

Profili evolutivi della responsabilità in Rete: il ruolo degli *Internet Service Provider* tra prevenzione e repressione*

The Evolution of the Concept of Liability on the Internet: the Role of Internet Service Providers, between Prevention and Repression

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

Giuseppe Miceli*

Legal Advisor in Diritto commerciale e Diritto industriale, Università di Camerino

Abstract

Si analizzano ruolo e responsabilità degli attori dell'informazione digitale, nonché l'evoluzione che sta segnando il ruolo degli *ISP* e i profili di responsabilità ad essi imputabili nei confronti dei terzi lesi e danneggiati da condotte riferibili ai clienti utilizzatori del sistema, per loro tramite. Per scongiurare il rischio di una anarchia virtuale diffusa, con l'alibi di una – apparente – abdicazione dei rimedi giuridici, è avvertita l'esigenza di individuare ed applicare efficaci strumenti di prevenzione e repressione dei reati commessi mediante Internet e delle violazioni di diritti patrimoniali e personali.

Un intervento di tipo interpretativo – prima ancora che legislativo – risulterebbe risolutorio rispetto alla definizione dei profili di responsabilità sulle piattaforme digitali, sia in termini di prevenzione che di repressione delle condotte illecite. Facendo leva sulla teoria dei nuovi diritti, deve evidenziarsi che il diritto di accesso a Internet non è – ancora – un diritto meritevole di tutela costituzionale e, quindi, deve cedere di fronte al rischio che siano compromessi diritti fondamentali, quali: l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori.

The core of the research is based on the possible actions that should be taken to tackle fake news or hate speech and the most common types of illegal activities carried out on the web, along with the role and responsibilities of the suppliers of information. There is the need to seize one's attention on the evolution that is marking the role of Internet Service Providers (ISP) and the profiles of liability relating to third parties that could be harmed and damaged by customers' misbehaviors while using the Internet.

In order to avoid the risk of a widespread virtual anarchy, due to the alibi of an apparent abdication of legal remedies, it is necessary to identify and apply effective tools to prevent and prosecute the crimes committed on the Internet and the infringement of property and personal rights.

This research should consider the "principle requiring the legal issues linked to the Internet being regulated by applying the laws in force in similar fields and proper adjustments to the peculiarities, if needed".

This analysis is aimed at showing that an interpretative intervention rather than a legislative one can be a means to define profiles in compliance with the responsibilities of digital platforms, based on the prevention and repression of illegal conduct.

Sommario

1. Premessa. Analisi di contesto. - 2. *Internet Service Provider*: ruolo e funzioni. - 3. La funzione degli standard di diligenza. - 4. Profili evolutivi e prospettive di contrasto. - 5. La responsabilità per l'esercizio di attività pericolose ex art. 2050 c.c.

responsabilità del provider
Internet Service Provider
modello 231
direttiva e-commerce
ISP

1 Premessa. Analisi di contesto.

Non v'è dubbio che il peculiare e caratterizzante connotato di internet, quale moltiplicatore esponenziale di opportunità di comunicazione fra una moltitudine di utenti, abbia reso la Rete un eccezionale volano per la commissione e diffusione di illeciti la cui gamma risulta notevolmente ampliata, così come il numero degli autori¹.

La grande facilità di diffusione di messaggi, immagini e filmati, la potente capacità di divulgazione di ogni altro tipo di comunicazioni unite al carattere naturalmente ubiquo di internet complicano l'opera di regolamentazione giuridica e rendono estremamente difficile individuare i soggetti responsabili² delle azioni illecite commesse in questo *infinito non luogo*³. Tant'è che non sempre le più evolute tecnologie utilizzate per gestire una rete telematica consentono di identificare realmente l'utente che si sia reso autore di una violazione⁴.

La risonanza degli illeciti che vengono commessi attraverso internet e i preoccupanti effetti che ne scaturiscono rendono quanto mai urgente l'adozione di uno strumento capace di individuare i ruoli e differenziare le responsabilità di coloro che agiscono in Rete.

Gli studiosi del diritto sono impegnati nella ricerca di una formale tipizzazione delle diverse condotte che, a vario titolo, trovano configurazione in internet.

Anche tale ricerca dovrà tener conto del «principio secondo il quale le questioni giuridiche riguardanti internet devono essere regolate applicando il diritto vigente in settori analoghi, premessi, se necessari, gli opportuni adattamenti alle peculiarità della Rete»⁵.

Proprio su tale principio si basa la presente analisi con la quale si mira a dimostrare che un intervento di tipo interpretativo – prima ancora che legislativo – possa risultare risolutivo rispetto alla definizione dei profili di responsabilità sulle piattaforme digitali, sia in termini di prevenzione che di repressione delle condotte illecite.

Al centro di questa riflessione sulle possibili azioni di contrasto alle più diffuse tipologie di attività illecite realizzate sul web, nonché, sul ruolo e le responsabilità degli attori dell'informazione digitale, si pone l'attenzione verso l'evoluzione che sta segnando il ruolo degli *Internet Service Provider* (ISP)⁶ e i profili di responsabilità ad essi imputabili nei confronti dei terzi lesi e danneggiati da condotte riferibili ai clienti utilizzatori del sistema, per loro tramite⁷.

Periodicamente – per lo più, in concomitanza con le tragiche conseguenze che scaturiscono dalla pubblicazione e diffusione *online* di video privati, come nei casi di *revenge porn* o di *cyberbullismo* – si riaccende il dibattito sull'opportunità di attribuire una responsabilità oggettiva in capo all'ISP. In tale scenario, al fine di scongiurare il rischio di una *anarchia virtuale* diffusa, con l'alibi di una

¹ Si tratta dei “reati di massa”. C.E. Paliero, *Minima non curat praetor. Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Padova, 1985, 181 ss.

² Affermazione mutuata da T. Ballarino, *Internet nel mondo della legge*, Padova, 1998, nonché, A. Sirotti Gaudenzi, *Trattato breve di diritto della rete*, Rimini, 2001. Si tratta di una convinzione su cui saranno basate le considerazioni conclusive e le proposte risolutive sul tema della responsabilità degli ISP.

³ Non si ritiene di poter condividere il pensiero di quanti identificano il fenomeno Internet come un “ambiente”, ovvero, un luogo fisico, tanto da definirlo con l'espressione, di matrice fantascientifica, cd *cyberspace*. Parte, autorevole, della dottrina (C. Giurandella, *Problemi di giurisdizione*, in Aa. Vv., *Internet. Nuovi problemi e questioni controverse*, Milano, 2001, 373 ss.) come pure alcuni pronunciamenti giurisprudenziali nazionali (ad es.: Trib. Firenze, 7 giugno 2001, n. 3155, consultabile in *Interlex*) in effetti, fanno riferimento a quella espressione che fu utilizzata per la prima volta da W. Gibson, nel suo *Neuromancer*, New York, 1984 descrivendo la Rete come un “nuovo ordinamento” caratterizzato da proprie peculiarità.

