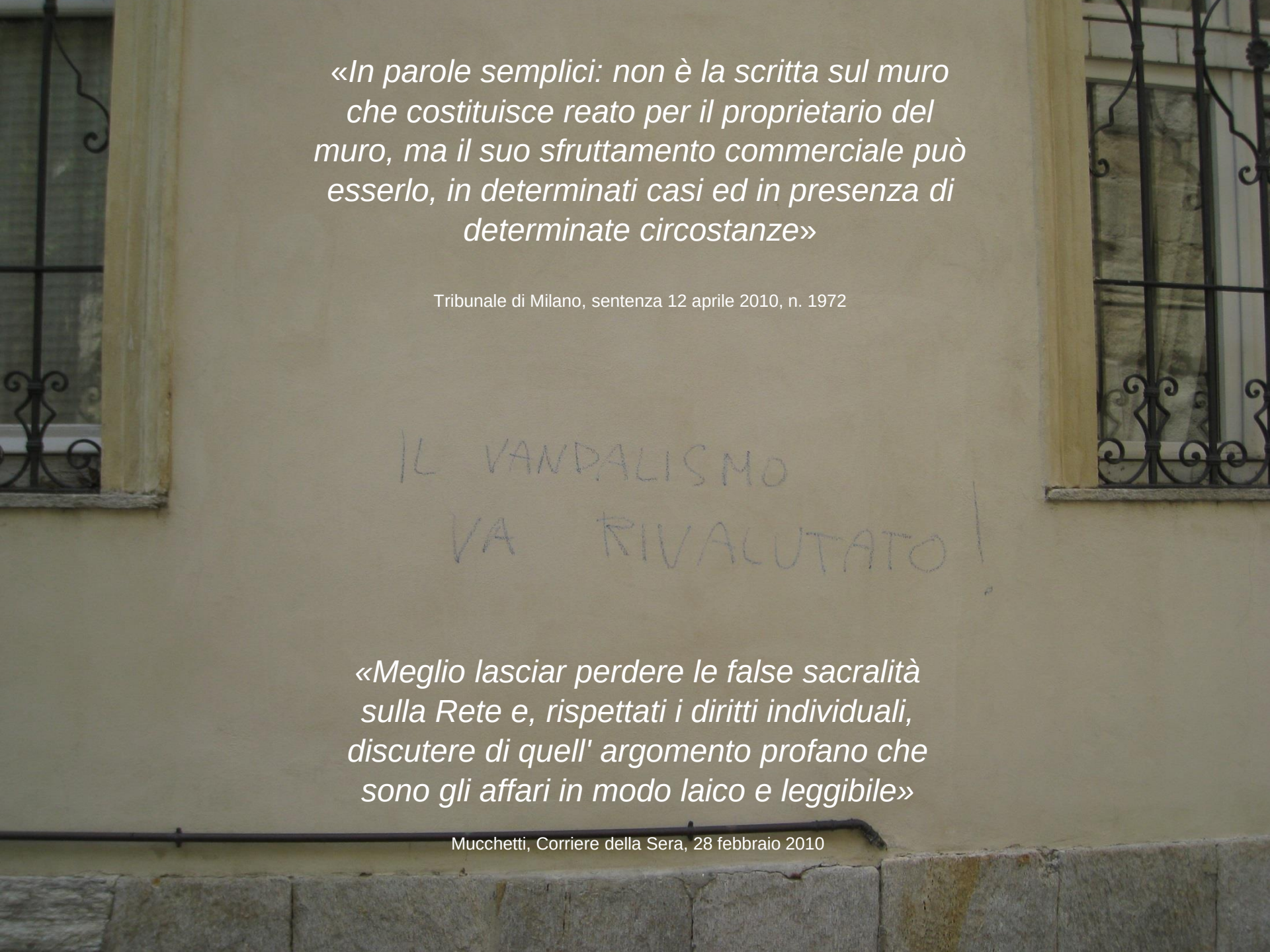
Data protection e Reg. UE 2016/679: la privacy nell'Europa 4.0

Torino, 6 novembre 2017

Giurisdizione, privacy e rapporti con gli ISP stranieri

«In parole semplici: non è la scritta sul muro che costituisce reato per il proprietario del muro, ma il suo sfruttamento commerciale può esserlo, in determinati casi ed in presenza di determinate circostanze»

Tribunale di Milano, sentenza 12 aprile 2010, n. 1972



«Meglio lasciar perdere le false sacralità sulla Rete e, rispettati i diritti individuali, discutere di quell' argomento profano che sono gli affari in modo laico e leggibile»

Mucchetti, Corriere della Sera, 28 febbraio 2010

2009/2010 → febbraio 2014

CORRIERE DELLA SERA / BLOG

HOME CORRIERE TV ECONOMIA SPORT LA LETTURA SCUOLA SPETTACOLI SALUTE SCIENZE INNOVAZIONE TEC

Vita Digitale

di Federico Cella

La trasparenza di Google

23 GIUGNO 2009 | di Federico Cella

Oggi a Milano era prevista una nuova seduta del processo "ViviDown contro Google", in cui il motore di ricerca è chiamato a rispondere di concorso in diffamazione e violazione della privacy in merito a un video del 2006 caricato su Google Video che riprendeva un ragazzo affetto dalla Sindrome di Down vessato dai compagni (qui tutti i dettagli). Il processo con rito abbreviato ha però subito uno slittamento a causa della malattia dell'interprete che avrebbe dovuto tradurre la testimonianza di un ingegnere arrivato appositamente in Italia da Mountain View. La cosa ha destato perplessità tra molti dei presenti, parti in causa e non, ma pare

«una sentenza che lascia l'amaro in bocca: a tali conclusioni si sarebbe potuto arrivare anni fa, evitando lungaggini processuali che, in un processo a forte impatto mediatico, gettano un'ulteriore ombra sul sistema giudiziario italiano. Ombre che, l'ho detto già in altra occasione, influenzano negativamente i potenziali investitori stranieri, spaventati dalle troppe incertezze della Giustizia»

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) **L'articolo 2, lettere b) e d), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell'articolo 2, lettera d), di cui sopra.**

2) **L'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro.**

3) Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

4) Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.

