GIURISPRUDENZA PENALE

La responsabilità penale dell'internet provider

di ***Gaetano Stea***

CASSAZIONE PENALE, SEZIONE QUINTA, 1 MARZO 2016 (UD. 13 LUGLIO 2015), N. 8328
BRUNO *Presidente* – PEZZULLO *Relatore*

SOMMARIO: 1. Il caso. – 2. Cenni introduttivi sulle attività telematiche. – 3. La problematica della responsabilità dell'access e caching provider. – 4. La responsabilità penale dell'hosting provider. – 5. Gli obblighi dell'hosting provider.

1. Il caso

Il Giudice per l'udienza preliminare presso il Tribunale di Palermo condannava l'imputato alla pena di euro 1.500,00 di multa, con la diminuente del rito abbreviato, per il delitto di cui all'art. 595, co.1 e 3, c.p., per avere, offeso la reputazione del Commissario Straordinario della Croce Rossa Italiana, comunicando con più persone, mediante la pubblicazione sul suo profilo Facebook, di alcune frasi, associandole - in taluni casi - all'immagine del predetto.

2. Cenni introduttivi sulle attività telematiche

La principale caratteristica di Internet consiste nella possibilità di offrire svariati servizi tra cui spiccano in maniera determinante quelli di informazioni *online*. Tanto che, proprio con riferimento a tali tipi di servizi, si parla di Internet come mezzo di comunicazione alternativo o complementare ai *media* classici della stampa, della radio e della televisione. La peculiarità di simili informazioni risiede nell'essere rappresentate sotto forma digitale in formato standard e spesso di essere accessibili in maniera gratuita. Si può arrivare a sostenere che la stessa Rete non è altro che un'immensa banca dati, se si considera la possibilità di inserire nei documenti richiami (*hyperlink*) ad altri documenti presenti in Internet.
E' proprio questa vastità che fa sì che più alto è il valore aggiunto della sistemazione critica delle fonti informative, più è alta la probabilità che le informazioni siano facilmente accessibili da parte dell'utente, che le reperisce attraverso vari sistemi di ricerca interattivi che ne facilitano il reperimento (c.d. *browser*).
Si è soliti distinguere due diverse tipologie di attività telematiche, che possono essere automatizzate o meno: (1) quella relativa all'ingresso delle informazioni nella rete e, dunque, la condotta di accesso, e (2) quella che riguarda la loro permanenza e,

dunque, la condotta di memorizzazione[1]. Mediante tali attività possono essere perpetrati dei reati (salvo verificarne l'effettiva tipicità), come nell'ipotesi oggetto della pronuncia in commento, in cui la Suprema Corte ha scrutinato la condotta telematica di un soggetto che aveva "postato" dei messaggi diffamatori su una pagina del noto social network "*Facebook*".

3. La problematica della responsabilità dell'access e caching provider

La problematica più interessante, invero non affrontata nella decisione annotata, riguarda la la posizione dell'Internet Provider in relazione all'impedimento del reato telematico (*rectius*, per mezzo della telematica) da parte degli utenti.

Si tratta, in breve, di verificare se l'Internet Provider assume una posizione di controllo nell'ambito della telematica. A tal fine occorre definire le attività svolte dal *provider*, esaminando il decreto legislativo n.70 del 9.4.2003, avente ad oggetto *taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, nel cui ambito, con scelta alquanto discutibile, trovano collocazione le disposizioni sulla responsabilità dei *providers* (artt. 14-17). Tale normativa individua tre diverse attività svolte dai *providers*: semplice trasporto, memorizzazione temporanea e memorizzazione (duratura). Su quest'ultima si appunterà maggiore attenzione.

La prima attività è quella del semplice trasporto, che consiste *nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione*. L'art.14, co.2, d.lgs. 70/2003 definisce le attività di trasmissione e di fornitura di accesso, come quelle che *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*.

