UNIVERSITÀ DI TRENTO

DIPARTIMENTO
FACOLTÀ DI GIURISPRUDENZA

lawtech
The Law and Technology Research Group

Università di Trento
Facoltà di Giurisprudenza
Diritto civile A-J
2020-2021
Prof. Roberto Caso

Lezione 15 – Il diritto all'anonimato

Questa lezione ha tre scopi:

1. Presentare il caso 1 e il relativo problema;

2. Accennare alla relazione tra anonimato, responsabilità civile e diritto alla protezione dei dati personali, illustrando una possibile soluzione al problema posto dal caso 1;

3. Delineare il caso 2, lasciando agli studenti il compito di formulare e risolvere il problema.

Parte 1 – Caso 1

> "La casa di edizioni musicali X, tramite l'impresa di sorveglianza digitale Y che offre servizi di monitoraggio di reti Peer to Peer, individua indirizzi Internet (IP) a cui sarebbero riconducibili violazioni del diritto d'autore.
> La stessa casa editrice cita in giudizio l'Internet Service Provider (ISP) che ha fornito l'accesso Internet agli abbonati ai quali sono riconducibili gli indirizzi IP individuati. In particolare, chiede all'ISP l'ostensione dei dati personali degli abbonati.
> L'ISP si rifiuta.
> Qual è il problema? Qual è la soluzione?"

Parte 2 – Anonimato, responsabilità civile e protezione dei dati personali

L'anonimato è strumento di libertà. In particolare, è strumento di libertà di manifestazione del pensiero (un pilastro della democrazia).
Ora è anche un diritto (almeno secondo alcuni), parte del diritto alla protezione dei dati personali.

Allo stesso tempo, l'anonimato può mascherare il responsabile di un atto illecito.

Il problema è stato affrontato per i mezzi di comunicazione di massa analogici ed è diventato di fondamentale importanza nell'era di Internet.

L'anonimato è parte della storia di Internet (ad es., TOR, wireless community networks ecc.).
Una rete priva dell'anonimato renderebbe egemone la sorveglianza di massa.

Scrive in proposito Giorgio Resta [Resta 2020, 487, note omesse]:

> [Nell'analisi di diritto comparato, il modello giuridico imperniato sul riconoscimento di principio della liceità dell'anonimato online] "è ritenuto da molti coessenziale ai tratti distintivi dello spazio cibernetico, come sin qui conosciuto. È conforme alla natura della rete e ai suoi caratteri di intrinseca democraticità, si osserva da più parti, incentivare uno scambio quanto più autonomo, libero e decentrato di idee e informazioni e permettere la costruzione di rapporti sociali su base volontaria e persino artificialmente definita. L'anonimato – ivi compreso il ricorso a network anonimi come TOR – rappresenterebbe uno dei più importanti strumenti di salvaguardia di tali caratteristiche. Esso, da un lato, consentirebbe la libera manifestazione del pensiero e la libera esplica- zione della personalità di ciascun individuo (nel senso dell'art. 2 Cost.), ponendolo al riparo dai rischi di intimidazione e stigmatizzazione propri del mondo reale".

Sussiste però il problema dei soggetti colpiti da illeciti schermati da anonimato (in particolare, illeciti compiuti contro persone fisiche e gruppi di persone).

Con riferimento alla responsabilità civile per illeciti commessi tramite la Rete il primo punto di riferimento è rappresentato dagli Internet Service Provider (ISP), ovvero i fornitori dei servizi Internet (connessione, memorizzazione, pubblicazione di contenuti ecc.).

Giovanni Pascuzzi rileva sul punto [Pascuzzi 2020, 309]:

> Gli ISP "svolgono un ruolo delicato, perché di fatto, sembrano poter controllare la rete e ciò che viaggia al suo interno. Ne deriva che possono, in linea teorica, evitare che tramite la rete vengano commessi abusi. Ma se davvero si attribuisce a loro un potere di controllo di questo tipo, automaticamente li si eleva a potenziali censori. In ogni caso hanno la caratteristica di poter diventare bersaglio naturale delle richieste di risarcimento da parte delle vittime di illeciti: sia perché facilmente identificabili sia perché economicamente più in grado di corrispondere i risarcimenti di quanto non possa esserlo il singolo autore dell'illecito"

Attualmente la responsabilità degli ISP è disciplinata dagli art. 12, 13, 14, 15 della direttiva "commercio elettronico" 2000/31/CE e dagli art. 14, 15, 16 e 17 del d.lgs. 9 aprile 2003, n. 70 di attuazione della medesima direttiva.

Il modello giuridico a cui si è ispirato il legislatore europeo è quello statunitense. L'idea dominante negli anni in cui furono emanate quelle normative era di favorire lo sviluppo di ISP commerciali e di evitare di caricare gli stessi di una responsabilità gravosa. La direttiva commercio elettronico, dunque, pone il principio dell'assenza di un obbligo generale di sorveglianza e individua alcune esenzioni di responsabilità riferibili ad alcune categorie di ISP.