Si ritiene, piuttosto, di condividere il pensiero che nel 1996, J. Perry Barlow ha espresso nella sua *Dichiarazione di indipendenza del Cyberspazio* ovvero: «Il Cyberspazio è fatto di transazioni, di relazioni e di pensiero puro disposti come un'onda permanente nella ragnatela delle nostre comunicazioni. Il nostro è un mondo che si trova contemporaneamente dappertutto e da nessuna parte, ma non è dove vivono i nostri corpi».

⁴ L'accesso alla Rete avviene mediante una procedura di login, con un nome di accesso, o username e una password. Tecnicamente, salvo i casi di navigazione segreta in Internet - il cd *dark web* - è sempre possibile identificare il nome d'accesso dell'utente che ha commesso la violazione attraverso quello che viene chiamato il log file, contenente l'identificazione dell'utente che ha effettuato il login e i tempi di accesso di ogni utente, tuttavia nulla vieta che tale nome possa essere stato in precedenza sottratto, insieme alla sua password ed utilizzato fraudolentemente da terzi al fine di evitare ogni possibile conseguenza. La stessa difficoltà di individuazione si ha quando uno stesso nome di accesso alla rete è utilizzato da più persone contemporaneamente. Analogo discorso vale per indirizzo numerico IP che viene assegnato ai computer e a tutti gli altri dispositivi connessi a Internet per identificarli e consentirgli di interagire l'uno con l'altro, rappresentando una vera e propria impronta digitale del dispositivo utilizzato.

⁵ Così A. Gili, *Abuso del diritto di cronaca e diffamazione online*, disponibile online.

⁶ In informatica e telecomunicazioni un *Internet Service Provider* (ISP), termine mutuato dalla lingua inglese, letteralmente “fornitore di servizi Internet”, è una struttura di natura imprenditoriale e che offre agli utenti, dietro la stipulazione di un contratto commerciale di fornitura, servizi inerenti a Internet. L'ISP è assegnatario di indirizzi IP e fornisce il collegamento con la rete telematica, direttamente o tramite un provider collocato ad un livello più alto. È rilevante rappresentare che già da alcuni anni i costi del servizio di connessione sono tendenti allo zero, tanto che ai provider risulta molto più proficuo offrire sul mercato l'utilizzo di pagine web pubblicitarie e di promozione commerciale (i cd. *banner*) registrando, così, interessanti livelli di introiti economici.

⁷ Altri ordinamenti hanno definito i profili di responsabilità degli ISP, tra questi: la Germania, che per prima si è dotata di un sistema fondato sulla Legge Federale del 2 luglio 1997; Gran Bretagna, che prevede la responsabilità degli ISP nei casi di diffamazione in Rete. Sul piano giurisprudenziale, si segnala che in Olanda un ISP è stato condannato per essere stato responsabile della violazione per negligenza, non avendo impedito il comportamento illecito di suoi utenti che avevano violato la normativa sul copyright (Trib. Rotterdam, 1995). In Francia con sentenza del 10 febbraio 1999, la Corte d'Appello di Parigi ha ritenuto configurata la responsabile extracontrattuale dell'ISP per il contenuto illecito presente in siti “ospitati”. La sentenza dell'8 dicembre 1999 del Trib. Nanterre attribuisce responsabilità all'ISP in considerazione di un obbligo di prudenza e diligenza che grava in capo ai *Provider*. In Italia: Ordinanza Trib. Napoli, 8 agosto 1996; Trib. Catania, 25-29 giugno 2004, n. 2286; Trib. Milano, ord. 24 marzo 2011 e, ancora, sent. 9 settembre 2011, n. 10893. Ancora, una serie di pronunce della Corte di giustizia dell'Unione europea e – come se non bastasse – significative sono le Conclusioni del 26 novembre 2013, causa C-314/12, dell'Avvocato Generale.

– apparente – abdicazione dei rimedi giuridici, è avvertita l'esigenza di individuare ed applicare efficaci strumenti di prevenzione e repressione dei reati commessi mediante internet e delle violazioni di diritti patrimoniali e personali.

2 Internet Service Provider: ruolo e funzioni.

Volendo incentrare l'attenzione sul dibattito circa l'opportunità di attribuire una responsabilità oggettiva in capo all'ISP nell'ambito di quella che è già stata definita la ricerca di una formale tipizzazione delle diverse condotte che, a vario titolo, trovano configurazione in internet, giova il riferimento alla distinzione operata dalla direttiva n. 2000/31/CE sul commercio elettronico, in ragione della capacità degli stessi ISP di immagazzinare, modificare e trasmettere una, più o meno, ampia mole di informazioni, anche in via permanente, nelle piattaforme informatiche e di garantire un'agevole condivisione di tali dati tra gli utenti⁸.

Il legislatore nazionale, con la legge delega 1 marzo 2002, n. 39 e il d. lgs. 9 aprile 2003, n. 70, ha dato attuazione alla direttiva 2000/31/CE sul commercio elettronico, iniziando l'opera di armonizzazione del regime di responsabilità civile dei cd prestatori intermediari, i *provider*, nei confronti dei terzi⁹.

In altre parole, il legislatore italiano, al pari di quello comunitario, applica il principio della distinzione dei *provider*, a seconda che questi svolgano funzioni di "semplice trasporto" (*mere conduit*), di "memorizzazione temporanea" (*cached*) e di "hosting".

A ben vedere, il d. lgs. 70/2003, si limita a riprodurre la direttiva 2000/31/CE, travasandone il contenuto nel nostro ordinamento giuridico. Nelle tre disposizioni (artt. 14, 15 e 16) corrispondenti a diversi menzionati profili di *provider*, emerge soltanto che i fornitori di servizi non sono responsabili dei contenuti per loro tramite veicolati purché non intervengano su di essi, confermando una *ratio iuris* già presente nel nostro impianto normativo.

La direttiva, inoltre, agli artt. 12, comma 3, 13, comma 2, e 14, comma 3, con riguardo alle tre diverse attività di *provider* lascia aperta la possibilità per gli Stati membri di disporre che un organo giurisdizionale o un'autorità amministrativa ordini al prestatore di porre fine alla violazione e con riguardo alla sola attività di *hosting*, nella seconda parte dell'art. 14, comma 3, prevede la possibilità in sede di recepimento di «definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

L'assetto normativo sin qui analizzato deve essere letto con il dettato dell'art. 17, il quale esclude che il *provider* possa essere assoggettato a un generale obbligo di sorveglianza sulle informazioni che trasmette o memorizza, ovvero ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Tuttavia, la direttiva, all'art. 15, comma 2, prevede che gli Stati membri possano «stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati»¹⁰.

Gli Stati membri hanno facoltà di prescrivere *standard* di diligenza a carico degli intermediari *online*, idonei a individuare in via preventiva i contenuti lesivi, ma senza che questi vadano a costituire un vero e proprio dovere di ricercarli attivamente.