A differenza del caso milanese – quando Schmidt paragonò la sentenza di un tribunale legittimo a una «stronzata» (*bullshit*) – i toni cambiano. «*Siamo ligi alla legge e la legge è chiara*», afferma

La Corte di Giustizia UE, nel caso Google Spain, interpreta la legislazione privacy allo stesso modo della impostazione sostenuta dalla Procura di Milano nel caso Google vs. Vividown !

Le memorie dei PM nel caso Google Video:

F. CAJANI, ***Quella Casa nella Prateria: gli Internet Service Providers americani alla prova del caso Google Video,*** *in "Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali"* (a cura di L. PICOTTI e F. RUGGIERI), Giappichelli, 2011

volume liberamente disponibile su
https://irinsubria.uninsubria.it/

“Provider, chi era costui”?

Nozione e classificazioni

To provide = fornire

Network provider = si limita a fornire le infrastrutture di comunicazione

Access provider = consente all’utente finale di collegarsi ad Internet

Service provider = offre all’utente di disporre di ulteriori servizi (es. e-mail)

Host provider = offre all’utente lo spazio web del proprio server

Content provider = è fornitore di contenuti

Una definizione di valore giurisprudenziale dei **diversi tipi di providers** è rintracciabile nella sentenza del Tribunale di Bologna n. 331 del 14.06.2001

"*Il termine **access provider** individua il soggetto che consente all'utente l'allacciamento alla rete telematica. Il compito dell'access provider è per lo più quello di accertare l'identità dell'utente che richiede il servizio, di acquisirne i suoi dati anagrafici e, quindi, di trasmettere la richiesta all'Autorithy Italiana affinché provveda all'apertura del relativo sito Web. L'access provider può anche limitarsi a concedere al cliente uno spazio, da gestire autonomamente, sul disco fisso del proprio elaboratore. **Service provider** è invece quel soggetto che, una volta avvenuto l'accesso in rete, consente all'utente di compiere determinate operazioni, quali la posta elettronica, la suddivisione e catalogazione delle informazioni, il loro invio a soggetti determinati, ecc. **Content provider** è, infine, l'operatore che mette a disposizione del pubblico informazioni ed opere di qualsiasi genere (riviste, fotografie, libri, banche dati, versioni telematiche di quotidiani e periodici, ecc.) caricandole sulle memorie dei computers server e collegando tali computers alla rete. Content

províder è anche chi si obbliga a gestire e ad organizzare le pagine "web" immesse in rete dal proprio cliente*".

I due pilastri *ex* art. 4 Direttiva 95/46/CE:

- il **principio di stabilimento,**
- il **principio di ubicazione degli strumenti elettronici**.

Parere n. 8/2010 del Gruppo Articolo 29

Sintesi

Il presente parere chiarisce il campo di applicazione della direttiva 95/46/CE e, in particolare, dell'articolo 4, che stabilisce le disposizioni nazionali in materia di protezione dei dati adottate in attuazione della direttiva applicabili al trattamento dei dati personali. Il parere, inoltre, mette in evidenza alcuni settori suscettibili di ulteriori miglioramenti.

Definire l'applicabilità del diritto dell'UE al trattamento dei dati personali serve a chiarire la portata delle norme dell'Unione sulla protezione dei dati sia nell'UE/nel SEE, sia in un contesto internazionale più ampio. Una chiara comprensione del diritto applicabile contribuirà a garantire sia la certezza giuridica per i responsabili del trattamento sia l'esistenza di un quadro normativo preciso per le persone fisiche e altre parti interessate. Inoltre, una corretta comprensione delle disposizioni legislative applicabili dovrebbe assicurare l'assenza di lacune o di elusioni nell'elevato livello di protezione dei dati personali garantito dalla direttiva 95/46/CE.

“Quale giurisdizione”?

La giurisprudenza della
Corte di Giustizia UE

(*dopo il caso Google Spain*)

Con la sentenza C-230/14 (Weltimmo) la Corte di Giustizia europea ha sancito ulteriormente che **la forma giuridica di stabilimento (cioè il rappresentante nel territorio nazionale) non è il fattore predominante per decidere sulla giurisdizione**.

In pratica occorre verificare se:
- l'azienda esercita un'attività reale anche minima;
- l'attività viene realizzata mediante un'organizzazione stabile;
- i dati sono trattati nel contesto di tale attività.

In presenza di tali requisiti l'azienda è soggetta alla giurisdizione dello Stato nel quale esercita tale attività.

