COMMISSIONE PARLAMENTARE DI INCHIESTA SUI FENOMENI DELLA CONTRAFFAZIONE, DELLA PIRATERIA IN CAMPO COMMERCIALE E DEL COMMERCIO ABUSIVO

RESOCONTO STENOGRAFICO

44.

SEDUTA DI GIOVEDÌ 18 FEBBRAIO 2016

PRESIDENZA DEL PRESIDENTE **MARIO CATANIA**

INDICE

PRESIDENZA DEL PRESIDENTE MARIO CATANIA

La seduta comincia alle 14.45.

(La Commissione approva il processo verbale della seduta precedente).

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso impianti audiovisivi a circuito chiuso.

(Così rimane stabilito).

Audizioni in materia di contrasto della contraffazione via *web* e in sede internazionale.

Audizione dell'avvocato Andrea Caristi e del professor Ferdinando Ofria.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'approfondimento tematico in materia di contrasto della contraffazione via web e in sede internazionale, l'audizione dell'avvocato Andrea Caristi e del professor Ferdinando Ofria, consulenti della Commissione.

Do la parola al professor Ofria.

FERDINANDO OFRIA. Ringrazio il presidente Catania. Sono un economista e da diversi anni mi interesso del problema della contraffazione come un fallimento di mercato. In particolare, si intende come fallimento di mercato qualcosa che non garantisce la parità dei punti di partenza oppure la concorrenzialità.

Nella fattispecie del bene contraffatto, si tratta di un fallimento di mercato perché, come molti sanno, esso genera un fenomeno distorsivo in riferimento alle imprese, dal momento che quelle sane e corrette si trovano ad avere di fronte una concorrenza sleale, e pone un problema grave anche per lo Stato poiché si ha una sottrazione di gettito fiscale, oltre al fatto che si utilizza personale a volte minorile o in nero.

L'elemento fondamentale del fenomeno sta nel fatto che il bene contraffatto proviene da un'attività della criminalità organizzata o in senso lato delle mafie, che utilizzano la contraffazione perché è un'attività imprenditoriale come tante altre, dalla quale ottengono molto profitto, con un rischio minimo rispetto ad altri settori, come le droghe e quant'altro.

Un'altra caratteristica della contraffazione, come della prostituzione e del contrabbando, è quella di offrire prestazioni a persone consenzienti. A differenza di altre realtà, in cui la criminalità utilizza l'intimidazione o l'attentato, in questo caso ottiene un consenso – questo è il punto centrale della mia nota – da parte di chi acquista i beni, quando ne è consapevole.

L'attività della contraffazione fa parte di una criminalità non solo locale, ma anche internazionale. Vorrei soffermarmi su questo aspetto. Per esempio, dalle indagini si evidenzia che il profumo *Chanel n. 5* è prodotto a Napoli da personale nordafricano, ma le boccette vengono prodotte in Olanda, le etichette in Spagna, mentre le essenze arrivano dal Messico. Considerando tutto insieme, c'è una rete a livello internazionale della criminalità. La

contraffazione, quindi, non è da sottovalutare dal punto di vista criminale. Oltretutto, i suoi proventi vengono riciclati in altre attività, per cui alimentano ancora di più la criminalità.

Le aggressioni al fenomeno sono state ben evidenziate. La proposta Catania, per esempio, inasprisce le pene, cosa che diventa fondamentale dal lato dell'offerta. Tuttavia, sul versante della domanda l'intervento è nei riguardi dei consumatori.

In particolare, ci sono stati due studi sul tema. Uno è stato quello della Direzione generale per la lotta alla contraffazione, che ha commissionato un lavoro a un'associazione di consumatori per vedere per quale motivo i consumatori acquistano questi beni.

Nello specifico, si evidenzia che il 90 per cento dei consumatori sa che è un reato, perciò vi è una consapevolezza da parte del campione considerato; il 70 per cento non si sente in colpa; il minor prezzo diventa l'elemento base per la domanda; il 96 per cento è consapevole che il bene è dannoso; il 15 per cento del campione acquista, comunque, questi beni. Questa è l'analisi effettuata.

Tuttavia, questo studio non considera un altro elemento che, invece, emerge in altre ricerche condotte dall'università di Messina (non ultima quella del 2010), in cui si valuta anche l'ipotesi di verificare se questo tipo di bene sia di tipo inferiore.