Parafrasando quanto acutamente osserva Oreste Pollicino¹¹, è necessario distinguere in maniera adeguata il piano della responsabilità del *provider* fondata sull'esercizio, da parte dello stesso, di un'attività editoriale che lo escluderebbe dalle esenzioni di responsabilità e quello della responsabilità che scaturisce dall'inerzia del *provider* quando ricorrano le condizioni per le quali l'art. 16 del d. lgs. 70/2003 sarebbe doveroso un intervento dello stesso volto alla rimozione dei contenuti.

⁸ Gli ISP dispongono di propri *data center* e di proprie apparecchiature che consentono l'interfacciamento con la rete Internet; tuttavia, vi sono anche alcuni ISP virtuali capaci di offrire abbonamenti ai loro servizi senza possedere un'infrastruttura di Rete propria, si servono, cioè, di un altro provider cosiddetto *wholesale*, fornitore di servizi per rivenditori.

⁹ La direttiva sul commercio elettronico è applicata ai settori *online*, come i servizi di informazione (giornali, riviste); pubblicità; commercio; servizi professionali (avvocati e medici); servizi finanziari e di accesso alla Rete. Non viene applicata a settori come quello tributario, ai servizi sulla privacy della società dell'informazione; attività di notai o figure professionali equivalenti che esercitano pubblici poteri e i giochi d'azzardo (inclusi lotteria e scommesse).

¹⁰ A ciò si deve aggiungere quanto previsto dal Considerando 48, ovvero, la possibilità per gli Stati membri «di chiedere ai prestatori di servizi, che detengono informazioni fornite dai destinatari del loro servizio, di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire taluni tipi di attività illecite». Il Considerando 48 costituisce il fondamento di un'obbligazione di mezzi e non di risultato. G. M. Riccio, *La responsabilità civile degli internet providers*, Torino, 2002, 213.

¹¹ O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *ConsultaOnline*, 2014.

Tuttavia, anche nel primo caso, per effetto di un eventuale accertamento della natura di *hosting* non passivo, ovvero non neutro, bensì di un ruolo “attivo”, si giustificherebbe l’addebito di responsabilità, proprio per non essere il *provider* del tutto estraneo alla gestione dei contenuti¹².

Ecco quindi che l’elemento significativo ai fini della configurazione di una responsabilità del *provider* è rappresentato dalla sua neutralità ma – risiede proprio qui il problema, visto che - in mancanza di un intervento legislativo chiarificatore, sarà il giudice a doversi fare carico di individuare il confine tra *hosting* attivo e *hosting* passivo¹³.

Si è giunti così, a compiere talora una forzatura del dato legislativo per coniare una nuova figura per così dire “ibrida”, diversa dal mero *provider* passivo, l’*hosting* cosiddetto attivo, concepito come un *provider* non neutrale nella prestazione di servizi, così da attrarne la responsabilità in concorso con gli autori degli illeciti di volta in volta contestati.

Tale circostanza, in effetti, non manca di generare profili altamente problematici proprio per l’elevato rischio di abuso connesso alla variegata platea di fruitori dei servizi offerti dagli stessi ISP.

A dirimere la questione risulterebbe utile la corretta individuazione e puntuale applicazione dei *cd standard* di diligenza previsti dalla direttiva sul commercio elettronico.

3 La funzione degli standard di diligenza.

In effetti, rispetto alla prevista facoltà riconosciuta agli Stati membri di prescrivere *standard* di diligenza a carico degli intermediari *online*, capaci di individuare in via preventiva i contenuti lesivi, ma senza che questi vadano a costituire un vero e proprio dovere di ricercarli attivamente, si ritiene auspicabile un caso particolare di messa in sicurezza delle Reti che può ravvisarsi nell’azione di stimolo per l’adozione “spontanea” da parte degli ISP di “programmi di collaborazione” e, ove non bastasse, l’onere di applicare il Modello organizzativo previsto dal d. lgs. 231/2001¹⁴.

Come è noto, proprio in ragione della continua evoluzione degli ordinamenti giuridici, emerge, sia a livello nazionale che internazionale, una chiara apertura verso alternative forme di regolamentazione, complementari alla classica elaborazione dottrinale del “diritto”¹⁵.

Tali forme alternative di elaborazione del diritto trovano configurazione nel cosiddetto *soft law*¹⁶ che rappresenta quell’insieme di tecniche e strumenti di produzione normativa idonee a gestire e dirigere le attuali vicende statali, internazionali e comunitarie. In altre parole, tale forma di diritto è una manifestazione di *ius publicum*, quale diritto prodotto, o quanto meno indirizzato, orientato e controllato da parte delle istituzioni pubbliche dei differenti ordinamenti, anche laddove gli attori protagonisti della concreta ed effettiva elaborazione regolamentare siano soggetti di natura chiaramente privata.

Il *soft law* potrebbe trovare valida applicazione anche per ciò che attiene la corretta definizione dei profili di responsabilità degli *internet Service Provider*, per colmare l’evidenziata lacuna con l’emanazione di un Codice di regolamentazione dell’attività dei *provider* relativamente ai profili di responsabilità che ne possono scaturire.

Nel caso in cui non dovesse registrarsi una spontanea adesione a tale soluzione, si potrebbe efficacemente ricorrere ad una più incisiva richiesta di assunzione di responsabilità da parte dei *provider*, assoggettandoli all’onere di adottare ed efficacemente attuare il «Modello di organizzazione, gestione e controllo» previsto dal d. lgs. 231/2001 sulla responsabilità amministrativa degli enti.¹⁷ Ciò che si propone, dunque, è “vincolare” il regime autorizzatorio dei *provider* all’onere di redigere ed

¹² Come si evince da G. Cassano - A. Contaldo, *La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza*, in *Corriere giuridico*, 9/2009, 1210, «Un orientamento riconosce la responsabilità del provider per l’illecito commesso anche da colui che si serva di strumenti forniti dal prestatore, richiamando l’equiparazione tra provider e direttore di giornale, o sottolineando la portata di Internet e quindi la strumentalità del sito del provider nel consolidare l’illecito, con la conseguente copertura da parte del provider riguardo l’anonimato dell’utente. Un altro orientamento nega che il provider possa essere responsabile per il semplice fatto di offrire l’accesso alla rete o lo spazio sul proprio server, dubitando dell’assimilabilità del sito internet alla testata giornalistica (Trib. di Cuneo, sez. I civ., sentenza 23 giugno 1997; Trib. Roma, sez. I civ., 4 luglio 1998, ord.)».

¹³ A tal proposito, un esame delle più importanti decisioni in tema di responsabilità degli ISP - soprattutto nell’ambito di asserite violazioni del diritto d’autore, della *privacy* o di altri beni giuridicamente tutelati (l’onore e la reputazione, per esempio, nei casi di diffamazione *online*) - documenta come i giudici abbiano spesso faticato a qualificare il ruolo effettivamente esercitato dai *provider* di volta in volta interessati entro i limiti normativi che sono configurati dagli artt. 14, 15 e 16 del d. lgs. 70/2003.