Si tratta, in pratica, del ruolo svolto dall'*access provider*. L'*access provider* è ritenuto irresponsabile per il contenuto delle informazioni trasmesse telematicamente, a tre condizioni (tutte *negative*): a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse. Lo *standard* di diligenza è minimo, atteso che non può essere imposto all' *access provider* di predisporre sistemi di prevenzione dell'illecito (quali, ad esempio, filtri, motori di ricerca, ecc.) e che lo stesso *provider* non è tenuto ad *invitare* gli utenti dei propri servizi a diffondere esclusivamente informazioni che non rechino danni a terzi. Leggendo *a contrario* l'art.14, co.3, d.lgs. 70/2003, si evince, inoltre, che l'*access provider* non è tenuto ad impedire o a porre fine alle violazioni perpetrate tramite il suo servizio, salvo che ciò gli sia imposto da un'autorità giudiziaria o amministrativa avente funzioni di vigilanza. Da ciò, non solo, l'*access provider* non può essere ritenuto responsabile del contenuto delle informazioni che transitano tramite il servizio offerto, se si limita ad un ruolo passivo (ossia di mera

[1] R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *Dir. Pen. Proc.*, 2013, 5, pp. 660 s.

intermediazione tecnica), ma poi non assume alcuna posizione di controllo.
La definizione normativa dell'attività di memorizzazione temporanea (cd. *caching*) consiste nella *memorizzazione automatica, intermedia e temporanea delle informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta*. Il prestatore che esercita l'attività di *caching* (cd. *caching provider*) non è responsabile, a condizione che: 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) 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. La previsione legislativa, facendo un costante rinvio a dati extragiuridici, realizza, indubbiamente, un fenomeno di eterointegrazione tra diritto e tecnica, parametrando, dunque, la diligenza del *caching provider* alle possibilità rese praticabili dagli sviluppi tecnologici. Rispetto alla diligenza nell'esercizio dell'attività di *access*, quella in esame è, certamente, qualificata dall'obbligo, da parte del prestatore intermediario, di attenersi alle *norme di aggiornamento del settore*. A tale *ratio* risponde anche l'inciso di cui alla lett. d) dell'art.15 d.lgs. 70/2003, laddove rimanda all'uso *lecito* della tecnologica *ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni*. L'aggettivo *lecito*, peraltro, sottolinea la necessità che il prestatore agisca secondo correttezza e senza interferire direttamente nella selezione delle informazioni, come, espressamente, imposto dalla lettera a) della norma in commento.
Interessante è quanto previsto dall'art.15, lett. e), D.lgs. 70/2003, che impone ai *providers* di rimuovere le informazioni memorizzate o di disabilitarne l'accesso, almeno in tre distinte ipotesi:
a) quando le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete;
b) quando l'accesso alle informazioni è stato disabilitato;
c) quando un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.
Nulla quaestio in ordine all'ultima ipotesi: il *provider* agisce solo dopo aver ricevuto un ordine da parte di un organo giurisdizionale o amministrativo.
Difficile, invece, l'interpretazione delle altre due ipotesi.
Va osservato, prima d'ogni altro, che, in tali casi, il *provider* è a conoscenza dell'informazione illecita (o presunta tale) poiché ha consultato direttamente il sito *web* oppure perché è stato informato da terzi.
Il prestatore intermediario, dunque, dovrebbe disabilitare l'accesso *non appena*

venga effettivamente a conoscenza del fatto [...] che l'accesso alle informazioni è stato disabilitato. Parimenti, in base alla formulazione della norma, è possibile che si realizzi anche una seconda fattispecie: al prestatore può, infatti, essere imposto di *rimuovere le informazioni che ha memorizzato [...] non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete.* Avventurarsi nel tentare di comprendere giuridicamente una simile norma appare compito ingeneroso per l'interprete. Ad ogni modo, va ricordato che il *provider* deve, ai sensi dell'art. 15 d.lgs. 70/2003, agire *prontamente*. L'avverbio in questione, sebbene non indichi un arco temporale predefinito, sottolinea la necessità di arrestare, nel minor tempo possibile, gli effetti causati dall'informazione fonte di danno.

4. La responsabilità penale dell'hosting provider

Più problematica la posizione del *provider* che mette a disposizione dell'utente uno *spazio telematico* (tecnicamente si tratta di una porzione dell'*hard disk* del proprio computer): la scelta delle informazioni da fornire sarà però del soggetto che con il prestatore stipula il contratto di *hosting*.

L'*hosting provider*, dunque, non può rispondere degli eventuali illeciti commessi all'interno dei siti *ospitati*, in base a quanto previsto dall'art.16 d.lgs. 70/2003, qualora *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*» ovvero *non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*.