Spiego meglio cosa si intende per « bene inferiore » in termini microeconomici. Si definisce « inferiore » un bene la cui domanda, al crescere del reddito, si riduce invece di aumentare. Faccio l'esempio più semplice. Nel dopoguerra i contadini acquistavano i legumi, ma non la carne perché non avevano il reddito necessario; poi, crescendo il reddito, paradossalmente, invece di aumentare, la domanda di legumi si riduce.

Allora, per analogia possiamo riflettere su questo punto e domandarci se al crescere del reddito del consumatore la domanda del bene contraffatto si riduce e si sostituisce con quella del bene originale oppure no. Questo è il punto fondamentale perché, se dovesse essere così, ci sono degli elementi su cui ragionare.

Uno studio fatto a Messina – non di tipo econometrico o altamente statistico perché è stato eseguito da sociologi che hanno utilizzato il metodo delle analisi di gruppo, ovvero degli attori privilegiati – ha evidenziato l'esistenza di una correlazione forte tra il reddito e la domanda di questi beni; quindi, paradossalmente, al crescere del reddito la domanda si riduce.

Questo significa che c'è un elemento di debolezza nella « cultura » del cittadino che preferisce questo tipo di bene: mostrare ad altri un certo bene diventa un elemento di *status* sociale e di apparenza. Bisogna, dunque, approfondire quali sono gli stimoli che spingono gli individui a guardare la forma e non la sostanza, talvolta anche a discapito della salute perché spesso, come abbiamo detto, questi beni sono dannosi per la salute.

Questo è – ripeto – l'elemento fondamentale. In futuro, se si dovesse fare una ricerca più generale e nazionale sul caso, si potrebbe verificare fino a che punto questo fenomeno condizioni i singoli individui che preferiscono e domandano questo tipo di bene.

A ogni modo, l'apparire e lo *status* sono un elemento di debolezza, non certo di sviluppo o qualità culturale, bensì di frivolezza (volendo usare questo termine). Se dovesse essere questa la motivazione forte, come è apparso dallo studio fatto a Messina e da altri tentativi indiretti, a questo punto le politiche di contrasto dal lato della domanda dovrebbero essere volte ad aggredire questo fenomeno con un'informazione forte nelle scuole e mediante i *media*, ma anche con un investimento di lungo periodo, cioè con una campagna di sensibilizzazione per le giovani generazioni.

Gli accordi di partenariato 2014-2020 – per intenderci i finanziamenti previsti per le aree deboli a sviluppo e coesione, come quella del Mezzogiorno – prevedono notevoli strumenti per l'inclusione sociale e per la crescita del capitale umano, per cui penso che in questi anni bisognerà atten-

zionare e analizzare questi fenomeni. Infatti, è giusto che il contrasto avvenga dal lato dell'offerta, inasprendo le pene, ma deve avvenire anche da quello della domanda, creando una coscienza sul tema. Grazie.

PRESIDENTE. Ringrazio il professor Ofria. Ascoltiamo ora l'avvocato Caristi, poi faremo eventualmente delle repliche.

ANDREA CARISTI. Grazie, presidente. Buonasera ai signori commissari. Nel mio intervento ho cercato di focalizzare, da un punto di vista anche pratico, in base all'esperienza professionale, gli ostacoli che si incontrano con riferimento specifico all'ambito contraffattivo o di contrasto della pirateria, ma in generale agli illeciti perpetrati a mezzo di internet.

Il primo nodo problematico che è stato posto alla vostra attenzione è quello di una apparente acefalia transnazionale della rete, che è un organismo molto complesso. Non è questa la sede per approfondire i punti critici del suo funzionamento tecnico, che si traducono in alcune normative.

A ogni modo, la cosiddetta *governance* – ovvero il modello che si è imposto per la gestione normativa della rete, che è un sistema non gerarchizzato dipendente dalla normativa statale, che, però, si autoproduce in forza di accordi o protocolli orizzontali – si rivela insufficiente.

In questo ambito si condivide e si dà conferma pratica al fatto che l'*internet service provider* (ISP) si colloca in uno scenario in cui tanto la produzione dei beni contraffatti quanto l'immissione sul mercato avviene in realtà che non ricadono sotto la giurisdizione interna, quindi non è l'anello della filiera aggredibile o che può dare riscontro a chi si trovi a combatterlo, siano le autorità di polizia o anche un privato.

