *Foro ambrosiano*, 2002, 322, secondo la quale anche nel caso di una pagina web dovrebbe applicarsi la normativa di cui all'art. 1 r.d.lgs. n. 561/1946 in tema di stampa che non consente di procedere al sequestro di giornali e delle altre pubblicazioni, se non in virtù di una sentenza irrevocabile dell'Autorità Giudiziaria.
Per quanto riguarda i profili di esecuzione del sequestro preventivo di un post pubblicato in blog si è osservato che "*un'errata procedura di applicazione del sequestro preventivo di un post pubblicato su di un blog può comportare la distruzione del corpo del reato, con tutte le importanti implicazioni che ne conseguirebbero sul piano probatorio. Infatti, quando l'Autorità Giudiziaria intima al Provider di rimuovere il 'brano incriminato' dal blog, questo rischia di essere direttamente cancellato e non è detto che, a distanza di mesi o forse anni, possa essere recuperato dallo stesso Provider qualora non siano state preventivamente richieste e adottate tutte le garanzie opportune per la preservazione della prova digitale.*
Pertanto, qualora la Polizia Giudiziaria non presti particolare attenzione alle modalità operative di attuazione della misura, il provvedimento, che ha carattere provvisorio, rischia di divenire definitivo", v. G. Vaciago, *E' ammissibile il sequestro preventivo di un blog?*, in *http://www.leggioggi.it/2011/03/23/sequestro-preventivo-di-un-blog-la-cassazione-lo-ammette-speriamo-solo-che-non-diventi-una-misura-definitiva/*

2) il provvedimento in data 29.5.2012 del G.I.P. di Brescia secondo il quale è ammissibile il sequestro preventivo di un sito web di condivisione di contenuti;

3) l'ordinanza in data 30.4.2012 del Tribunale di Pinerolo secondo la quale le combinazioni poste in essere dal servizio "Google suggest" non costituirebbero diffamazione e sarebbero delle mere domande tali da non integrare estremi di reato;

4) l'ordinanza inedita in data 15.11.2012 del Tribunale di Pavia, Giudice dott. Lambertucci che - nell'ambito di procedimento sommario ex art. 702-bis c.p.c. - ha, in motivazione, attribuito natura di "confessione" ad affermazioni offensive pubblicate su Facebook dal resistente condannato al risarcimento danni nei confronti del ricorrente[34 e 34bis].

---

34 Con riferimento ad alcune problematiche relative alla diffamazione a mezzo di social network v. A. Fiorenzi, op. cit., pag. 286 ove si legge che "*la mancanza di una legislazione in linea con l'evoluzione tecnologica pone problemi seri agli operatori del diritto che, si trovano a trattare prove informatiche o elettroniche senza avere a disposizione processi e strumenti d'indagine chiari, adeguati e di accertata efficacia. Dal punto di vista tecnico lo scenario risulta ancora più complesso. Da un lato la prova digitale, che per sua natura estremamente volatile e alterabile, richiede l'adozione di procedure consolidate, competenze e strumenti adeguati per tutelare la validità e integrità della prova. Dall'altro l'innovazione continua del mondo dell'Information Technology e di Internet pongono quotidianamente nuove sfide su scenari nuovi e imprevedibili in cui i processi non sono definiti, a cui i tecnici devono dare risposta garantendo il rispetto dei principi della Computer Forensics*" e che "*il caso trattato diventa molto più complesso se le entità che si vanno ad interrogare quali, il server provider, il titolare del dominio, il gestore dell'email e l'ISP non sono posti sul territorio italiano. Se queste aziende o i loro server sono posti in Stati che hanno sottoscritto accordi internazionali o bilaterali di collaborazione, le indagini possono procedere*" attraverso accurate procedure "*nei limiti previsti dagli accordi. Se invece fra i due Paesi non sussistono accordi di alcun genere, come nel caso delle relazioni dell'Italia con molti Paesi sudamericani, dell'Est Europeo e dell'Asia, è praticamente impossibile procedere nelle indagini*" (v. op. cit. pag. 316).