Cfr. anche il Garante privacy italiano (provvedimento 11 febbraio 2016), sulla base dei principi della sentenza Weltimmo e Google Spain:

PRESO ATTO che, pur non risultando il trattamento dei dati personali in questione effettuato direttamente dal predetto stabilimento italiano, lo stesso viene comunque svolto "nel contesto delle attività" di Facebook Italy s.r.l. e considerato altresì che le attività delle due società sono "inestricabilmente connesse" poiché l'attività svolta da Facebook Italy s.r.l. è volta a rendere economicamente redditizio il servizio reso da Facebook Ireland Ltd (cfr. art. 5, comma 1, del Codice in materia di protezione dei dati personali, art. 4 paragrafo 1, lett. A) della Direttiva 95/46/EC, sentenza della Corte di Giustizia Europea Google Spain del 13 maggio 2014);

Articolo 4 Direttiva 95/46/CE

Diritto nazionale applicabile

1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:
a) effettuato nel contesto delle attività di uno ***stabilimento del responsabile del trattamento nel territorio dello Stato membro****; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;*
b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;
c) il ***cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro****, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.*
2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento

Art. 3 Regolamento (GDPR)

Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle ***attività di uno stabilimento*** *da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) ***l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione****, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b)* ***il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione****.*
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Pur mantenendo il principio di stabilimento, e con esso il riferimento alla presenza di strumenti elettronici nel territorio dell'Unione, il GDPR oggi guarda anche ai soggetti destinatari dei servizi e beni offerti dall'azienda per stabilire la soggezione alla normativa europea.

Il Considerando 23 ritiene rilevanti, a tale scopo, fattori quali l’utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell’Unione.

(23) Onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione.

60 In the civil law cases Pammer and Halpenof, the Court of Justice of the European Union determined "whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001", and stated that:

> … it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader's overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.
>
> The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.
>
> On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established. [43]

T-CY(2015)10 Criminal justice access to data in the cloud: challenges

"It was much nicer before people started storing all their personal information in the cloud."

Dove eravamo rimasti?

(***ovvero: cosa abbiamo sostenuto, a partire dal 2008, in materia di ISP e relativa applicazione della normativa dello Stato ove vengono offerti i servizi)***

Communication interception regarding Skype, Google, Yahoo! & Microsoft tools and electronic data retention on foreign server: a legal prospective from the State which is conducting an investigation.

1st Strategic Meeting on Cybercrime

Athens, 23rd October 2008

EUROJUST

HELLENIC REPUBLIC

MINISTRY OF ECONOMY AND FINANCE

“no server no law” opinion

vs

“no server but law” opinion

“*Internet law and regulation*”: the Internet jurisdiction analysis executed by the American Courts

U.S. courts have developed two general lines of analysis in determining whether jurisdiction can be exercised in cases involving Internet activity:

- ✓ The first, a "**sliding scale" approach**, seeks to classify the "nature and quality" of the commercial activity, if any, that the defendant conducts over the Internet *[Zippo Manufacturing. Co. v. Zippo Dot Com. Inc., 952 F Supp 1199 (WD Pa 1997)]*

- ✓ The second analysis (called **"effects test"**) seeks to determine to what extent a defendant's intentional conduct outside the forum state *[Calder vs Jones, 465 U.S. 783 (1984)]*

<< The cases discussed above demonstrate that a foreign Internet entrepreneur, although lacking “continuous and systematic” contacts with any U.S. forum state sufficient to subject him or her to general jurisdiction, may nonetheless be subject to personal jurisdiction in the U.S. based on two broad theories of “specific” personal jurisdiction.

Under the *Zippo* “sliding scale” analysis, a U.S. court will classify the “nature and quality” of any commercial activity that the defendant conducts over the Internet and place it on a continuum ranging from “passive”, where no business is conducted, to “clearly conducting business”. **The closer the Internet activities are to “clearly conducting business”, the more likely that a U.S. court will exercise personal jurisdiction.**

Courts may also apply the *Calder* “effects test” to determine whether the defendant’s intentional conduct was calculated to cause harm to plaintiff within the forum state. **Where a defendant “purposefully directs” his activities at the jurisdiction, he may be liable to suit for any injury relating to or arising from those activities** >>

[G.J.H. Smith, “Internet law and regulation”, Sweet and Maxwell, 2002 (3rd edition), pp. 347-349]

(19) Il luogo di stabilimento del prestatore va determinato in base alla giurisprudenza della Corte di giustizia delle Comunità europee, secondo la quale la nozione di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata mediante l'insediamento in pianta stabile. Tale condizione è soddisfatta anche nel caso in cui una società sia costituita a tempo determinato. **Il luogo di stabilimento, per le società che forniscono servizi tramite Internet, non è là dove si trova la tecnologia del supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica**. Se uno stesso prestatore ha più luoghi di stabilimento, è importante determinare da quale luogo di stabilimento è prestato il servizio in questione. Nel caso in cui sia difficile determinare da quale dei vari luoghi di stabilimento un determinato servizio è prestato, tale luogo è quello in cui il prestatore ha il centro delle sue attività per quanto concerne tale servizio specifico.

Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico")

Contro una responsabilità del provider

È di tutta evidenza, comunque, che una improvvida estensione a carico degli ISP di obblighi di controllo, vigilanza e garanzia, nei confronti dei soggetti che materialmente commettono atti illeciti su Internet, presenta quantomeno **tre ordini di inconvenienti: uno di rilievo economico, uno di rilievo giuridico, uno di rilievo sociale**.

Da un punto di vista economico, infatti, una simile estensione potrebbe rendere eccessivamente onerosa l'attività degli ISP, i quali a loro volta potrebbero essere indotti a scaricare i maggiori costi sia su coloro che intendono immettere contenuti in rete (ossia i *content provider*), sia sugli utenti finali, ad esempio riducendo l'offerta di servizi liberi e aumentando invece quelli a pagamento: e in entrambi i casi, la conseguenza sarebbe una compressione delle potenzialità libertarie della rete . Inoltre, l'attribuzione della responsabilità agli ISP determinata dal criterio di una loro (presunta) maggiore «capienza» economica potrebbe disincentivare l'ingresso nel mercato (o agevolare l'uscita dal mercato) di operatori di piccole o medie dimensioni.