Un altro aspetto che si è tenuto a evidenziare è che spesso nei dibattiti pubblici o di stampa si vede con sfavore – quasi si volesse mettere un bavaglio alla rete, secondo un'espressione che è stata utilizzata – l'idea che già in prima istanza il danneggiato possa adire e avere un interlocutore al quale richiedere la cessazione della condotte illecite.

Questo rientra nello schema generale dell'ordinamento. Non è nulla di strano. In questo mio intervento si è evidenziata – a mio avviso, ma credo possa essere riscontrabile – un'anomalia dell'attuale disciplina interna di regolamentazione dei prestatori di servizi.

Vado subito al punto, che nel mio intervento è spiegato meglio, anche perché il tempo è poco, ma forse avrete modo di approfondirlo successivamente.

L'anomalia è che se da un canto viene precisato che il prestatore di servizi è responsabile quando è a conoscenza dell'illiceità del fatto, dall'altro si è subordinato – concedendogli, di fatto, un privilegio – l'obbligo di interrompere la condotta illecita alla comunicazione dell'autorità giudiziaria.

Si è messo, quindi, in evidenza che spesso, a causa di un altro buco normativo che consente una forma di anonimato diffuso nella rete, la possibilità di adire l'autorità giudiziaria non sussiste neanche. Il riferimento va a quegli illeciti (uno su tutti, la concorrenza sleale) che spesso non hanno profili penalistici, quindi non si può compulsare l'autorità di polizia al fine di svolgere le investigazioni idonee a individuare l'autore.

Anche sotto questo profilo si è evidenziata un'altra debolezza del sistema, che è quella per cui i dati di *log*, in forza della normativa sulla *privacy* attualmente in vigore, vengono conservati solo per 12 mesi. Infatti, questa tempistica innanzitutto è diversa – non se ne comprende la ragione – dall'obbligo di conservazione dei tabulati telefonici, che è di 24 mesi, e poi è incompatibile con la durata reale delle indagini preliminari. Infatti, il termine codicistico è di 6 mesi, ma spesso le indagini vengono prorogate, quindi nell'esperienza pratica capita che i dati non siano più comunicabili all'autorità di polizia.

Un altro punto debole sotto il profilo di un'autotutela anche in via stragiudiziale da parte del primo danneggiato è conte-

nuta nell'attuale Codice della *privacy*. Infatti, l'*internet service provider* rifiuta di comunicare all'asserito danneggiato i dati identificativi che conosce, anche se potrebbero non essere veritieri, dal momento che ci si registra, ma nessuno poi controlla nei portali di fornitura di servizi. Certamente, però, il *provider* detiene i dati di *log*.

Viene detto che ciò non sarebbe conforme all'attuale normativa sulla *privacy*. Dico, però, che probabilmente questa sarà presto sostituita dall'entrata in vigore del nuovo regolamento europeo sulla *privacy*, quindi bisognerà vedere se la mia osservazione rimarrà valida.

A ogni modo, l'attuale normativa, all'articolo 24, prevede espressamente che i dati identificativi « possano » essere comunicati quando sono necessari per tutelare un diritto o ai fini di investigazione preventiva. Ecco, questo « possano » ingenera il muro che si incontra quando si richiede in via collaborativa che vengano comunicati i dati.

Un altro punto che potrebbe essere migliorato sotto un profilo normativo è quello dell'inibitoria speciale, prevista dal combinato disposto fra la legge sul diritto d'autore e il decreto legislativo che regolamenta l'attività dei prestatori di servizi, inibitoria che in giurisprudenza la Corte di Cassazione ha trovato problematica perché è istituto di natura obbligatoria, mentre è preferibile un istituto di natura reale. Questo è un tecnicismo quale il sequestro preventivo, quindi incontra delle difficoltà di ordine pratico.

Si è posto poi un problema di ordine generale nel ritenere che gli organismi interni e comunitari dovrebbero decidere se intendono dare una regolamentazione alla rete – un fenomeno naturalistico come qualunque altro – che sia coerente con l'ordinamento nel suo complesso o se si voglia continuare a seguire la strada del *goodwill*, cioè della buona volontà, magari stipulando protocolli con i grossi *player*.

Quello che, a mio avviso, è poco chiaro nel dibattito sul tema è che spesso una regolamentazione non è l'ostacolo allo sviluppo di un fenomeno, ma una tutela per il più debole. Quello che credo stia emergendo anche nel dibattito attuale sui problemi della rete è che la mancanza di regole certe e coercibili da parte dell'autorità lascia spesso campo libero ai *player* più forti. Questo è il mio intervento in sintesi.