34 *bis* Con riferimento all'efficacia probatoria dell'email come possibile prova scritta ai fini dell'emissione del decreto ingiuntivo v. M. Scarpa in *Le nuove leggi civ. comm.* n. 1, 2011, pag. 3 ss.

A pag. 9 l'autrice afferma che "*al documento redatto con l'ausilio del computer, il quale contenga una dichiarazione negoziale ed al quale non sia apposta alcuna forma di sottoscrizione, non possa essere attribuita nessuna efficacia probatoria né sostanziale. Quanto al documento informatico sottoscritto con firma elettronica c.d. semplice, il C.a.d.*" (d.lgs. 7 marzo 2005, n. 82) "*all'art. 21, comma primo, stabilisce che 'il documento cui è apposta una firma elettronica, sul piano probatorio, è liberamente valutabile in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità' e, all'art. 20, comma primo bis, che 'l'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità'*"

E' controverso l'inquadramento dell'email nel senso che secondo alcuni potrebbe essere considerato "*documento sottoscritto con firma elettronica semplice*" mentre altri la ritengono "*come priva di sottoscrizione alcuna*" (v. per i relativi riferimenti dottrinali e giurisprudenziali le note nn. 21 e 22 dello scritto di M. Scarpa cit.).

La casistica sopra indicata offre spunti per l'approfondimento di problematiche ben lungi da una soluzione univoca.

Uno dei nodi cruciali è rappresentato dalla questione preliminare relativa alla corretta e rapida individuazione del Giudice avente giurisdizione e competenza, anche nei casi di cybercrime.

Il problema sussiste anche per la corretta individuazione del Giudice civile, in caso di illeciti commessi attraverso Internet.

Quest'ultima - pur negando che l'email possa esser qualificata come documento informatico con firma elettronica semplice – in considerazione dell'ampia definizione ("*prova scritta*" di cui all'art 633 c.p.c. che comprenderebbe anche, ad esempio, il telegramma) per l'emanazione del decreto ingiuntivo ritiene sufficiente un'eventuale dichiarazione di riconoscimento di debito o una promessa di pagamento contenuta in email.
Tuttavia considerato che quest'ultima "*non è in grado di fornire alcuna garanzia in ordine alla provenienza dall'apparente mittente, gioco forza non potrà considerarsi integrato il requisito legale richiesto dall'art 642, comma 2, c.p.c.: il messaggio infatti non potrebbe essere con certezza considerato 'proveniente' dal debitore*".
Conseguentemente "*l'email contenete una promessa di pagamento o un riconoscimento di debito potrà essere considerata prova idonea ai fini dell'ottenimento dell'ingiunzione di pagamento, ma mai in forma immediatamente esecutiva*".
L'autrice (v. pag. 16 op. cit.) auspica "*un intervento legislativo che chiarisca, in modo risolutivo, il valore dell'email, strumento che ha ormai sostituito i più tradizionali fax e addirittura la scrittura cartacea e che è ormai entrato nell'uso quotidiano in ogni settore. Sembra infatti che il legislatore si sia preoccupato di più della disciplina di strumenti per vero poco adusi (il documento informatico sottoscritto con firma digitale, o ancora la posta elettronica certificata) che non di affrontare e risolvere la questione, forse più urgente, del valore di un mezzo di fruizione comune, sul quale, peraltro, i cittadini spesso paiono riporre fin troppo affidamento*".
Nel condividere tale auspicio rilevo che, nelle more – considerata l'incertezza dell'email, *in primis* quanto alla riconducibilità all'apparente inviante e dei costi di un eventuale giudizio di opposizione – occorrerebbe, a mio parere, un *quid pluris* al fine dell'emanazione del decreto ingiuntivo, seppur non immediatamente esecutivo.
Un esclusivo affidamento, *inaudita altera parte*, sull'email della quale non è, salvo accurate indagini, certa la provenienza non dovrebbe essere sufficiente per l'emanazione di decreto ingiuntivo e causa di pregiudizio per l'eventuale resistente che fosse costretto a difendersi in costoso giudizio pur non essendo, in ipotesi, l'inviante dell'email.
Sono purtroppo note disfunzioni nell'utilizzo della mail, anche per illecite azioni di terzi generatrici di messaggi di posta elettronica che potrebbero avere solo la parvenza di provenienza dalla casella email di un determinato soggetto, ma che, in realtà, non sarebbero riconducibili ad un'azione o volontà di quest'ultimo.
In un'ottica garantista e di giusto processo ex art. 111 Cost. occorrerebbe particolare cautela nella valutazione di elementi di prova a maggior ragione nelle fasi processuali che si svolgono *inaudita altera parte*.
Per uno studio accurato in tema di valutazione delle prove richiamo l'approfondito trattato di L. P. Comoglio, *Le prove civili*, TO, 2010, 3^ ed., ed ivi in particolare pag. 529 ss. con riferimento al "*documento informatico od elettronico*".