Da un punto di vista giuridico, poi, è tutt'altro che remoto il rischio che, per questa via, si arrivi a conseguenze aberranti: si consideri, in particolare, la difficoltà o anche l'impossibilità materiale da parte dell'operatore di controllare l'enorme mole di informazioni (che peraltro viene di solito aggiornata molto rapidamente) che egli ospita sulle proprie attrezzature. Inoltre, l'ISP non è necessariamente dotato delle competenze tecnico-giuridiche che lo possono mettere in condizione di riconoscere alcuni tipi di illeciti (ad esempio, le violazioni della proprietà intellettuale). Imporre una responsabilità da omesso controllo su tali contenuti a carico degli ISP equivarrebbe, di fatto, ad introdurre in maniera occulta una forma di responsabilità oggettiva, sia in campo civile che in campo penale.

Da un punto di vista sociale, infine, l'attribuzione di stringenti obblighi di sorveglianza e controllo agli ISP (al fine di evitare di incorrere nell'eventuale responsabilità) avrebbe l'effetto di indurre questi ultimi a rifiutare la prestazione dei propri servizi ad utenti «eterodossi», reputati presuntivamente non affidabili circa l'eventuale conformità ai *boni mores* delle informazioni che potranno immettere nel circuito telematico. La conseguenza, palesemente, sarebbe di trasformare il *provider* da intermediario tecnico ad «intermediario sociale», con poteri censori, in quella che finora ha rappresentato la più concreta approssimazione al *free marketplace of ideas*.

G. PINO, Assenza di un obbligo generale di sorveglianza a carico degli Internet Service Providers sui contenuti immessi da terzi in rete, 2004

La responsabilità del provider nella prime elaborazioni dottrinali

(1996-1999)

Interesse dogmatico del problema e implicazioni concrete

“Non si tratta di questione avente un interesse soltanto teorico – pur giustificato dall’ampia costellazione di istituti di <parte generale> che essa investe – bensì anche di evidente rilevanza pratica, per l’esigenza posta dalla prassi di verificare, da un lato, l’applicabilità in sede giudiziale delle disposizioni penali vigenti, e di considerare, dall’altro, l’opportunità di eventuali nuove specifiche regole, in un settore che sta diventando sempre più importante…

Si tratta, infatti, di garantire, in un quadro di certezza giuridica per operatori ed utenti, la piena esplicazione delle liberta di comunicazione e manifestazione del pensiero…; ed **altresì un’efficace tutela di altri beni ed interessi, di non minore importanza o rilevanza costituzionali, facenti capo alla collettività e ai singoli individui, riconducibili in specie alla categoria dei <diritti inviolabili dell’uomo>, e in particolare a quelli della personalità**…”

L.PICOTTI, Fondamento e limiti della responsabilità penale dei Service Providers in Internet, 1999

GLI “SCHEMI” DI RESPONSABILITA’….

- **Responsabilità per fatto proprio**
- **Responsabilità concorsuale ex art. 110 c.p.**
- **Responsabilità ex art. 40 cpv cp.**

La normativa sul commercio elettronico

Il d.lgs 70/2003 (“*Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell’informazione nel mercato interno, con particolare riferimento al commercio elettronico*”)

Il d.lgs 70/2003 (“*Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell’informazione nel mercato interno, con particolare riferimento al commercio elettronico*”) **fissa criteri di individuazione della responsabilità in relazione ad attività di:**

- **mero trasporto (*mere conduit*) delle informazioni o di semplice fornitura dell’accesso alla rete (art. 14);**
- **memorizzazione temporanea di informazioni (*caching*) allo scopo di rendere più efficace il successivo inoltro ad altri destinatari su loro richiesta (art. 15);**
- **memorizzazione duratura di informazioni (*hosting*) fornite dai destinatari del servizio (art. 16).**

L’entrata in vigore del D. Lgs. n. 70/2003 ed in particolare degli artt. 14-17, seppure in parte lacunosi da un punto di vista tecnico, permette agli operatori di potere operare in un quadro di maggiore sicurezza. In particolare per quanto attiene alla concreta responsabilità dei *service providers* la disciplina attuale è così sintetizzabile:

a) **irresponsabilità del *provider*** che si limiti a fornire la connessione alla rete (*access provider*) , con una sorta di equiparazione al gestore di una rete telefonica, assolutamente irresponsabile per gli illeciti commessi dagli utenti della rete.

b) **responsabilità del provider** che non fornisca solo la connettività, ma che eroghi anche servizi aggiuntivi (sono i casi di *caching* ed *hosting*). In tali ipotesi, però, la responsabilità è subordinata alla circostanza che il provider sappia che l’attività o l’informazione trasmessa o svolta suo tramite siano illecite.

c) La **responsabilità del provider** viene delineata quale responsabilità soggettiva, colposa o dolosa (quando il fornitore del servizio pur essendo a conoscenza della presenza sul sito di materiale sospetto, non provveda ad accertarne l’illiceità ed eventualmente a rimuoverlo).