PRESIDENTE. Grazie, avvocato. Abbiamo ascoltato due profili molto lontani tra loro.

Abbiamo avuto un *focus* sul versante del consumatore e di tutto quello che ruota intorno all'atteggiamento psicologico e alle motivazioni nell'acquisto del prodotto contraffatto. Aggiungo, a titolo personale, che sarebbe più corretto spezzettare il comportamento dei consumatori a seconda della tipologia di prodotto perché, probabilmente, l'atteggiamento psicologico che si ha nei confronti dell'acquisto di una borsa contraffatta non è lo stesso che si può avere nei confronti di altre merci presenti sul mercato. Questo ragionamento, però, ci porterebbe lontano.

L'avvocato Caristi, che ringrazio nuovamente non solo per l'intervento di oggi, ma anche per la memoria molto dettagliata, con molti spunti, con citazioni di giurisprudenza e con varie angolazioni molto interessanti, ci ha portato sul tema della normativa vigente in materia in particolare di *web* e di riflessi conseguenti sulla contraffazione.

Su questo abbiamo un relatore già operante, il collega Baruffi, quindi direi che è importante che a lui, e a noi di riflesso, venga data la possibilità di approfondire la tematica nelle forme che egli stesso riterrà opportune, non necessariamente qui e in questo momento.

Do ora la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

FILIPPO GALLINELLA. Ringrazio gli auditi perché le relazioni che ci hanno inviato tempo fa sono state molto apprezzate.

Relativamente al rapporto con il consumatore è interessante notare che, forse, ci si riferisce più all'oggettistica che all'alimentare.

In ogni caso, dalla sua relazione si evince che il 90 per cento è appagato oppure non si fa scrupolo, anche se sa che è un reato. Ora, finché c'è la domanda, penso ci sarà sempre anche l'offerta, indipendentemente dalle norme a contrasto che possiamo inserire. Allora, bisogna lavorare sul lato dell'offerta, quindi sicuramente sull'educazione. Questo è fondamentale.

Non so se sarà possibile, ma sarei curioso di sapere se le risposte fossero simili in caso di cibo contraffatto. Ecco, la mia ipotesi è che non lo siano.

Riguardo, invece, alla relazione che riguarda tutto il sistema digitale, alla fine del documento il professore dà sei spunti di riflessione. Vorrei concentrarmi sul terzo in particolare che riguarda l'opportunità del sistema del *provider* di intervenire a seguito di una segnalazione. Ora qui bisogna capire qual è la procedura, perché è l'autorità giudiziaria che deve farla e lui la deve bloccare, anche perché se si lascia la libertà di scelta al *provider* e poi si fa una contestazione o un appello si apre una battaglia di giurisprudenza importante. Questo è un tema sicuramente da approfondire.

Sulla questione dei tempi, si possono anche raddoppiare, dunque si va a 24 mesi per la tenuta dei dati per i controlli. Tuttavia, bisogna lavorare anche sul lato delle indagini perché non vorrei che, avendo ancora più tempo, le indagini si allunghino ancora di più. Insomma, è un cane che si morde la coda. Questo, però, riguarda forse il sistema della giustizia che necessita di risorse specifiche in un settore così particolare.

Riguardo all'accesso, mi soffermerei sulla questione dei protocolli 4 e 6. In particolare, con il protocollo 4 che fa da centralino è chiaro che ci si imbatte nel problema della *privacy* per sapere chi ha inserito quei dati o quel servizio che vende materiale contraffatto. Invece, con un protocollo individuale come il 6 si sa direttamente chi è la persona che immette i dati. Tuttavia, anche lì si pone il problema della *privacy*. Ci sono sentenze della Corte di giustizia in merito. Certo, la *governance* di internet è fondamentale, ma come ci si mette relazione con la salvaguardia dei dati ?

Allora, forse bisognerebbe trovare strumenti che blocchino il flusso finanziario. Visto che quasi tutti i pagamenti avvengono tramite conto *paypal* o carte di credito, si potrebbe bloccare il circuito digitale affinché le banche lavorino sul fatto che quel circuito viene interrotto su segnalazione. Ecco, questa, forse, è la strada di giurisprudenza più attuabile rispetto all'affrontare la questione della *privacy*, che, peraltro, possiamo fare in Italia e in Europa, ma non nel resto del mondo.