La disposizione sembra individuare due distinti livelli di conoscenza, distinguendo, da un lato, le ipotesi di illeciti penali, che interessano in questa sede, nel qual caso l'accusa sarà tenuta a dimostrare l'*effettiva* conoscenza da parte del *provider* della perpetrazione criminale e, dall'altro, gli illeciti civili, ove, invece, il danneggiato avrà l'onere di dimostrare fatti o circostanze *che rendono manifesta l'illiceità dell'attività o dell'informazione*.

Paiono, però, persistere alcuni elementi incerti: in primo luogo, la nozione di *effettiva conoscenza* utilizzata dal legislatore parrebbe rimandare all'espressione *actual knowlegde*, che ha un preciso significato nell'ambito della *copyright law* statunitense, ma che nel nostro ordinamento rimarca, esclusivamente, che non può trattarsi di *mera conoscibilità*: non sarà, quindi, sufficiente dimostrare che il *provider* avrebbe potuto conoscere (*conoscibilità*), essendo invece necessario che sia fornita la dimostrazione dell'effettiva conoscenza (*conoscenza*). Da ciò, sembrerebbe configurarsi in capo all'*hosting provider* un'ipotesi di responsabilità omissiva impropria, ai sensi dell'art.40, co.1 2, c.p., qualora, essendo a conoscenza dell'attività illecita già perpetrata, non impedisca la relativa diffusione telematica, con l'effetto che l'omissione rappresenta la partecipazione concorrente alla consumazione delittuosa. A tal fine, dunque, l'*hosting provider* dovrebbe avere la possibilità di intervenire, inibendo o rimuovendo il sito ospitato onde evitare che il

danno conseguente all'illecito si protragga anche in un momento successivo rispetto a quello in cui ha avuto conoscenza che il materiale illecito era *online*. Tuttavia, a prescindere da ogni considerazione sulla tipicità, non v'è chi non veda che l'obbligo di rimozione non può coincidere con l'obbligo di impedimento, in quanto logicamente il primo sorge allorquando il reato si è già consumato, mentre il secondo è posto proprio per prevenire la commissione di illeciti penali. L'inadempimento dell'obbligo di rimozione non integra dunque l'omissione impropria di cui all'art.40, co.1 2, c.p. Va esclusa qualsiasi responsabilità dell'*hosting provider* in caso di reato a consumazione istantanea, poiché l'effettiva conoscenza che innescherebbe l'obbligo posto a carico del *provider* sorge solo dopo la consumazione del fatto di reato.

Quale la responsabilità dell'*hosting provider* nell'ipotesi di attività criminale organizzata per la commissione di più reati ? Si pensi ad un sito *web* di vendite *online* ove si accerti la sistematica realizzazione di truffe ai danni di consumatori.

In tale ipotesi, l'*hosting provider*, essendo a conoscenza dell'attività illecita, perpetrata dal sito ospitato, potrebbe rispondere, a titolo di concorso omissivo in reato commissivo, nella consumazione degli illeciti realizzati successivamente al sorgere dell'obbligo di rimozione ?

Qui il potere di rimuovere significa la concreta possibilità di impedire l'illecito telematico. Tuttavia, a tale doverosa azione, la stessa norma pone due limiti importanti:

(1) l'*hosting provider* deve rimuovere il sito ospitato non appena a conoscenza dei fatti, ma solo su comunicazione delle autorità competenti. È evidente, pertanto, che la conoscenza *postuma* dell'illecito deve essere, non solo, effettiva, ma anche qualificata, nel senso che l'informazione deve provenire solo dalle autorità competenti (cd. *informativa pubblica*). Con tale qualificazione, dunque, il legislatore ha reso ininfluenti le informative *private*, con ciò delimitando eccessivamente l'ambito di operatività dell'obbligo di rimozione, che, invero, sarebbe potuto essere sottoposto anche alla sola *informativa privata non anonima*;

(2) è indispensabile poi la conoscenza effettiva dell'illiceità del fatto, nel senso che non appare sufficiente che l'autorità competente comunichi al gestore che l'attività *potrebbe* essere illecita, in quanto, ad esempio, sono state proposte diverse denunce da parte di presunte vittime dell'attività perpetrata da un sito ospitato, ma è necessaria la comunicazione dell'accertamento giudiziale (passato in giudicato) della certa illiceità dell'attività *de qua*, con l'effetto che, solo allora, sorgerà l'obbligo per l'*hosting provider* di rimuovere o disabilitare l'accesso al sito web. Tale lettura interpretativa pare avallata dalla previsione di cui all'art.17 D.lgs. 70/2003, che esamineremo più avanti, in cui è fatto riferimento alla *presunzione* di illiceità del fatto [2]. Da ciò, l'obbligo di rimozione così come delineato dall'art.16 d.lgs. 70/2003