Trattasi, come da molti osservato, di **norme che – per quanto previste in materia di responsabilità civile – appaiono ricognitive dei criteri di responsabilità, anche penali, già delineabili alla luce dei principi generali**

E’ stato ben osservato come la Direttiva 2000/31/CE (recepita dal D.lvo 70/2003) non faccia riferimento tanto agli *Internet Service Provider* quanto, più propriamente, ai cd. *Information Society Service Providers* ossia, come precisato nel titolo della sezione IV della Direttiva, agli *«intermediary service providers»*. Il che ci fa meglio comprendere, già da una prima analisi letterale, come le norme ivi previste in punto di responsabilità non siano *de plano* applicabili a tutti gli *(Internet) Service Provider* ma solamente a coloro che, nel loro modo di *fornire servizi*, possano dirsi *intermediari.*

Responsabilità nell'attività di memorizzazione di informazioni – Hosting (Art. 16)

1. Nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a. non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;

b. non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

2. ***Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.***

3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.

Art. 17 - «Assenza dell’obbligo generale di sorveglianza»:

«1. **Nella prestazione dei servizi di cui agli articoli** 14, 15 e **16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite**.

2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto:

a) ad informare senza indugio l’autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell’informazione;

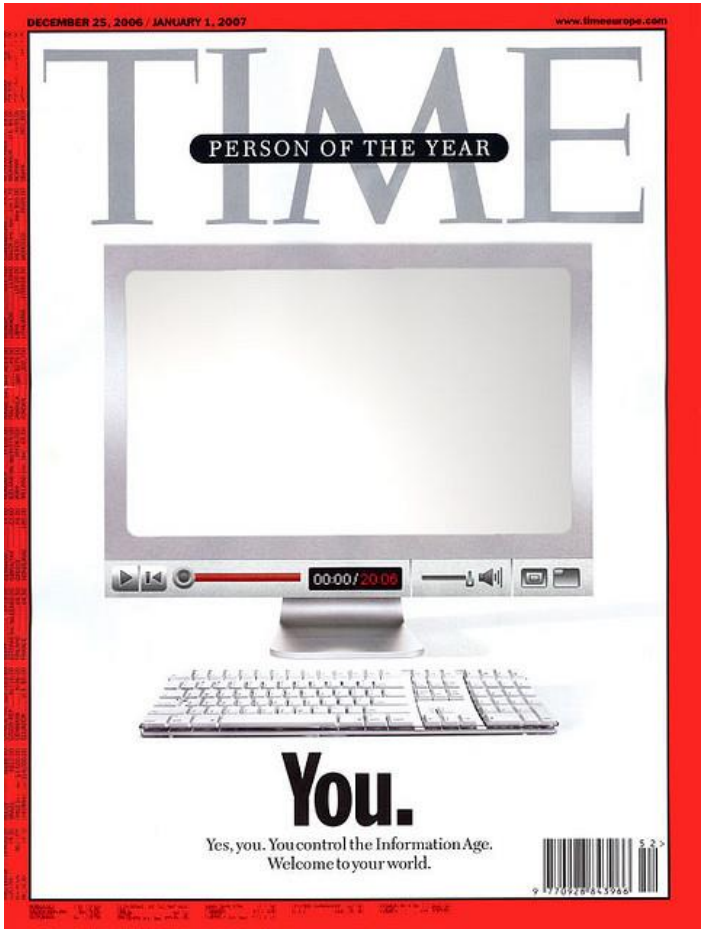
b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l’identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall’autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l’accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l’accesso, non ha provveduto ad informarne l’autorità competente».

E’ davvero difficile pensare che la Direttiva 2000/31/CE avesse in mente anche il fenomeno del cd. web 2.0: e questo per un dato prima logico e cronologico che giuridico.

Il famoso articolo di Tim O’Reilly *«What is Web 2.0»* nel quale si ritrova, per la prima volta, una definizione del fenomeno (oltre che il suo nome di battesimo) è del settembre del **2005**.

Nel febbraio dello stesso anno nasceva *Youtube*, il cui omonimo sito diventò operativo due mesi dopo. L’avvento di *Google Video*, anche se di poco precedente, sarà tutto una rincorsa verso l’acquisizione del suo maggiore *competitor*, che avverrà nell’ ottobre **2006**. E proprio alla fine di quell’anno la rivista americana *Time* sancirà l’affermarsi del Web 2.0 con quella famosa scritta sulla copertina: *«Time’s Person of the Year: You»* .



Sebbene la Comunicazione della Commissione al Parlamento (COM)97 157 facesse riferimento a numerose attività di *e-commerce*, nella Direttiva 2000/31/CE *«il commercio elettronico viene circoscritto ai servizi della società dell'informazione, cioè a qualsiasi servizio normalmente prestato dietro retribuzione, a distanza, senza la presenza simultanea delle parti, per via elettronica, con riferimento esclusivo alla comunicazione e a richiesta individuale di un destinatario di servizi»* [G. COMMANDE' – S. SICA, *Il commercio elettronico. Profili Giuridici*, Torino, 2001, pp. 5-6].

Alla fine degli anni '90 pertanto esistevano solo gestori di telecomunicazioni che era in grado fornire

- connettività (tra le parti),
- spazio web (a mezzo del quale si potesse aprire "un negozio sulla Rete"),
- servizi di ricerca (a mezzo di appositi motori di ricerca),

con ciò rendendo (di fatto tecnicamente) possibile l'esistenza di tale *«commercio elettronico»*.

La natura di tali servizi offerti dal *«prestatore»*, di regola peraltro per la maggior parte gratuiti, anche ove fossero stati a pagamento per l'utente evidenziavano comunque un dato ben preciso: l'assoluta irrilevanza, per il prestatore, di quanto venisse "veicolato" per il tramite dei servizi da lui offerti.