¹⁴ Decreto legislativo 8 giugno 2001, n. 231 “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’articolo 11 della legge 29 settembre 2000, n. 300”.

¹⁵ La stessa direttiva 2000/31/CE demanda all’importanza di una autoregolamentazione.

¹⁶ Il primo a teorizzare il concetto di *soft law* (ovvero, in Italia diritto attenuato e in Francia *droit mou*) agli inizi degli anni settanta, fu il Professor Dupuy; R.J. Dupuy, *Droit déclaratoire et droit programmatore: de la coutume sauvage à la soft law*, in *L’élaboration du droit international public*, Colloque de Toulouse, Société Française de Droit International, Paris, 1975, 132 ss.

¹⁷ Peraltro, il catalogo dei *cd reati* presupposto in materia di 231 comprende già «I delitti in materia di violazione del diritto d’autore» ex l. 99/2009.

attuare un documento che contenga le regole e le procedure organizzative dell'ente¹⁸ volte a prevenire la commissione dei reati specifici.¹⁹ Nemmeno, il d. lgs. 231/2001 sancisce l'obbligatorietà riguardo alla sua adozione²⁰, tuttavia, l'approvazione di un Modello idoneo a prevenire i reati costituisce causa di esclusione o limitazione della responsabilità dell'ente ai sensi del d. lgs. 231/2001²¹. Ecco quindi che tale strumento costituirebbe uno *standard* di diligenza i cui effetti avrebbero riverberato rispetto a quanto si dirà nel prosieguo di questa analisi a proposito dell'auspicata applicazione del regime di responsabilità oggettiva (ex art. 2050 c.c.) e della conseguente inversione dell'onere della prova.

Ciò significa – volendo anticipare l'evidenza dell'effetto – che l'ISP sul quale graverebbe la responsabilità oggettiva per il danno causato suo tramite, sarebbe responsabile «se non prova di avere adottato tutte le misure idonee a evitare il danno» e – al contrario - sarebbe esente da responsabilità ove dimostrasse di avere adottato tutte le misure idonee a evitare il danno, ovvero, come testualmente recita l'art. 6 del d. lgs. 231/01, che «l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi».

4 Profili evolutivi e prospettive di contrasto.

Si deve evidenziare che prima dell'entrata in vigore del decreto legislativo che ha recepito la direttiva sul commercio elettronico, la responsabilità civile dell'*Internet Service Provider*, per gli atti pregiudizievoli compiuti dal proprio cliente, trovava fondamento e regola nell'art. 2043 c.c. che sancisce: «qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno». Si tratta della responsabilità extracontrattuale, ovvero, la situazione di soggezione alle conseguenze di una condotta umana illecita (attiva o omissiva) che abbia determinato in capo ad un terzo un danno ingiusto. Tuttavia, nel corso degli anni, la giurisprudenza che si è occupata di tali questioni non sembra aver assunto posizioni univoche. Secondo un iniziale orientamento giurisprudenziale, il *provider* non risultava tenuto ad accertare la liceità delle comunicazioni e dei messaggi che, per suo tramite, fossero stati trasmessi *on line*; vi sarebbe stata responsabilità solo nel caso in cui il medesimo avesse fornito, con dolo o colpa, un cosciente apporto causale, contribuendo così alla determinazione del danno, secondo quanto stabilito, in via generale, dall'art. 2043 c.c.²².

Tale orientamento escludeva, già, la presenza di un dovere di vigilanza che imponesse al *provider* di verificare la liceità delle informazioni circolanti *on line* per suo tramite²³.

In evidente antitesi, un successivo orientamento giurisprudenziale ha ritenuto dover constatare una responsabilità oggettiva del *provider* per l'illecito contenuto delle informazioni immesse in Rete "per conto terzi"²⁴.

¹⁸ Analogamente a quanto disposto dalla Regione Calabria che, con l. 60 del 4 dicembre 2012, ha reso obbligatoria l'adozione dei modelli di organizzazione, gestione e controllo ex d. lgs. 231/2001 per alcune categorie di enti.

¹⁹ Peraltro, la gran parte di tali illeciti è già prevista tra le fattispecie di reato rilevanti in base al d. lgs. 231/2001 e s.i.

²⁰ Nonostante ciò, si registrano i primi esempi di "vincolo", come nel caso della Regione Lombardia e la Regione Calabria.

²¹ Si tratta della circostanza esimente prevista dal d. lgs. 231/2001, art. 6 "Soggetti in posizione apicale e modelli di organizzazione dell'ente".

²² Prima dell'entrata in vigore del d. lgs. 9 aprile 2003, n. 70, la responsabilità civile dell' *internet service provider* per gli atti pregiudizievoli compiuti dal proprio cliente trovava fondamento e regola nell'art. 2043 c.c.: «qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno», prevede e disciplina la fattispecie della responsabilità extracontrattuale e, cioè, la situazione di soggezione alle conseguenze di una condotta umana (attiva o omissiva) illecita che abbia determinato in capo ad un terzo un danno ingiusto. Tuttavia, la giurisprudenza che si era occupata di tale questione aveva assunto posizioni contrapposte. Da un lato talune pronunce sostenevano che il *provider* non potesse reputarsi tenuto ad accertare la liceità delle comunicazioni e dei messaggi che, per suo tramite, venivano trasmessi *on line*. La sua responsabilità era pertanto ravvisabile solo laddove il medesimo avesse fornito, con dolo o colpa, un cosciente apporto causale, contribuendo così alla determinazione del danno, secondo quanto stabilito, in via generale, dall'art. 2043 c.c.

Tale orientamento escludeva, dunque, la presenza di un dovere di vigilanza che imponesse al *provider* di verificare la liceità delle informazioni circolanti *on line* per suo tramite. In antitesi si registrava un'opposta opinione, che ipotizzava una responsabilità oggettiva del *provider* per l'illecito contenuto delle informazioni immesse in rete "per conto terzi". Così: Trib. Napoli, 8 agosto 1997. Ad analoga conclusione giunge il Trib. Roma, 22 marzo 1999.

²³ Tale assetto, tuttavia, iniziava a lasciare il campo a un opposto orientamento giurisprudenziale che ammetteva la configurabilità di una responsabilità oggettiva del *provider* per l'illecito contenuto delle informazioni immesse in Rete "per conto terzi". L'entrata in vigore del d. lgs. 9 aprile 2003, n. 70, coerentemente con quanto stabilito dalla direttiva 2000/31/CE, sancisce la responsabilità del *provider* sulla base del tipo di attività concretamente svolta.