Cybercrime ed illeciti, anche civili: globalità del fenomeno e necessità di soluzioni in tema di giurisdizione e competenza.

Durante la Conferenza Internazionale promossa dal 2 al 4 dicembre 2011 in Courmayeur dall'ISPAC[35] il dott. Buttarelli (Assistant European Data Protection Supervisor) ha richiamato l'elaborazione di normative volte a tutelare qualsiasi cittadino residente in un Paese dell'Unione Europea, precisando che la Convenzione di Budapest del 23 novembre 2001, non ancora ratificata da tutti gli aderenti, non si applica solo al cybercrime, prevedendo anche ipotesi di collaborazione tra i Paesi firmatari, ad esempio per quanto riguarda le prove.

Sempre nel corso della predetta Conferenza Ulrich Sieber - Director and Head, Criminal Law Section, Max Planck Institute - ha sottolineato l'importanza della collaborazione tra pubblico e privato al fine di contrastare il fenomeno del c.d. cybercrime.

Infatti oggi i singoli Stati non possono, da soli, disciplinare un fenomeno "globale" ed occorrono pertanto soluzioni sempre più estese e globali, anche per ricercare necessario giusto equilibrio tra sicurezza e libertà.

Sempre nel corso della predetta Conferenza Emilio Viano – Professor, Department of justice,

35 "*Cybercrime: globalità del fenomeno e sfide*" è stato il tema dell'interessante Conferenza Internazionale promossa dal 2 al 4 dicembre 2011 in Courmayeur, cit. alla nota n. 3; v. per qualche ulteriore notizia G. Siniscalchi, *Le sfide della rete e la necessità di una normativa globale in materia (relazione alla conferenza internazionale "Internet fra libertà e diritti"*, in www.aaalegalitadiritti.it, cit. e G. Siniscalchi, *Cybercrime: globalità del fenomeno e sfide*, cit.
Per una panoramica sulle tendenze e problematiche della giustizia penale di fronte alla criminalità informatica v. gli atti del Convegno di Como del 21/22 maggio 2010 *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, TO, 2011ove viene riportato altresì lo scritto di F. Cajani "*Quella casa nella prateria: gli Internet Servervice Providers alla prova del caso Google Video*" (scritto che "*trae origine dalle sollecitazione sul tema 'il diritto sulla personalità, tutela della privacy e libertà della rete' "* emerse nel seminario di studi in onore di Corso Bovio tenutosi a Milano il 20 maggio 2010 presso il Circolo della Stampa:
http://www.fondazionecalamandrei.it/html/attivita/convegni/milano_20_maggio_2010_bovio.pdf

Law and Society, American University, Washington College of Law, Washington DC – ha sottolineato l'importanza del rispetto della privacy, anche nella rete, rilevando molti attacchi, minacce a tale imprescindibile diritto che necessita di maggior tutela.