Si arriva quindi alla individuazione dei criteri di cui agli artt. 14 ss D.lvo 70/2003, dove *l'host provider* (per quanto riguarda il caso che a noi interessa) viene necessariamente inteso nel senso già indicato, *«considerato che la sua prestazione non incide – anzi, non deve incidere – sul contenuto della comunicazione on line»* [S. SICA in G. COMMANDE' – S. SICA, *op. cit*, p. 223].

Su tale presupposto convergono tutti i più importanti commenti dottrinali in materia.

E la stesse definizioni di *host provider* sono in linea con quanto finora affermato, laddove autorevolmente è stato sostenuto come *«la finalità della prestazione di hosting è, dunque, quella di consentire alla clientela di pubblicare* on line *e gestire autonomamente brevi contenuti, ovvero un integrale sito web, senza, tuttavia, acquisire e gestire l'hardware e le infrastrutture di telecomunicazione occorrenti per la divulgazione in Rete, valendosi allo scopo di mezzi messi a disposizione dal* provider*»* [I.P. CIMINO, *I contratti degli Internet Providers e per i data services on line* in G. CASSANO - I.P. CIMINO (a cura di), *Diritto dell'internet e delle tecnologie telematiche*, Padova, 2009, p. 20]

Ed infatti *«la* guide line *è esplicitata nei considerando 42) e 43) »* della Direttiva 2000/31/CE*: «si può discorrere di esonero di responsabilità del* prestataire, *purchè egli non sia "in alcun modo coinvolto nell'informazione trasmessa" ed assolva ad un ruolo "di ordine meramente tecnico, automatico e passivo"»* [S. SICA in G. COMMANDE' – S. SICA,, *op. cit*, p. 229].

Questo principio emerge già fin dalla Proposta della Commissione Europa del 1998 ove, a commento della sezione IV dedicata alla *«responsabilità degli intermediari»*, si legge come *«soltanto le attività coinvolte nella prestazione di servizi di intermediazione online rientrano in tale fattispecie»*.

Della *ratio* di una simile impostazione vi è una testuale conferma **nell'art. 16 comma 2 d.lvo 70/2003** che prevede, in conformità con la previsione dell'art. 14 comma 2 Direttiva 2000/31/CE, come il regime di responsabilità indicato dall'art. 16 comma 1 non si applichi *«se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore»*. In questo caso *«il provider non agisce da mero intermediario, ma è il soggetto che volontariamente decide quali informazioni trasmette e attraverso quali modalità»* [G. M. RICCIO, *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e responsabilità*, 2003, 12, 1164], con consequenziale applicazione delle ordinarie norme sulla responabilità.

Ebbene tale norma era volta a distinguere nettamente la figura dell' *host provider* da quella del *content provider* e non poteva prendere espressamente in considerazione – per quanto analizzato in precedenza - la diversa figura di colui che, nella memorizzazione dei contenuti, li sfrutta commercialmente ponendo in essere una condotta *attiva* su di essi (fin dalla loro immissione nella piattaforma informatica).

Tale ultima ipotesi è stata definita – dalla più attenta dottrina anglosassone e dalla giurisprudenza francese - come quella dell' ***hoster attivo***, identificandola altresì come figura problematica (ai fini della individuazione del regime di responsabilità) in quanto si pone nel mezzo tra la posizione di (mero) *hosting provider* e quella di *content provider* (ovvero di produttore "in proprio" di contenuti).

L. EDWARDS, *The Fall and Rise of Intermediary Liability Online*, in L. EDWARDS – C. WAELDE, *Law and the Internet*, 3 ed, Oxford and Portland, 2009, p. 62. pp. 47 ss.

Tribunale Ordinario di Roma, XI sezione civile, ordinanza 16 dicembre 2009

(ud. 24 novembre 2009) in *Guida al Diritto*, 2, 9 gennaio 2010, 56 ss.

"***la normativa - vedi d.lgs n. 70/2003 - e la giurisprudenza sta ormai orientandosi nel senso di una valutazione caso per caso della responsabilità del provider".***

"ritenuto che, a fronte di una condotta così palesemente e reiteratamente lesiva dei diritti ***non è sostenibile la tesi delle resistenti su una presunta assoluta irresponsabilità del provider che si limiterebbe a svolgere l'unica funzione di mettere a disposizione gli spazi web*** *sui quali gli utenti gestirebbero i contenuti dagli stessi caricati e sulla legittimità di avere un ritorno economico - escludendo il fine commerciale - connesso al proprio servizio in mancanza di un obbligo di controllare i contenuti illeciti e disabilitarne l'accesso;* ***tali asserzioni infatti sono smentite dagli stessi scritti difensivi delle convenute nonché dalla documentazione prodotta in giudizio relativa alle indicazioni desumibili sui siti YouTube e Google riguardanti "le regole" stabilite dal provider****, che consentono la esclusione di contenuti pedopornografici, prevedono l'accettazione dell'utente di ogni aggiornamento deciso da YouTube, il diritto di controllare i contributi, la assoluta discrezionalità nell'interrompere in maniera temporanea o permanente la fornitura del servizio «in qualsiasi momento, senza previo avviso ed a sua esclusiva discrezione» nonché il diritto di risolvere il contratto con l'utente quando la fornitura non è più «vantaggiosa dal punto di vista commerciale»….* ***nella specie innegabile ed evidente è la responsabilità delle convenute che, oltre ad organizzare la gestione dei contenuti video, anche a fini di pubblicità (raccolta con le diverse modalità disponibili sulla Rete)****, nonostante le ripetute diffide e le azioni giudiziarie iniziate da Rti e la consapevolezza della sua titolarità dell'opera hanno continuato la trasmissione …. ad ulteriore, anche se non necessaria conferma, della consapevolezza della violazione dei diritti sicuramente inconciliabile con l'addotta semplice «messa a disposizione della piattaforma»"*

Cfr. la **sentenza della Corte Europea del 23 marzo 2010** *in materia di* keyword advertising che, sebbene fu affrettatamente commentata come favorevole a Google, ad un più attento lettore indica che *«l'art. 14 della direttiva 2000/31 deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati»*.