Queste sono riflessioni che intendevo portare alla vostra attenzione, anche come spunto di approfondimento.

DAVIDE BARUFFI. Grazie, presidente. Ringrazio, innanzitutto, i nostri ospiti, in particolare l'avvocato Caristi, a cui mi rivolgo. Ho letto la sua memoria molto interessante, ma anche molto tecnica, quindi ho avuto qualche difficoltà. Vorrei capire, pertanto, un aspetto, anche in riferimento a quanto diceva poc'anzi il collega Gallinella.

Vi è un punto specifico in cui mi pare si provi a costruire uno spazio di agibilità più forte circa il problema dell'anonimato. C'è il tema della *privacy*, ma anche quello della tutela e dell'autotutela degli aventi diritto, che più che a costituire – mi riferisco alla sua proposta – un obbligo a corrispondere azioni da parte degli *internet service provider* chiamati in causa, sia un dovere a farsi carico del problema, quindi a farsi parte diligente.

Se è così, mi pare che si centri una questione particolarmente importante, per come segnalataci dai portatori di interesse. Infatti, senza dilatare lo spazio della responsabilità astratta dei soggetti in campo, si definisce un ambito interessante di tutela anche stragiudiziale.

Mi pare che sia questo il senso, senza sconfinare – ripeto – in attività di altro ambito, quale quella dell'autorità giudiziaria, che, tra l'altro, non sempre è nella

disponibilità diretta, per le ragioni che indicava anche lei nella sua breve relazione verbale di oggi.

Questo è il punto che vorrei mettesse a fuoco perché credo sia di grande interesse per la Commissione, anche per rispondere a sollecitazioni che ci stanno pervenendo in proposito.

Come seconda questione, lei fa riferimento alla nuova legge messa in campo dalla Federazione russa, che dispiega la sua efficacia negli ultimi mesi, ovvero dal settembre 2015.

Traducendo volgarmente non da avvocato, si tratta dell'obbligo, laddove si registrino e gestiscano i dati dei cittadini russi, di avere il *database* sul territorio russo. Ciò non significa che Google diventi russa, ma che deve aprire una propria sede di responsabilità in quel territorio.

Ora, la questione, se portata all'assoluto, genererebbe un impazzimento e un irrigidimento del sistema, quindi scoraggerebbe anche lo sviluppo della rete e dell'accessibilità da parte dei cittadini e del mercato in generale. Tuttavia, se presa in carico – come capisco anche da alcune considerazioni che lei ha fatto senza dare giudizi – su sistemi di dimensione ampia può essere guardata con attenzione, anche se siamo a livello sperimentale.

Per farmi capire dai colleghi, pensare che un obbligo di questo genere possa essere messo in carico rispetto alla comunità di Canicattì è irragionevole; pensare che possa essere messo in carico rispetto allo Stato italiano può essere problematico, ma se messo in carico alla dimensione comunitaria può assumere una valenza completamente diversa, anche perché l'interesse da parte degli operatori rimarrebbe comunque molto forte su mercati sviluppati, popolati e così via.

Pertanto, le chiedo, anche da questo punto di vista, una sua considerazione aggiuntiva, visto che si è fermato un centimetro prima di esprimere una valutazione.

L'ultima cosa davvero telegrafica è una richiesta di chiarimento. Avrei potuto anche documentarmi personalmente, ma non ho avuto tempo e modo. A pagina 7 della sua relazione, lei parla giustamente della possibilità di introdurre clausole di esonero e anche nella raccomandazione dice che ritiene opportuno introdurre meccanismi di cooperazione che facilitino l'attività di repressione grazie all'informazione di cui è in possesso l'ISP.

Ecco, mi spiega tecnicamente che cosa significa ? Lo chiedo anche per riuscire a dare un senso a quello che ho letto dopo.

PRESIDENTE. Siccome ha avuto delle domande più puntuali e complesse, direi di cominciare dall'avvocato Caristi, a cui cedo la parola per la replica.

ANDREA CARISTI. Cerco di rispondere sul primo punto, che se ben ricordo, è comune alle domande dei due onorevoli, ovvero sulla questione della normativa sulla prestazione dei servizi.