Il prof. Viano ha espresso preoccupazione per il diffuso fenomeno della “registrazione” di milioni di dati che alimentano un vero e proprio mercato di miliardi di euro considerata l'esistenza di società che sfruttano alcuni dati per finalità di marketing, talvolta senza che gli utilizzatori della rete siano a conoscenza.

Si tratta di argomenti di fondamentale importanza che meritano approfondimenti per la ricerca di soluzioni equilibrate.

Ciò affinché non vengano calpestati diritti fondamentali dell'individuo che non possono prescindere, in primis, dall'individuazione certa del Giudice avanti il quale poter tutelare eventuali diritti lesi.

Ribadisco il mio pensiero - già espresso pure per iscritto nella relazione "Le sfide della rete e la necessità di una normativa globale in materia" presentata alla Conferenza internazionale dell'11 e 12 novembre 2011 in Milano - nel senso della necessità di soluzioni rapide e, per quanto possibile, univoche, soprattutto su imprescindibili profili di carattere preliminare: giurisdizione e competenza.

Nella permanenza della situazione di grave incertezza – anche su profili preliminari imprescindibili (giurisdizione e competenza) – vi è il rischio di frustrazione per l'effettiva tutela dei diritti sostanziali che fossero lesi, sia in materia penale sia in campo civile.

In proposito richiamo la sentenza della Corte di Giustizia Europea secondo la quale “*in caso*

di asserita violazione dei diritti della personalità per mezzo di contenuti messi in rete su un sito Internet, la persona che si ritiene lesa ha la facoltà di esperire un'azione di risarcimento, per la totalità del danno cagionato, o dinanzi ai giudici dello Stato membro del luogo di stabilimento del soggetto che ha emesso tali contenuti, o dinanzi ai giudici dello Stato membro in cui si trova il proprio centro d'interessi. In luogo di un'azione di risarcimento per la totalità del danno cagionato, tale persona può altresì esperire un'azione dinanzi ai giudici di ogni Stato membro sul cui territorio un'informazione messa in rete sia accessibile oppure lo sia stata. Questi ultimi sono competenti a conoscere del solo danno cagionato sul territorio dello Stato membro del giudice adito"[36].

Nel contesto di attuale globalizzazione e relative problematiche, assumono sempre più importanza le sentenze, anche sovranazionali, che, come si è affermato, "*contribuiscono a far sì che le procedure diventino il cuore vero del diritto che sta al di là dei confini statuali*".[37]

36 Così si legge nella sentenza della Corte di Giustizia UE (Grande Sezione) in data 25 ottobre 2011 nei procedimenti riuniti C-509/09 e C-161/10; sentenza che ho avuto occasione di ricordare anche nel corso della mia relazione *Internet fra libertà e diritti*, cit.

37 V. M. R. Ferrarese, *Prima lezione di diritto globale*, ed. Laterza, 2012, ove vi sono spunti interessanti in tema di "*Diritto globale*", pag. 151. ed ivi per ulteriori spunti di riflessione.
Come giustamente affermato dall'autrice, allo stato, si "*generano 'spazi giuridici' variabili che non coincidono più con i territori degli Stati e che gli esorbitano in vario modo e in varia misura*"..."*non esiste più necessariamente un territorio predefinito politicamente per il diritto, ma che anche le diverse configurazioni spaziali del diritto - sovranazionale, internazionale, o globale - non bastano a soddisfare l'irrequietezza giuridica globale*", cfr. pag. 68/72.
L'autrice usa l'espressione "*prodotto non finito*" facendo l'esempio di un "*oggetto snodabile … che si articola di continuo, rinunciando in gran parte ad una forma fissa e definita*", op. cit. pag. 64.
Particolarmente delicato è altresì il tema della legge applicabile ed occorrerà, ovviamente, una valutazione caso per caso. Per qualche spunto sulle problematiche della materia v. F. Cajani op. cit. pag. 225 ss.