Il bilanciamento di contrapposti diritti costituzionalmente garantiti

….. due parole sulla libertà di iniziativa economica (art. 41 Cost):

"*Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla* ***dignità umana***"

Lo scenario internazionale:

dal caso Yahoo! Belgio

al caso Microsoft vs. U.S.A

Court of Appeal of Antwerp confirms Yahoo!'s obligation to cooperate with law enforcement agencies

15.07.2014

On 20 November 2013, the Court of Appeal of Antwerp partially confirmed the Criminal Court of Dendermonde's judgment dated 2 March 2009. The Criminal Court convicted Yahoo! and obliged it to disclose the identity of the persons who committed fraud via their Yahoo! e-mail accounts.

The public prosecutor of Dendermonde had requested US-based Yahoo! to disclose the identity of certain people who used their Yahoo! e-mail accounts to commit Internet fraud. The public prosecutor's charge against Yahoo! was based on Article 46bis of the Criminal Procedure Code, which obliges electronic communication services providers to disclose identification data to law enforcement agencies when these agencies request them. Although Yahoo! is established in the US and has no branch or office in Belgium, the public prosecutor was of the opinion that Yahoo! is considered an electronic communications service provider and is consequently obliged to comply with law enforcement agencies' request for such information.

Yahoo!, however, refused to disclose the identification data, arguing that it is not subject to Article 46bis of the Criminal Procedure Code because it was not an electronic communications service provider. According to Yahoo!, the term "electronic communications service provider" in Article 46bis of the Criminal Procedure Code had the same meaning as the term "electronic communications service provider" in Article 2 of the Electronic Communications Act of 13 June 2005. Since this Article 2 states that a provider of information society services, such as providers of free e-mail addresses, are not considered a provider of electronic communications services, Yahoo! asserted that it was not obliged to disclose identification data to the public prosecutor.

The Criminal Court of Dendermonde did not follow Yahoo!'s argument, but Yahoo! challenged the decision successfully before the Court of Appeal of Ghent. However, the public prosecutor appealed this decision before Belgium's supreme Court (Cour de cassation/Hof van cassatie), and

YAHOO!
voor mobiel
Download in de App Store
VERKRIJGBAAR OP Google play

UNITED STATES DISTRICT COURT

for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation	))))))	Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Microsoft

14-2985-cv

United States Court of Appeals

for the

Second Circuit

In the Matter of a Warrant to Search a Certain E-mail Account
Controlled and Maintained by Microsoft Corporation

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF FOR *AMICI CURIAE* COMPUTER AND DATA SCIENCE EXPERTS IN SUPPORT OF APPELLANT MICROSOFT CORPORATION

https://www.eff.org/files/2014/12/15/computer_science_experts_microsoft_ireland_amicus_brief.pdf

CONSEIL DE L'EUROPE

26 May 2015
Strasbourg, France

T-CY (2015)10
Provisional

Cybercrime Convention Committee (T-CY)

Criminal justice access to data in the cloud: challenges

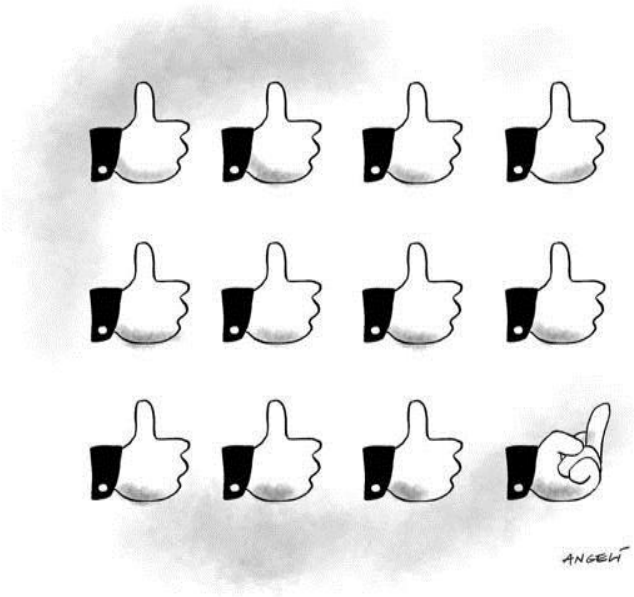
Discussion paper

prepared by the T-CY Cloud Evidence Group

https://www.coe.int/en/web/cybercrime

A proposito della evoluzione della tecnologia:

7 CORRIERE DELLA SERA
18 maggio 2017 – n. 20



I social potrebbero fare di più per arginare il fenomeno dell'*hate speech*? E come?