A questo riguardo ho cercato di evidenziare che, allo stato, il prestatore di servizi, qualora venga messo a conoscenza da un privato di fatti che, in una delle ipotesi, presume illeciti, è già responsabile. Non viene esonerato, ma tecnicamente ha un privilegio, cioè un'esclusione rispetto a un obbligo di *facere*, ovvero di provvedere a quanto dovrebbe in base alla normativa generale dell'ordinamento.

Il riferimento va all'articolo 40 capoverso del Codice penale che impone di attivarsi per impedire un evento giuridico che si ha l'obbligo giuridico di impedire e all'articolo 2043 del Codice civile, ovvero alla responsabilità aquiliana. Quindi, il soggetto è già in posizione di responsabilità.

Allo stato, c'è un inciso che va oltre la delega originaria conferita al Governo perché il nostro decreto legislativo origina dal recepimento della direttiva comunitaria. Tuttavia, con questo inciso si è andati – ripeto – oltre la stessa delega perché l'operatore viene fatto salvo dall'obbligo normale che incombe.

Questo è un punto importante che differisce rispetto a qualunque altra attività espletata. Se a imprenditore che compie un'attività si segnala un illecito, egli – come qualunque altro cittadino – ha que-

sto obbligo. Dunque, il criterio non è quello che viene detto sulla stampa. Giuridicamente sarebbe un diritto potestativo (con una dichiarazione influisco nella sfera giuridica altrui), ma non è così perché c'è comunque la barriera dell'ordinaria diligenza.

Peraltro, riguardo al Codice della *privacy* viene da ritenere che la norma faccia riferimento alle investigazioni difensive anche preventive, per le quali la parte deve dare uno specifico mandato, quindi è un'attività che ha già un *fumus* di sussistenza. Insomma, non è una telefonata, quindi non è un diritto potestativo, cioè non si attribuisce a un soggetto, con una mera dichiarazione, la facoltà di incidere nella sfera giuridica altrui.

Si assoggetterebbero, quindi, i prestatori di servizi e le attività *internet* al normale regime di responsabilità del resto dell'ordinamento senza, a mio personale giudizio, ostacolarne lo sviluppo, anzi favorendo la normalizzazione di uno sviluppo coerente con i valori dell'ordinamento.

PRESIDENTE. Ringrazio l'avvocato Caristi. Penso di interpretare lo spirito di molti qui presenti raccomandando al collega Baruffi – lui l'avrebbe fatto ugualmente – di fare in modo che la Commissione ne parli anche per capire dove si va a parare, stante la estrema sensibilità di questa materia e gli spaventosi interessi in campo tra il mondo di internet e dei *provider* e tutte quelle scuole di pensiero e di interessi che, invece, vorrebbero (secondo lo spirito dell'avvocato Caristi) un intervento. Chiedo scusa al collega perché forse la mia raccomandazione è pleonastica.

Cedo ora la parola al professor Ofria per la sua replica.

FERDINANDO OFRIA. Rispondo all'onorevole Gallinella. Ovviamente, ci deve essere consapevolezza nell'acquisto di questi beni. Forse non l'ho specificato nella mia esposizione, ma lo dico nella mia nota. Addirittura, qui spiego il falso come possesso: il compratore sa di acquistare un falso e desidera farlo per identificarsi con esso. Il motivo principale che caratterizza quest'ultimo punto è l'apparire, ovvero raggiungere, attraverso il falso, lo *status* sociale di chi si può permettere di acquistare l'originale.

Questo è il punto fondamentale. È ovvio, però, che per gli alimenti è diverso. Ci vuole educazione anche per capire che mangiare alimenti diversi da quelli originali potrebbe essere nocivo. Tuttavia, questo è un altro campo.

ANDREA CARISTI. Intervengo brevemente sulla questione posta dall'onorevole, che immagino si riferisse al richiamo alla legge federale russa. Certamente, il mio invito era in chiave comunitaria. Altrimenti, non sarebbe né realistico, né possibile, anche per le condivisibili ragioni di mercato. Peraltro, io stesso evidenziavo che, a fronte di un mercato vasto, il *player* difficilmente lo abbandona nel suo stesso interesse.

PRESIDENTE. Ringrazio ancora gli auditi del loro contributo, dichiaro conclusa l'audizione e dispongo che la documentazione presentata sia allegata al resoconto stenografico della seduta odierna.