Il principio generale dell'assenza di un obbligo generale di sorveglianza è posto dall'art. 15.1 della direttiva commercio elettronico:

> "[…] gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite".

L'art. 12 direttiva 2000/31 così recita:

> "Semplice trasporto ("mere conduit")
> 1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli:
> a) non dia origine alla trasmissione;
> b) non selezioni il destinatario della trasmissione; e
> c) non selezioni né modifichi le informazioni trasmesse.
> 2. Le attività di trasmissione e di fornitura di accesso di cui al paragrafo 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.
> 3. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione".

L'art. 13 direttiva 2000/31 così recita:

“Memorizzazione temporanea detta "caching"
1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli:
a) non modifichi le informazioni;
b) si conformi alle condizioni di accesso alle informazioni;
c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore,
d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e
e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso.
2. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione”.

L’art. 14 direttiva 2000/31 così recita:

“"Hosting"
1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:
a) non sia effettivamente al corrente 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'illegalità dell'attività o dell'informazione, o
b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.
2. Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.
3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime”.

Il regime di favore dell’ISP è stato progressivamente eroso per via giurisprudenziale e per via normativa (si veda, in particolare, la giurisprudenza sulla distinzione tra hosting provider attivo e passivo; nonché l’art. 17 della direttiva 2019/790 UE sul diritto d’autore nel mercato unico digitale).

Svolti questi brevi cenni sulla responsabilità dell’ISP è ora il momento di illustrare la soluzione al caso 1 che riguarda il confronto tra tutela della proprietà intellettuale (nello specifico, il diritto d’autore) e diritto all’anonimato come parte del diritto alla protezione dei dati personali.

Il primo decennio del terzo millennio ha visto fiorire diverse tecnologie per lo scambio di file tra utenti di Internet (*file sharing*). Tali tecnologie vengono denominate Peer to Peer (P2P) con riferimento al fatto che gli utenti non hanno bisogno di altri intermediari all'infuori dell'ISP che fornisce l'accesso e la connessione a Internet.

Le reti P2P possono essere utilizzate, come in generale Internet, per fini leciti e illeciti.
I titolari del diritto d'autore hanno adoperato diverse strategie di contrasto all'uso delle reti P2P per lo scambio non autorizzato di opere protette dal diritto d'autore.
Tra queste strategie, figura la sorveglianza sistematica (monitoraggio) delle reti P2P.

Scrivono in proposito Caso e Pascuzzi [Caso, Pascuzzi 2020, 228, note omesse]:

> "Alcune imprese titolari di diritti d'autore su repertori di opere musicali si servono di altre imprese, che forniscono, mediante l'utilizzo di appositi software, servizi di monitoraggio delle reti P2P, al fine di individuare e memorizzare elementi che comprovino le violazioni dei propri diritti e l'individuazione dei responsabili di tali violazioni. L'esatto funzionamento dei software di monitoraggio non è chiaro (anche perché sembra coperto da segreti industriali). Tali software sono in grado di tracciare e memorizzare una serie di informazioni – tra le quali gli indirizzi IP – relative alle presunte attività illecite. Una volta ottenute le informazioni (in particolare, gli indirizzi IP), le imprese titolari dei diritti d'autore richiedono (direttamente, o per il tramite delle associazioni di categoria) agli Internet Service Providers (ISP) coinvolti nel traffico P2P di rivelare l'identità e l'indirizzo fisico delle persone titolari delle utenze telefoniche associabili agli indirizzi IP tracciati. Nei casi in cui gli ISP si rifiutano di fornire i dati, le imprese titolari agiscono presso il giudice civile per ottenere coattivamente le informazioni. In Europa queste azioni si basano sulla direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale".

Scrive in proposito Giorgio Resta [Resta 2020, 504, note omesse]:

> […] "si deve rilevare che, a seguito dell'approvazione della direttiva 2004/48/CE, gli Stati Membri si sono dotati di un sistema processuale di tutela della proprietà intellettuale particolarmente incisivo e penetrante. Esso annovera al suo interno anche misure istruttorie, e segnatamente lo strumento dell'ordine di esibizione e della richiesta di informazioni su fatti rilevanti per il processo, il quale rende utili servigi anche nel campo degli illeciti commessi online in forma anonima".