²⁴ Il proprietario di un "sito" Internet ha obblighi precisi di vigilanza sul compimento di atti di concorrenza sleale eventualmente perpetrati attraverso la pubblicazione di messaggi pubblicitari. La colposa o dolosa inottemperanza a questi obblighi comporta la sua corresponsabilità nell'illecito concorrenziale. Trib. Napoli, 8 agosto 1997, in *Diritto e giurisprudenza*, 1997, 472 ss. nota di Catalano

Il *provider* che effettua il collegamento in rete non è tenuto ad accertarsi del contenuto illecito delle comunicazioni e dei messaggi che vengono immessi in un sito: tuttavia, sussiste la sua responsabilità per colpa se il contenuto delle dette comunicazioni da trasmettere appaia all'evidenza illecito; in questo caso, il *provider*, dando corso al collegamento concorre nel fatto illecito in quanto dà un apporto causale alla commissione dello stesso. Nella specie, il *provider* ha concorso nell'illecito consistente in un atto di concorrenza sleale per non aver rilevato, secondo l'ordinaria diligenza, l'uso di un noto acronimo da parte di un soggetto non autorizzato. Trib. Roma, 22 marzo 1999, in *Diritto dell'informazione e dell'informatica*, 2000, 66 con nota di Sammarco; *Rivista del diritto commerciale*, 2/1999, 273 ss., con nota di Visconti.

Come puntualmente osservato, «tra i fattori che hanno contribuito allo sviluppo di internet nel nostro paese, va senz'altro considerata la presenza dei c.d. *Internet Service Provider* (ISP), la cui funzione consiste appunto nel fornire agli utilizzatori l'accesso alla Rete, essendo l'interfaccia fra l'utenza e il *Network Service Provider* (NSP), che si appoggiano a loro volta agli operatori di telecomunicazioni». Gli stessi citati autori rilevano, pure, che «l'attività dell'ISP presenta le caratteristiche di una vera e propria attività commerciale»²⁵.

Il legislatore nazionale non ha definito un apposito regime amministrativo per i *provider* su internet, per cui il regime autorizzatorio vigente per i fornitori di servizi in materia di telecomunicazioni costituisce anche il quadro normativo di regolamentazione delle comunicazioni di dati via internet, finendo per rendere l'ISP un mero «fornitore di servizi pubblici di telecomunicazioni»²⁶. Sul piano amministrativo, in virtù di tale quadro normativo, il rivenditore di servizi pubblici di telecomunicazioni (tra cui i *provider*), per poter attivare la fornitura dei servizi offerti, deve essere autorizzato dal Ministero dello Sviluppo Economico²⁷. Ne consegue che per effetto della normativa in questione si è giunti ad assicurare le basi per uno statuto giuridico di tale figura che, se esercitata professionalmente, attiene ad una vera e propria attività d'impresa.

Pertanto, se è vero - com'è vero - che l'ISP svolge un ruolo fondamentale per il funzionamento di internet, è altrettanto vero che tale attività non possa non tener conto di un continuo ed equo bilanciamento tra contrapposti diritti: da una parte il diritto di accesso a internet e dall'altra l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori. L'assenza di una previsione normativa, sia europea, sia nazionale, in relazione ad un obbligo di sorveglianza - non generale - in capo agli ISP, non ha impedito, nel tempo, pronunce giurisprudenziali circa uno specifico obbligo degli stessi²⁸.

Ecco perché, l'individuazione di una responsabilità in capo all'ISP e la scelta dell'*an* e del *quomodo* della responsabilità dell'ISP comportano attente e propedeutiche valutazioni per le delicate scelte di contrasto alla criminalità specifica che si potranno realizzare.

Forti del pensiero di Vittorio Frosini, condiviso anche da Aldo Loiodice, facendo leva sulla teoria dei nuovi diritti, deve evidenziarsi che il diritto di accesso a internet non è - ancora - un diritto meritevole di tutela costituzionale²⁹. Dai risultati della attenta analisi compiuta dagli autorevoli autori emerge che l'art. 2 Cost. è - certamente - interpretabile come norma aperta e, come tale, consente il riconoscimento di nuovi diritti fondamentali, rispetto a quelli specificamente individuati dalla Carta costituzionale. Tuttavia, Frosini e Loiodice, mentre affermano che la libertà informatica è desumibile anche dalla definizione di alcune altre libertà³⁰ ed è, quindi, meritevole di tutela costituzionale tanto da essere riconosciuta come nuovo diritto costituzionale; con altrettanta convinzione sostengono che lo stesso non possa dirsi per il diritto di accesso a internet che resta privo di altri riferimenti costituzionali.

²⁵ G. Cassano - A. Contaldo, *La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza*, cit.

²⁶ Secondo quanto già previsto nel d. lgs. 17 marzo 1995, n. 103 e nel d.P.R. 14 settembre 1995, n. 420, non essendovi un esplicito riferimento ai casi di fornitura di servizi telematici su Internet, l'ISP è considerato un mero “fornitore di servizi pubblici di telecomunicazioni”.

²⁷ Sempre ai sensi del d. lgs. 17 marzo 1995, n. 103 e del d.P.R. 14 settembre 1995, n. 425.

²⁸ Trib. Milano, ord. 21/25 gennaio 2011 e ord. 24 marzo 2011. Secondo il Tribunale, dal momento che «l'associazione tra il nome del ricorrente e le parole 'truffa' e 'truffatore' è opera del software messo a punto appositamente e adottato da Google per ottimizzare l'accesso alla sua banca dati operando con le modalità [...] volutamente individuate e prescelte per consentirne l'operatività allo scopo voluto [...] non può che conseguire la diretta addebitabilità alla società, a titolo di responsabilità extracontrattuale, degli eventuali effetti negativi che l'applicazione di tale sistema può determinare». Trib. Pinerolo, ord. 30 aprile 2012; Trib. Milano, ord. 25 marzo 2013. Precisa il giudice che «le associazioni, tuttora visibili su Autocomplete e Ricerche Correlate, ai nomi dei ricorrenti [...] dei termini setta e plagio di cui gli stessi si dolgono non costituiscono una frase di senso compiuto né una manifestazione di pensiero, né dunque 'quello che Google pensa', né un pensiero, né un pensiero attribuibile a Google, ma esclusivamente il risultato delle ricerche più popolari effettuate dagli utenti, ovvero la visualizzazione dei termini ricorrenti nelle pagine web incluse tra i risultati di ricerca di una determinata *query*, entrambi resi disponibili agli utenti come strumenti di aiuto alla ricerca»; in prospettiva comparata: Corte d'Appello di Parigi, 14 dicembre 2011. Cfr.: O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, cit. La responsabilità del *provider* si configurava alla stregua di una responsabilità soggettiva: colposa, quando il fornitore del servizio, consapevole della presenza sul sito di materiale sospetto, si astenga dall'accertarne l'illiceità e, al tempo stesso, dal rimuoverlo; dolosa, quando egli sia consapevole anche della antigiuridicità della condotta dell'utente e ometta di intervenire. I sopracitati orientamenti giurisprudenziali trovano ulteriore conferma anche in Trib. Torino, sez. I impresa, ord. 23 giugno 2015.