[2] Appare evidente che la responsabilità dell'*hosting provider*, come sopra delineata, costituisce un'ipotesi delittuosa concorsuale certamente remota, poiché è impensabile che il gestore, messo a conoscenza dell'accertamento giudiziale dell'illiceità di un'attività telematica (continuativa) perpetrata tramite il suo servizio, non provveda alla rimozione della

non è utile a configurare, in capo all'*hosting provider*, una posizione di controllo sulle attività degli utenti [3], tanto ancor di più in base all'art.17, co.1 1, d.lgs. 70/2003 che, a chiusura della disciplina delle responsabilità dei *providers*, stabilisce che il prestatore intermediario non è tenuto a monitorare il contenuto delle informazioni trasmesse [4].

5. Gli obblighi dell'hosting provider

Non resta ora che esaminare proprio l'art.17, co. 2, D.lgs. 70/2003, che stabilisce che il *provider* è 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*.

L'obbligo di informazione (*rectius*, di denuncia), sulla base di quanto previsto dalla norma in commento (lett. *a*), sorge non appena il *provider* viene a conoscenza dell'illecito perpetrato tramite il suo servizio, sia ove ciò si realizzi con una *notification* da parte di un terzo, sia quando lo stesso prestatore, *navigando* sui propri siti, si imbatta in un'informazione ritenuta illecita.

Non è necessaria, infatti, la preventiva valutazione, da parte del *provider*, dell'effettiva illiceità dell'informazione, in quanto l'obbligo di denuncia è imposto anche laddove l'illecito sia solo *presunto*.

Da ciò, il *provider* ha l'obbligo di denuncia nell'ipotesi in cui, in qualsiasi modo, venga a conoscenza di un fatto che, presuntivamente, potrebbe integrare un illecito, onde consentire all'autorità competente di *individuare e prevenire attività illecite*, adottando le più opportune iniziative, anche d'urgenza.

La conoscenza dell'illiceità *presunta* di un'attività o informazione *online* impone,

---

stessa (se ancora esistente, dopo il *lungo* procedimento di verifica giudiziale e nell'*isolato* caso in cui la stessa autorità non abbia disposto la rimozione).

[3] A. MANNA, *Corso di diritto penale. Parte generale*, II Ed., Padova, 2012, p.246, afferma che è del tutto inaccettabile ravvisare un posizione di controllo dell'*internet provider*, al pari di quella dell'ufficiale o agente di polizia giudiziaria, poiché «solo a quest'ultimi, il codice di rito, all'art.55, configura l'obbligo giuridico di impedire la commissione di reati». Sul tema ampiamente con particolare riguardo al reato omissivo improprio colposo, A. MASSARO, *La responsabilità* colposa *per omesso impedimento di un fatto illecito altrui*, Napoli, 2013

[4] R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *Dir. Pen. e Processo*, 2013, 5, p. 603, condivisibilmente, afferma che «l'impossibilità di configurare una responsabilità dell'ISP per omesso impedimento *ex ante* del reato non è una questione soltanto tecnica (impossibilità di controllo o eccessiva dispendiosità di tale controllo), ma per l'appunto sostanziale, nel senso che il provider non ha alcuna relazione con la fonte del pericolo (con l'utente), né sono individuabili beni da proteggere particolarmente vulnerabili, così come non esistono in capo allo stesso veri e propri poteri giuridici di interferenza o inibizione rispetto alla condotta dell'autore del reato».

dunque, al gestore solo l'obbligo di denuncia, come previsto dall'art.17, co.1 2, lett. a), D.lgs. 70/2003, ma non fa sorgere, in capo allo stesso prestatore, l'obbligo di rimozione, stabilito dall'art.16, co.1 1, D.lgs. 70/2003, salva la richiesta cautelare dell'autorità competente, come visto, secondo parametri e condizioni *vincolate*.