La seduta termina alle 15.25.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. RENZO DICKMANN

Licenziato per la stampa il 22 aprile 2016.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

Commissione Parlamentare di inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo

Proposta di ricerca

La domanda di beni contraffatti: fattori socio economici determinanti e politiche di contrasto

Come è noto, il fenomeno della contraffazione penalizzare l'economia italiana sotto diversi profili. Produce, infatti, danni elevati: 1) ai consumatori, se inconsapevoli o, comunque, ignari dei rischi che corrono qualora dovessero utilizzare componenti non omologati; 2) alle imprese, per la perdita di fatturato che devono subire e per i costi che devono sostenere nel difendere i loro prodotti costruiti a norma, secondo i requisiti di legge; 3) agli Stati, per aspetti connessi alla fiscalità e alle attività criminose cui spesso la contraffazione si accompagna, come quelle legate sia allo sfruttamento del lavoro (anche minorile) per la produzione, sia al fatto che la maggior parte degli introiti finisce nelle mani delle organizzazioni criminali. Tali capitali vengono poi riciclati o nell'economia legale attraverso operazioni finanziarie, oppure reinvestiti in ulteriori attività delittuose, quali ad esempio il traffico di armi o di droga. Al tempo stesso, l'analisi dell'economia legata alla contraffazione svela comportamenti inediti sul piano della domanda e dell'offerta. La contraffazione appare contemporaneamente variabile strutturale della produzione, mercato parallelo, area di continuo ridisegno del limite tra legalità e illegalità[1].

In termini di *policy*, al fine di contrastare la contraffazione, bisogna che siano interventi sia dal lato della domanda sia dal lato dell'offerta[2].

Per potenziare le politiche di contrasto alla contraffazione dal "lato della domanda", lo scrivente propone alla "Commissione Parlamentare d'inchiesta sui fenomeni della contraffazione" di affidare ad un Ente di ricerca pubblico (es. Università) o Privato, uno studio statistico, di natura socio-economica,

[1] Centorrino M, Ofria F. (2004) *L'economia della contraffazione. Un fallimento di mercato*, Rubbettino, Soveria Mannelli, pp. 108

volto a rilevare fino a che punto la domanda di beni contraffatti da parte del consumatore sia condizionata dal reddito, dal contesto sociale, dal livello di alfabetizzazione –in Appendice 1, si specifica cosa si intende per "consapevolezza del consumatore ad acquistare beni contraffatti"; mentre, in Appendice 2 si riportano in sintesi i risultati di una ricerca[3] riferita alla percezione della contraffazione tra i consumatori**.** In tale studio, ovviamente, in tale studio la correlazione tra bene inferiore e reddito non è oggetto di analisi. In particolare, l'ipotesi da verificare, attraverso questa analisi statistica, è se il bene contraffatto sia da definirsi, anche, come "bene inferiore" -sul concetto teorico di bene inferiore, si veda Appendice 3. Qualora i risultati della ricerca statistica confermino questa ipotesi, le politiche di contrasto alla contraffazione dal lato della domanda dovrebbero essere caratterizzate, oltre che da una forte campagna di sensibilizzazione sulla pericolosità dell'acquisto di prodotti falsi e dei possibili effetti nocivi sulla salute, da forti investimenti in capitale umano, attraverso l'educazione scolastica e le informazioni offerte dai media. Sul punto, un ruolo rilevante potrebbero ricoprirlo le politiche volte alla crescita del capitale umano presenti nell'Accordo di Partenariato 2014-2020[4].

Prof. Ferdinando Ofria
Università degli Studi di Messina
Esperto della Commissione Parlamentare di inchiesta sui fenomeni della contraffazione

[2] Per una dettagliata sintesi degli strumenti e delle politiche di contrasto nazionali ed europee al fenomeno, dal lato dell'offerta, si veda: http://www.uibm.gov.it/index.php/lotta-alla-contraffazione).
[3] http://www.uibm.gov.it/attachments/indagine_percezione_contraffazione.pdf
[4] http://www.agenziacoesione.gov.it/it/politiche_e_attivita/programmazione_2014-2020/Accordo_di_Partenariato.html

Appendice 1

Non tutti i consumatori sono sempre consapevoli di acquistare un bene contraffatto. In letteratura, infatti, esistono tre fattispecie di consumatori di tali beni. Canestrari (2007)[5] espone la seguente classificazione: 1) *Falso per vero:* l'acquirente crede di acquistare un prodotto originale; 2) *Falso quasi vero:* l'utente crede di comprare un prodotto di marca rimasto invenduto o con piccole imperfezioni o una sottomarca. Anche in questo caso è ignaro del falso acquisto; 3) *Falso come possesso:* il compratore sa di acquistare un falso e desidera farlo per identificarsi con esso. Il motivo principale che caratterizza quest'ultimo punto è l'"apparire", ovvero raggiungere, attraverso il falso, lo *status sociale* di chi si può permettere di acquistare l'originale.