²⁹ Come ha osservato Vittorio Frosini, il cui pensiero è stato condiviso anche da Aldo Loiodice, l'art. 21 Cost. non statuisce - per esempio - un autonomo diritto di stampa o di accesso alla stampa, ma - soltanto - di stampa come *species del genus* “mezzo di diffusione”, funzionale all'unico diritto testualmente previsto e tutelato, ossia quello di manifestazione del pensiero. di trasmissione del pensiero *in certam personam*, qualunque sia la “forma” prescelta per tale trasmissione. Cfr.: V. Frosini, *L'orizzonte giuridico dell'Internet*, in *Diritto dell'informazione e dell'informatica*, 2002, 275 ss.; T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, in M. Pietrangelo (a cura di), *Il diritto di accesso ad Internet*, Napoli, 2011, 32 ss.; A. Valastro, *Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano*, *ivi*, 47 ss.; A. Loiodice, *Informazione e partecipazione nella società tecnologica*, Roma-Reggio Calabria, 1974. Sul fronte opposto, si deve, tuttavia, considerare che la Legge Stanca del 9 gennaio 2004, relativa alle disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici, riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione ed ai relativi servizi, compresi quelli che si articolano attraverso gli strumenti informatici e telematici. L'art. 1 della menzionata legge fonda il diritto di accesso ad Internet sul principio di eguaglianza *ex* art. 3 della Costituzione, qualificandolo come uno strumento di realizzazione dell'eguaglianza sostanziale dei cittadini. Ma si può obiettare che il mancato accesso alla rete di molti individui comporta l'esclusione dell'accesso ad Internet come diritto universale e consente, invece, di inquadralo come una libertà negativa, intesa come possibilità di utilizzare il mezzo informatico senza interferenze esterne.

³⁰ In particolare, la libertà di espressione, anche a mezzo Internet, consente diverse modalità e finalità di comunicazione, quindi, oltre agli artt. 15 e 21 Cost., si potrebbe fare richiamo agli artt. 19, 33, comma 1, e 34 Cost.

5 La responsabilità per l'esercizio di attività pericolose ex art. 2050 c.c.

Orbene, avendo così chiarito i termini oggetto di una inevitabile opera di bilanciamento dei contrapposti diritti in campo ed evidenziando che su un "piatto della bilancia" viene riposto il diritto di accesso, in ordine al quale gli ISP ne rivendicano il riconoscimento e la connessa tutela di rango costituzionale e, sullo stesso "piatto" si pone pure il diritto di iniziativa economica (questo sì, di rango costituzionale) mentre sull'altro "piatto della bilancia" la collettività – non solo degli utenti della Rete – ripongono una serie di diritti fondamentali, tutti degni di tutela costituzionale³¹, non resta che interpretare la normativa vigente e dimostrare l'applicabilità all'*Internet Service Provider* della responsabilità oggettiva ex art. 2050 c.c., fermo restando il dover garantire la «assenza dell'obbligo generale di sorveglianza» ex art. 17 del d. lgs. 70/2003.

In effetti, da una attenta lettura dell'art. 17 emerge, da un lato l'assenza di un generale obbligo di sorveglianza, dall'altro, una serie di adempimenti da parte del *provider* che consente la concretizzazione di un'attività di monitoraggio³².

Dato che l'art. 2050 c.c. fa riferimento, oltre che alle attività pericolose tipizzate, nel codice o in leggi speciali, a quelle che, per la loro attitudine a produrre un rischio, si considerano attività pericolose atipiche e considerato che la giurisprudenza è unanime nel definire le "attività pericolose" in modo piuttosto ampio, comprendendo nella definizione non solo le attività qualificate pericolose dagli artt. 46 ss. T.U.L.P.S. o da altre leggi speciali, ma più in generale anche quelle che comportano la rilevante possibilità del verificarsi del danno per la loro stessa natura e per le caratteristiche dei mezzi usati; si vuole sostenere che nel caso di specie, l'oggettiva pericolosità emerge da una potenzialità lesiva, rilevabile attraverso dati statistici, elementi tecnici e di comune esperienza, notevolmente superiore al normale³³.

Proprio in considerazione di tale specificità, si ritiene poter sostenere l'ipotesi di incardinare l'attività svolta dall'ISP, caratterizzata da un potenziale elevato livello di pericolosità, nella fattispecie prevista e disciplinata dall'art. 2050 c.c.³⁴.

Incardinare l'attività dell'ISP all'interno del *genus* delle attività pericolose significa prescrivere l'adozione di condizioni di massima sicurezza e di ogni accorgimento utile a prevenire l'evento dannoso che, in tal modo, lo qualifica come inevitabile e, quindi, non in rapporto causale con l'attività stessa. Come anticipato, si procederà – ancora una volta - in virtù del «principio secondo il quale le questioni giuridiche riguardanti Internet devono essere regolate applicando il diritto vigente in settori analoghi, premessi, se necessari, gli opportuni adattamenti alle peculiarità della Rete».

Ecco quindi che l'ipotesi prospettata trova analogia nel caso della navigazione aerea che, pur non essendo *ex se* attività pericolosa è ritenuta tale, per la sua natura e/o le caratteristiche dei mezzi adoperati, in relazione alle possibili conseguenze dannose che ne possono scaturire. In altre parole, vi è pericolosità ogni qual volta la navigazione aerea non rientri nella normalità delle condizioni previste dai piani di volo, dalle condizioni di sicurezza, dalle ordinarie condizioni atmosferiche, ovvero, nei casi in cui la stessa sia esercitata in condizioni di anormalità o di pericolo, con conseguente applicabilità della disposizione dell'art. 2050 c.c.

Ulteriore analogia è data dal trasporto marittimo, in cui le condizioni di pericolosità dipendono dalla natura del bene trasportato, materiale infiammabile o produttivo di gas esplosivi. In questo caso, a nessuno sfugge il riferimento alla natura del "bene trasportato" dal flusso telematico che denota un carattere di pericolosità nei casi in cui consista di dati falsi e calunniosi, video appartenenti alla

³¹ Basti pensare a diritti quali: l'onore, la reputazione, la sicurezza pubblica, la riservatezza, la proprietà intellettuale e la protezione dei minori, il diritto di espressione e il diritto di informazione. Si tratta di tutti quei diritti di rango costituzionale che rischiano di essere lesi o, quantomeno, minacciati da condotte illecite perpetrate in rete

³² Trib. Catania, sez. II civ., 29 giugno 2004, n. 2286.