Certamente sì. Già nel 2006, durante il processo Google vs. l'Associazione Vivi Down*, scoprimmo che vi erano almeno 19 saggi scientifici (due dei quali a firma di ingegneri di Google) sulla possibilità di effettuare un controllo automatizzato, non esaustivo ma in grado di fornire all'operatore umano la possibilità di eliminare il più possibile, da subito, materiale indebito. Facemmo inoltre presente al Giudice come sarebbe bastato un controllo semantico sul titolo del video per impedire il protrarsi della diffusione dello stesso. Il discorso dell'impossibilità di controllare a me sembra una presa in giro all'intelligenza di coloro che sanno veramente di cosa stiamo parlando. Lo era allora e lo è a maggior ragione oggi, vista l'evoluzione delle tecniche e degli algoritmi di filtraggio. A otto anni dalla nostra Requisitoria, citerei ancora Victor E. Frank: «Se sulla costa dell'Oceano Atlantico, in arrivo al porto di New York, i passeggeri incontrano la Statua della Libertà, sarebbe meraviglioso poter edificare sulla costa opposta la Statua della Responsabilità».

S. Chia.

*Processo sul filmato caricato su Google Video che mostra alcuni studenti umiliare un compagno affetto dalla sindrome di Down e insultare l'associazione Vivi Down.

Prof. Sebastiano Battiato, Ph.D.
Dipartimento di Matematica e Informatica - Università di Catania
CITTÀ UNIVERSITARIA - Viale A. Doria, 6 – I 95125 – CATANIA

Image Processing Laboratory
http://www.dmi.unict.it/~iplab

Estratto/sintesi consulenza tecnica caso *Google vs. Vividown* realizzata per conto della Procura di Milano (incarico del 18 Aprile 2009).

La consulenza in questione ha dimostrato in maniera inequivocabile e documentata come all'epoca dei fatti (che risalgono al 2006) fossero già disponibili delle tecnologie in grado di automatizzare il processo di classificazione dei contenuti multimediali presenti nella Rete rispetto ai contenuti di alto livello o comunque nei casi specifici di classi "semantiche" omogenee (per esempio il genere: sportivo, spettacolo, ecc.) e non specifici contenuti (per esempio la ricerca di una data persona o di un dato oggetto o luogo, ecc.). Questo aspetto pone il problema dell'individuazione e quindi del controllo automatizzato sulla introduzione di video illeciti o potenzialmente tali, su un piano operativo di fattibilità non trascurabile.

http://www.dmi.unict.it/~battiato/download/Estratto%20Consulenza_Google_vs_ViviDown.pdf

john
2 giorni fa
Che bella classe di dementi e minorati! E ovviamente non mi riferisco al povero ragazzo preso crudelmente in giro. Complimenti ai genitori e agli insegnanti...
Anonimo
2 giorni fa
Vergogna...
gregorj
2 giorni fa
Complimenti: siete finiti su http://giornalettismo.ilcannocchiale.it
Anonimo
3 giorni fa
E' vergognoso! Andrebbe tolto immediatamente.
ummm
4-ott-2006
c'è più di un mongoloide in quella classe
ummm
4-ott-2006
madu che schifo

«La pagina web con i commenti non esiste più nella sua forma originale.

Da un punto di vista tecnico, se i nostri ingegneri provassero a ricreare la pagina web con i commenti, dovrebbero formulare supposizione e congetture relativamente al codice HTML originale. Ciò comporta che è improbabile che un simile tentativo possa essere completo e avere un risultato attendibile. Inoltre si tratta di un processo particolarmente complesso che richiederebbe un significativo dispendio di impegno e di energie da parte di ingegneri e apparecchiature elettroniche»

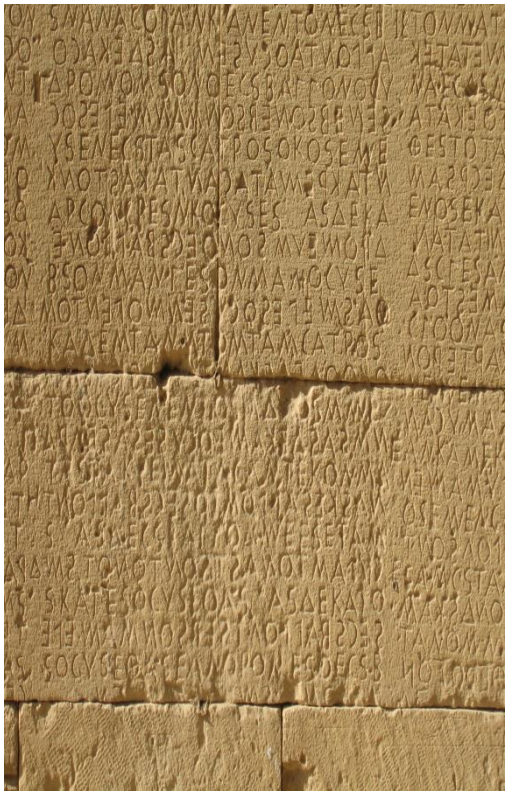
[risposta di Google Inc. nel caso Google vs. Vividown]

Conclusioni

“un atteggiamento così fortemente restrittivo, nel delineare e circoscrivere *ab origine* l’eventuale sfera di responsabilità penale dei *Providers,* non appare condivisibile, oltre che per le ragioni tecnico giuridiche che si esporranno, anche perché appare troppo sbilanciato, su di un piano di valutazione generale, a favore dell’esigenza di garantire le migliori e più libere condizioni d’esercizio della loro pur importante attività, unitamente ai fondamentali diritti di comunicazione e manifestazione del pensiero dei consociati: sacrificando, però, le contrapposte ed altrettanto esigenze di tutela di quei beni giuridici fondamentali, che ne costituiscono legittimo limite”.

L. PICOTTI, 1999

In conclusion, a strictly personal consideration …



Francesco Cajani

Procura della Repubblica presso il Tribunale di Milano

francesco.cajani@giustizia.it

www.iisfa.net