Caso e Pascuzzi rilevano quanto segue:

> "Una causa spagnola vertente su una di queste azioni è giunta davanti alla Corte di giustizia CE. La questione sottoposta al giudizio della Corte atteneva alla compatibilità della legge spagnola con la trama di direttive comunitarie relative, oltre alla proprietà intellettuale (il riferimento è alla direttiva 2004/48 appena citata), al commercio elettronico e alla protezione dei dati personali nelle comunicazioni elettroniche, incentrandosi sul quesito relativo alla sussistenza dell'imposizione rivolta agli Stati membri di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento

civile. La risposta della Corte è stata che il diritto comunitario non impone di istituire tale obbligo.

Ma in un caso più recente la Corte sembra aver assunto una posizione maggiormente favorevole ai titolari di copyright. Nella sentenza Bonnier Audio i giudici di Lussemburgo hanno stabilito che la direttiva 2006/24/Ce del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce, dev'essere interpretata nel senso che non osta all'applicazione di una normativa nazionale, istituita sulla base dell'art. 8 direttiva 2004/48/Ce del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale, la quale, ai fini dell'identificazione di un abbonato a Internet o di un utente Internet, consenta di ingiungere a un operatore Internet di comunicare al titolare di un diritto di autore ovvero al suo avente causa l'identità dell'abbonato al quale sia stato attribuito un indirizzo IP (protocollo Internet) che sia servito ai fini della violazione di tale diritto. […]

Nel più recente caso McFadden la Corte di giustizia UE ha stabilito che il diritto europeo non vieta l'adozione di un'ingiunzione che imponga a un fornitore di accesso a una rete di comunicazione che consente al pubblico di connettersi a Internet (collegamento wi-fi), di impedire a terzi di rendere disponibile al pubblico, attraverso tale connessione a Internet, su una piattaforma Internet di condivisione (peer-to-peer), una specifica opera protetta dal diritto d'autore o parti di essa, qualora il fornitore abbia la possibilità di scegliere le misure tecniche da adottare per conformarsi a detta ingiunzione. Specificando che ciò rimane fermo anche se tale scelta si riduca alla sola misura consistente nel proteggere la connessione a Internet mediante una password, nei limiti in cui gli utenti di detta rete siano obbligati a rivelare la loro identità al fine di ottenere la password richiesta e non possano quindi agire anonimamente, circostanza che spetta al giudice del rinvio verificare".

L'Italia ha dato attuazione alla direttiva 2004/48/CE modificando la legge autore (l. 1941/633). Particolarmente rilevante, per le controversie qui in discussione, è l'art. 156-bis della l. 1941/633 che così recita:

"1. Qualora una parte abbia fornito seri elementi dai quali si possa ragionevolmente desumere la fondatezza delle proprie domande ed abbia individuato documenti, elementi o informazioni detenuti dalla controparte che confermino tali indizi, essa può ottenere che il giudice ne disponga l'esibizione oppure che richieda le informazioni alla controparte. Può ottenere altresì, che il giudice ordini alla controparte di fornire gli elementi per l'identificazione dei soggetti implicati nella produzione e distribuzione dei prodotti o dei servizi che costituiscono violazione dei diritti di cui alla presente legge.

2. In caso di violazione commessa su scala commerciale il giudice può anche disporre, su richiesta di parte, l'esibizione della documentazione bancaria, finanziaria e commerciale che si trovi in possesso della controparte.

3. Il giudice, nell'assumere i provvedimenti di cui ai commi 1 e 2, adotta le misure idonee a garantire la tutela delle informazioni riservate, sentita la controparte.

4. Il giudice desume argomenti di prova dalle risposte che le parti danno e dal rifiuto ingiustificato di ottemperare agli ordini".

> “In Italia una controversia di questo genere è stata oggetto – oltre che di una serie di pronunce del Tribunale di Roma – di un pronunciamento del garante per la protezione dei dati personali il quale ha dichiarato illeciti i trattamenti effettuati dai soggetti coinvolti nel monitoraggio delle reti P2P, vietandone l’ulteriore trattamento e disponendone la cancellazione” [Caso, Pascuzzi 2020, 229].

Ecco allora la soluzione al problema posto dal caso 1.

Il Garante per la protezione dei dati personali nel provvedimento 28 febbraio 2008 ha affermato, tra l’altro, quanto segue:

> “I trattamenti in esame, effettuati in modo massivo e capillare per un periodo di tempo prolungato e nei riguardi di un numero elevato di soggetti, hanno consentito di tenere traccia analitica delle operazioni compiute da innumerevoli, singoli utenti relativamente a specifici contenuti protetti dal diritto d’autore.
>
> Per le modalità con le quali la raccolta dei dati è stata svolta, si è configurata un’attività di monitoraggio vietata a soggetti privati dalla direttiva 2002/58/Ce (art. 5; cfr. art. 122 del Codice). […]
>
> Le reti p2p sono finalizzate allo scambio fra utenti di dati e file per scopi sostanzialmente personali, mentre il software fsm "non è destinato allo scambio di dati, ma al monitoraggio ed alla ricerca di dati, che utenti di reti P2P mettono a disposizione a terzi" […]. I dati che gli utenti mettono in rete possono essere utilizzati per le finalità per le quali tale pubblicazione avviene […]. L’utilizzo dei dati dell’utente delle reti peer-to-peer può, quindi, avvenire per le finalità sue proprie e non già, in modo non trasparente, per scopi ulteriori, quali quelli perseguiti da Logistep, Peppermint e Techland.
>
> Il trattamento è risultato viziato anche sotto il profilo della trasparenza e della correttezza, posto che non è stata fornita alcuna informativa preliminare agli utenti. Dalla descrizione resa dalle società sul funzionamento del software fsm si è potuto rilevare che, mentre gli indirizzi Ip sono stati acquisiti da un terzo rispetto agli utenti (il tracker), gli altri dati (ossia, i file offerti in condivisione, data e ora del download) sono stati raccolti direttamente presso gli interessati”.

Qui di seguito la soluzione del Tribunale di Roma 14 luglio 2007 [in Dir. Internet, 2007, 463]:

> “Il titolare di diritti d'autore non ha diritto ad ottenere dal provider, in via d'urgenza, ex art. 156 bis l.a. l'ostensione dei dati anagrafici degli assegnatari degli indirizzi IP che, sulla base dei dati da esso autonomamente raccolti, appaiono essere autori di condotte di violazione dei propri diritti d'autore attraverso piattaforme di peer to peer; l'esercizio di tale diritto è precluso dalla vigente disciplina in materia di privacy e trattamento dei dati personali alla stregua della quale è illecita l'attività di raccolta degli indirizzi IP degli utenti di una piattaforma peer to peer in assenza di prestazione di idonea informativa all'interessato, acquisizione del consenso e notifica al garante per il trattamento dei dati personali; a tale illiceità consegue la radicale inutilizzabilità dei dati raccolti ex art. 11 codice privacy; in ogni caso l'art. 156 bis l.a. non consentirebbe la comunicazione dal provider al titolare dei diritti di dati relativi agli utenti del primo alla stregua della vigente disciplina in materia di privacy nelle comunicazioni

elettroniche; la fattispecie sarebbe, peraltro, estranea all'ambito di operatività della deroga contenuta all'art. 24 codice privacy".

Paradossalmente, mentre i diritti economici d'autore possono contare su disposizioni normative tese a comprimere il diritto all'anonimato, la tutela dei diritti della personalità di fronte a illeciti compiuti da anonimi non ha una disciplina ad hoc.

Sul punto Giorgio Resta rileva quanto segue [Resta, 2019, 506]:

> "Il problema è che, non appena si abbandona il terreno della proprietà intellettuale, protetto da reti di filo spinato sempre più fitte ed estese e salvaguardato da vigilantes dotati di potenti mezzi tecnologici e ampie risorse finanziarie, il grado di effettività di tale assunto tende a scemare in misura preoccupante. Nel campo dei diritti della personalità, in particolare, l'assenza di strumenti normativi tanto incisivi quanto quelli previsti a tutela delle posizioni proprietarie sembra indurre le corti a un atteggiamento molto più remissivo e rispettoso dell'interesse all'anonimato, a discapito delle stesse esigenze di tutela giudiziaria dei diritti altrove solennemente declamate".

Parte 3 – Caso 2

> "Sul Blog CasoSpia della società «Bincolettismo» viene pubblicato un post anonimo palesemente lesivo della identità personale della nota influencer «Bruna Bronzagni»
> L'influencer agisce in sede civile per ottenere i dati identificativi dell'autore del post e per far dichiarare responsabile la società «Bincolettismo» per violazione all'identità personale
> Qual è il problema?
> Qual è la soluzione?
> Argomentare la soluzione".

Bibliografia

R. Caso, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Diritto dell'Internet*, 2008, pp. 466-472.

R. Caso, G. Pascuzzi, *Il diritto d'autore dell'era digitale*, in G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2020, 195-234.

G. Finocchiaro, *Anonimato*, in *Digesto delle discipline privatistiche*, Sez. civ., Agg., Torino, 2010.

F. Giovanella, *Enforcement del diritto d'autore nell'ambito di Internet vs. protezione dei dati personali: bilanciamento tra diritti fondamentali e contesto culturale*, in *Riv. critica dir. privato*, 2013.

G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2020.

G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. informazione e informatica*, 2014, 171.

G. Resta, in G. Alpa e G. Resta, *Le persone e la famiglia 1. Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile* diretto da R. Sacco, Utet, Torino, 2019, pp. 145-632.

E-mail:
roberto.caso@unitn.it
Web:
http://www5.unitn.it/People/it/Web/Persona/PER0000633#INFO
http://lawtech.jus.unitn.it/
https://www.robertocaso.it/