³³ In tal senso: Cass. civ., sez. III, 6 aprile 2006, n. 8095, in *Responsabilità Civile*, 7/2006, 662 ss., con nota di Facci; Cass. civ., sez. I, 27 gennaio 2006, n. 1755; Cass. civ., sez. III, 21 ottobre 2005, n. 20359; Cass. civ., sez. III, 21 ottobre 2005, n. 20357; Cass. civ., sez. III, 27 maggio 2005, n. 11275; Cass. civ., sez. III, 15 ottobre 2004, n. 20334; Cass. civ., sez. III, 26 aprile 2004, n. 7916; Cass. pen., sez. IV, 27 maggio 2003, n. 34620; Cass. civ., sez. III, 10 febbraio 2003, n. 1954; Cass. civ., sez. III, 19 luglio 2002, n. 10551, in *Danno e Resp.*, 12/2002, 1214 ss., con nota di Agnino; Cass. civ., sez. III, 5 giugno 2002, n. 8148; Cass. civ., sez. III, 29 maggio 1998, n. 5341; Cass. civ., sez. III, 2 dicembre 1997, n. 12193, in *Danno e Responsabilità*, 6/1998, 567 ss., con nota di Laghezza; Cass. civ., sez. I, 9 dicembre 1996, n. 10951; Cass. civ., sez. III, 8 novembre 1996, n. 9743; Cass. civ., sez. III, 16 febbraio 1996, n. 1192, in *Diritto dei Trasporti*, 1998, 465 ss., con nota di La Torre; Cass. civ., sez. III, 1 aprile 1995, n. 3829; Cass. civ., sez. II, 21 dicembre 1992, n. 13530; Cass. civ., sez. III, 17 dicembre 1991, n. 13564; Cass. civ., sez. III, 27 luglio 1990, n. 7571; Cass. civ., sez. III, 29 maggio 1989, n. 2584; Cass. civ., sez. II, 12 dicembre 1988, n. 6739; Cass. civ., sez. III, 11 novembre 1987, n. 8304; Cass. civ., sez. III, 15 luglio 1987, n. 6241, in *Foro Italiano*, 1988, I, con nota di Caruso; Cass. civ., sez. III, 1 luglio 1987, n. 5764; Cass. civ., sez. III, 27 febbraio 1985, n. 1733; Cass. Civ., sez. III, 27 febbraio 1984, n. 1393; Cass. civ., sez. III, 23 febbraio 1983, n. 1394; Cass. civ., sez. III, 2 febbraio 1983, n. 908; Cass. civ., sez. III, 27 gennaio 1982, n. 542; App. Genova, sez. II, 8 maggio 2006; App. Bari, sez. III, 7 aprile 2006; Trib. Gallarate, 18 marzo 2005; Trib. Busto Arsizio, 1 febbraio 2005; App. Milano, 18 maggio 2001, in *Foro Padano*, 2002, I, 205 ss., con nota di Curti; Trib. Monza, 7 febbraio 2000; Trib. Pescara, 10 luglio 1999; Trib. Milano, 5 giugno 1995; Trib. Milano, 17 novembre 1994; App. Roma, 16 gennaio 1986; App. Milano, 17 marzo 1972.

³⁴ L'art. 2050, c.c. recita «Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno». Si veda: S. Sica, *Il commercio elettronico. Profili giuridici*, Torino, 2001.

sfera privata, informazioni tutelate da brevetto o, ancora, opere appartenenti al diritto d'autore. Anche il trasporto ferroviario, di per sé, non è catalogabile come attività pericolosa, ma lo diventa al verificarsi di circostanze che eccedano il normale rischio e che richiedano, quindi, l'adozione di cautele preventive³⁵.

Se quindi la Rete viene vista come una sorta di autostrada virtuale, ove le merci o i passeggeri sono le informazioni, ovvero i dati, possiamo affermare che ex art. 2050 c.c. il *provider* – al pari del vettore – abbia l'obbligo di adottare ogni possibile precauzione e cautela idonea ad evitare l'evento dannoso.

Stesso discorso vale anche nel caso in cui il servizio fornito dal *provider* sia utilizzato da terzi, in forma attiva, mediante il cosiddetto *uploading* e *downloading*. In questi casi caricare o scaricare contenuti digitali può essere paragonato, ad esempio, alle attività di carico e scarico merci che si svolgono in ambito portuale. È evidente che differente potrà essere la natura danno che ne potrà scaturire ma, altrettanto evidente è che, in ogni caso il bene giuridico protetto assume rilievo costituzionale³⁶ e che, per ciò, anche in tale contesto le Autorità portuali – dunque, analogamente, gli ISP – al fine di garantire la sicurezza delle operazioni, debbano adottare ogni idonea misura per evitare eventi pericolosi.

Gli esempi di attività alle quali si applica quanto disposto dall'art. 2050 c.c. sono numerosi³⁷ e sono conseguenza di provvedimenti giurisprudenziali³⁸.

Si ritiene che l'ISP nell'offrire i servizi di accesso alla Rete ed, in generale, di trasferimento di *file* multimediali svolga un'attività pericolosa rientrante nella vasta casistica che nel tempo la giurisprudenza consolidata ha individuato e per la quale si configura la responsabilità ai sensi dell'art. 2050.

Ove non bastasse, per dirimere eventuali divergenze interpretative circa la plausibilità di tale tesi, giova il parallelismo con le norme che disciplinano il trattamento dei dati personali contenute nel d. lgs. 30 giugno 2003, n. 196. In particolare, l'art. 15, comma 1, del menzionato Codice della privacy sancisce che: «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile»³⁹.

Parte della dottrina sostiene che il legislatore abbia inteso, così, qualificare il trattamento dei dati personali, *ipso iure*, in termini di attività pericolosa.⁴⁰ In effetti, è possibile considerare pericolosa l'attività di trattamento dei dati personali per sua natura, ovvero, «in relazione al rischio che essa presenta di ledere i diritti fondamentali dell'interessato»⁴¹, considerando le finalità della legge, consistenti «nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale». Ecco quindi che se il rischio tipico dell'attività di trattamento di dati personali è quello di ledere posizioni particolari e qualificate, dell'interessato, rischio che sussiste anche al di fuori dell'ipotesi di trattamento concernente dati sensibili, prende corpo il parallelismo con l'attività svolta dagli ISP⁴².

Il rinvio all'art. 2050 c.c. si dovrà collegare all'applicabilità del regime relativo alla prova liberatoria prevista in materia di attività pericolose.⁴³

In tal senso, l'estensione dell'applicabilità dell'art. 2050 c.c. all'attività degli ISP comporterebbe l'inversione dell'onere probatorio che opera solo in relazione alla prova dell'elemento soggettivo della colpevolezza; a quel punto, il preteso responsabile (ISP) dovrà dimostrare di avere adottato ogni cautela idonea ad evitare l'evento dannoso, mentre, permarrebbe sull'attore (danneggiato) l'onere

³⁵ Cfr. Cass. civ., sez. III, 1 aprile 1995, n. 3829.

³⁶ Nel caso di carico e scarico merci il bene giuridico che si intende tutelare è la salute e la vita dell'individuo mentre nel caso del carico e scarico di file o dati, il bene giuridico protetto è la dignità, la privacy, la reputazione, la proprietà intellettuale dell'individuo che potrà – anche in questi casi – essere vittima degli effetti di un'attività pericolosa.

³⁷ Ad esempio, anche nel caso della raccolta di gas in bombola, qualora non vengano effettuate corrette operazioni di bonifica, si configura a carico del distributore, ai sensi dell'art. 2050 c.c., la responsabilità per il danno causato dallo scoppio di una bombola consegnata ad un terzo. Così Cass. civ., sez. III, 13 gennaio 1981, n. 294.