L'obbligo generale di denuncia configura, pertanto, l'unica ipotesi di dovere di attivarsi, a carico del *provider*, senza indugio, nel caso di *presunta* attività illecita perpetrata da un sito ospitato [5], costituendo, pertanto, questione su cui appuntare l'attenzione esegetica.

L'obbligo *de quo* è finalizzato, evidentemente, al normale ed efficace funzionamento dell'attività istituzionale di repressione e prevenzione delle attività criminali, come suggerisce la previsione di cui all'art.17, co.1 2, lett. b), D.lgs. 70/2003.

Ma non è sufficiente a configurare una generale posizione di garanzia in capo al *provider,* in quanto tale obbligo di denuncia non implica un potere di impedire l'evento, nel senso che la tempestiva denuncia della presunta attività illecita (come imposta dall'art.17, co.1 2, lett. a), D.lgs. 70/2003) non può assurgere ad un vero e proprio potere del *provider* di interrompere l'azione criminale del terzo, ponendosi, piuttosto, come onere doveroso volto a non agevolare l'attività delittuosa.

Né varrebbe obiettare che la denuncia dell'attività presunta illecita, a cura del *provider*, è finalizzata all'esercizio dei poteri di repressione da parte dell'autorità competente e, dunque, costituisce un ipotesi (*mediata*) di obbligo di impedire l'evento di cui all'art.40, co.1 2, c.p.

L'obbligo di denuncia, di contro, ha una sua *ratio* [6], nel sistema penale, ben individuata dalle previsioni delittuose di cui agli artt.361 ss. c.p., che, dunque, lo distinguono dall'azione doverosa che configura la posizione di garanzia di cui all'art.40, co.1 2, c.p.

L'omessa denuncia, infatti, costituisce l'inadempimento di un obbligo di comunicazione, mentre, nell'ipotesi di inadempimento dell'obbligo di impedire l'evento, l'agente non omette la semplice notizia, ma omette il doveroso comportamento positivo (impedimento del reato) che poteva materialmente attuare e che invece non ha attuato, concorrendo così al compimento del reato stesso.

Tuttavia, pur volendo ammettere che l'obbligo di denuncia di cui all'art.17, co.1 2, lett. a), d.lgs. 70/2003 sia finalizzato all'impedimento (*mediato* ed *indiretto*) dell'evento, è indubbio che il gestore è sfornito di poteri di intervento, allo scopo di interrompere l'azione criminale e, dunque, impedire l'evento.

Per tali ragioni, la posizione del *provider* va inquadrata nell'alveo degli obblighi di sorveglianza, semmai, *temperata*, poiché la norma *de qua*, se da un lato esclude in capo allo stesso gestore il dovere di vigilare sulle attività degli utenti del servizio offerto, dall'altro, comunque, gli impone l'obbligo di denuncia senza indugio della presunta attività illecita, che sta a significare, evidentemente, una pretesa

[5] Tale obbligo ha carattere generale, nel senso che opera per tutti i soggetti della telematica

[6] I delitti di omessa denuncia, infatti, sono finalizzati a tutelare il normale funzionamento dell'amministrazione della giustizia

dell'ordinamento di attenzione nell'esercizio del servizio e, soprattutto, del relativo utilizzo da parte della collettività[7] . Ad ogni modo, tale posizione è assolutamente irrilevante dal punto di vista penalistico.

[7] Sul divieto posto dalla normativa europea di obbligare il prestatore di servizi di *hosting* ad una sorveglianza generalizzata sui contenuti da esso memorizzati, cfr. CGUE, Sez. III, causa C-360/10, 16 febbraio 2012, *SABAM c. Netlog NV*, che ha considerato contraria alla normativa comunitaria l'ingiunzione rivolta all'*hosting provider* di predisporre il sistema di filtraggio della maggior parte delle informazioni memorizzate sui suoi server, al fine di individuare file elettronici contenenti opere musicali, cinematografiche o audiovisive sulle quali si vantano dei diritti di *copyright* e, successivamente, di bloccarne lo scambio, perché un tale sistema di filtraggio implica una sorveglianza sulla totalità o sulla maggior parte delle informazioni memorizzate presso il prestatore di servizi di *hosting* in contrasto con quanto previsto, in particolare, dall'art. 3, § 1, Direttiva 2004/48, che richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose. Negli stessi termini, CGUE, Sez.III, causa C-70/10, 24 novembre 2011, *Scarlet Extended SA c. SABAM*