³⁸ La giurisprudenza ha giudicato la fangoterapia come attività pericolosa in considerazione della «frequenza con cui verificano degli incidenti ai clienti che utilizzano impianti»: Trib. Perugia, 04 ottobre 1991; lo spettacolo di un gruppo di sbandieratori è considerato attività pericolosa (Cass. civ., sez. III, 2 dicembre 1997, n. 12193); anche l'attività di giostra (App. Cagliari, 26 febbraio 2000) di gestione dei parchi divertimento (Cass. civ., sez. III, 27 luglio 1990, n. 7571), l'attività di pastificazione, per i mezzi impiegati (Cass. civ., sez. III, 5 giugno 2002, n. 8148), l'insegnamento delle tecniche per il conseguimento del titolo di guida alpina (Trib. Verbania, 17 febbraio 1994, in *Rivista di diritto sportivo*, 1999, 545 ss., con nota di Lanotte) e l'attività di caccia, per la quale è obbligatoria l'assicurazione per responsabilità civile (l. 11 febbraio 1992, n. 157).

³⁹ L'art. 15 del Codice Privacy disciplina il risarcimento del danno che precedentemente era disciplinato da due distinte norme: il danno patrimoniale dall'art. 18, quello non patrimoniale dall'art. 29 comma 9.

⁴⁰ In tal senso: V. Zeno-Zencovich, *Commentario alla legge 31 dicembre 1996, n. 675*, Padova, 1997; P. Ziviz, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla l. 675/96*, in *Responsabilità civile*, 1997, 1300 ss.

⁴¹ *Ibidem*.

⁴² La disciplina di cui all'art. 2050 c.c. risulterebbe applicabile solo in caso di lesione di diritti fondamentali dell'interessato e non per eventuali altri pregiudizi che ricadrebbero, invece, sotto la disciplina dell'art. 2043 c.c.

⁴³ Condividendo tale soluzione, si giunge a considerare il regime della prova liberatoria ex art. 2050 c.c. sempre applicabile, anche quindi se il danno non sia collegato alla lesione di un diritto fondamentale. M. Granieri, *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento di dati personali*, in *Danno e responsabilità*, 3/1998, 222; G. Visintini, *Trattato breve della responsabilità civile*, Padova, 1999, 404. In questo senso anche Trib. Orvieto 23 novembre 2002, in *Diritto dell'informazione e dell'informatica*, 2/2003, 337 ss.

di provare il nesso causale tra condotta ed evento lesivo.

In virtù di tale linea interpretativa, l'ISP sarebbe sollevato da responsabilità nel caso in cui riuscisse a dimostrare la mancanza di colpa e di aver agito con prudenza, diligenza e perizia, ovvero, di aver applicato lo standard di diligenza che – come si sostiene in questa analisi – sarebbe rappresentato, ai sensi dell'art. 6 del d. lgs. 231/2001, dall'aver «adottato ed efficacemente attuato [...] modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi».

L'analisi e la valutazione - sin qui proposta - dei mezzi di prevenzione e repressione applicabili alle condotte illecite che si realizzano in Rete, dimostra che l'abdicazione dei rimedi giuridici è solo apparente e che – evidentemente - ove non trovasse riscontro l'iniziativa dei *Provider* volta all'autoregolamentazione, vi sarebbero già i presupposti per l'applicazione di una tutela che, in *extrema ratio*, potrebbe giungere a rivestire carattere penale. Ciò che si vuole rilevare è che - come ha autorevolmente dimostrato Antolisei - l'illecito civile costituisce il c.d. "delitto nano" che identifica una condotta illecita priva di una sanzione penale.⁴⁴

L'illecito civile e l'illecito penale sorgono, storicamente, per il conseguimento di distinti obiettivi: in relazione all'illecito civile, si evidenzia la volontà dell'ordinamento di assicurare – attraverso il perseguimento dell'illecito civile, stesso – la riparazione complessiva del danno subito da interessi privati; rispetto all'illecito penale vengono, invece, perseguite quelle violazioni dell'ordine generale di gravità tale da richiedere l'intervento statale per la punizione del colpevole.⁴⁵

Pur operando in settori differenti, ambito civile e ambito penale, i due istituti condividono la struttura tripartita⁴⁶ che li caratterizza: entrambi possono essere, infatti, ontologicamente scomposti in fatto materiale (od oggettivo: nel diritto penale, il c.d. fatto tipico), antigiuridicità⁴⁷ e colpevolezza⁴⁷.

Pertanto un intervento da parte del legislatore potrebbe spostare la competenza sul piano penale e l'accertamento dei profili di responsabilità degli ISP a favore del rito penale.

Si tratterebbe di attribuire rilievo penale alla fattispecie di illecito oggettivamente imputabile all'ISP che non abbia fornito la prova liberatoria rispetto all'autonoma ipotesi di reato colposo, strutturata in forma omissiva, che troverebbe così disciplina analoga a quella che l'art. 57, al direttore responsabile di stampa periodica.

⁴⁴ Come sostiene Antolisei «Il fallimento delle teorie che sono state enunciate per distinguere il torto penale da quello civile, induce a concludere che una diversità sostanziale non esiste. La distinzione è puramente estrinseca e legale: il reato è il torto sanzionato mediante la pena; l'illecito civile è quello che ha per conseguenza le sanzioni civili (risarcimento, restituzioni, ecc.). Insomma, è la natura della *sancito juris* quella che consente di stabilire se ci troviamo di fronte all'una o all'altra specie di torto. Ciò non significa che la distinzione dipenda esclusivamente dall'arbitrio del legislatore. La scelta della sanzione, infatti, non avviene per puro capriccio, ma in base al criterio che più sopra abbiamo enunciato: la pena, essendo una sanzione onerosa anche per la comunità sociale, non viene adottata, se non quando i reggitori dello Stato ritengono che non se ne possa fare a meno; mentre, come già osservato, rispetto al risarcimento del danno essa presenta i caratteri della personalità, della necessaria determinatezza del precetto e della riserva di legge». F. Antolisei, *Manuale di diritto penale. Parte generale*, Milano, 2000, 98.

⁴⁵ Parafrasando, R. Mazzon, *La Responsabilità Civile - Responsabilità oggettiva e semioggettiva*, Torino, 2012, 2.

⁴⁶ «La teoria tripartita succede storicamente alla teoria bipartita classica. Sviluppata in Germania all'inizio del secolo, fu recepita in Italia negli anni trenta (soprattutto ad opera di G. Delitalia). Essa distingue nel reato tre componenti fondamentali: il fatto tipico, l'antigiuridicità oggettiva e la colpevolezza»: così T. Padovani, *Diritto Penale*, Milano, 2006.

⁴⁷ «Modernamente si usa distinguere nell'analisi dell'atto illecito il fatto materiale, l'antigiuridicità e la colpevolezza...»: *Ibidem*.