Appendice 2

Nel 2010 la Direzione Generale per la Lotta alla Contraffazione - UIBM ha affidato alle Associazioni dei Consumatori, cofirmatarie di uno specifico protocollo d'intesa[6], la realizzazione di una ricerca su "La percezione della contraffazione tra i consumatori", con l'intento di indagare su: 1) la dimensione del fenomeno; 2) le modalità e i canali di acquisto di prodotti contraffatti; 3) le tipologie di prodotti maggiormente acquistati; 4) la consapevolezza dei rischi personali che si corrono e dei danni economici causati da questo tipo di acquisti. L'indagine quali-quantitativa è stata articolata in due fasi. La prima è stata svolta tra dicembre 2010 (in modo di studiare le abitudini degli acquirenti nel periodo natalizio) e gennaio 2011 (così da rilevare i dati sulle modalità di acquisto in tempo di saldi). Ha coinvolto un campione di 4.000 persone tramite interviste telefoniche CATI (Computer Assisted Telephone Interviews). Dall'inchiesta è emerso che: 1) solo il 14,65% del campione si è dichiarato acquirente di prodotti contraffatti; 2) il 90% del campione sa che comprare prodotti contraffatti è un reato; 3)quasi il 73% degli acquirenti mostra tuttavia uno scarso senso civico, dichiarando di non sentirsi in colpa nei confronti del fisco, né per aver alimentato gli interessi della malavita organizzata, né per aver danneggiato l'economia; 4) i prodotti contraffatti più acquistati sono capi di abbigliamento e accessori, prevalentemente su bancarelle, da ambulanti e "vu cumprà"; 5) il prezzo è il principale stimolo all'acquisto del contraffatto (il 91,4% lo dà come primo o secondo motivo); 6) l'acquirente dichiara di

[5] Canestrari P. (2007), *Imitazione e falsificazione. Una prospettiva sociologica*, Franco Angeli, Milano

[6] http://www.uibm.gov.it/index.php/missione-17-156-34/2005978-20-07-2010-il-protocollo-di-intesa-con-le-associazioni-dei-consumatori

non trovare una significativa differenza di qualità con l'originale: il 71,2% dichiara anzi che è soddisfatto di ciò che ha comprato e che ripeterà la scelta. Nel corso del 2012 si è svolta la seconda fase dell'indagine conoscitiva. Sono state effettuate 1.200 interviste telefoniche CATI a un campione rappresentativo della popolazione italiana per sesso, età, area geografica e ampiezza demografica. Si è rilevato che: 1) la percentuale di intervistati che ha ammesso l'acquisto di prodotti contraffatti, pari al 30,6% del campione, continua a essere in difetto rispetto a quanto comunemente percepito; se risulta più elevata rispetto al corrispondente dato rilevato nella prima fase, ciò è dovuto al fatto che il secondo questionario è stato volutamente strutturato in modo più discorsivo e meno inquisitorio, al fine di superare le reticenze riscontrate; quasi il 96% degli Italiani è a conoscenza che i prodotti contraffatti possono essere dannosi per la salute; 3) l'abbigliamento e gli accessori (23,2%) sono risultate le categorie di prodotti contraffatti maggiormente acquistate: ciò è spiegabile perché in questi settori è più facile avere la coscienza di acquistare un prodotto contraffatto sia a causa della notorietà dei marchi contraffatti sia a causa dell'altissimo prezzo degli originali. Invece nelle categorie alimentare, cosmetici e giocattoli è più facile che l'acquisto avvenga in modo inconsapevole a causa della non conoscenza profonda del mercato originale; 4) il motivo economico (prezzo conveniente) domina fortemente tra le cause di acquisto di questi prodotti (79,8%).

Appendice 3[7]

I beni inferiori sono beni economici la cui domanda si riduce all'aumentare del reddito del consumatore. Un bene inferiore è generalmente caratterizzato da un prezzo molto basso e da una qualità molto inferiore rispetto ad altri beni sostituiti. Al crescere del reddito il consumo dei beni inferiori si riduce in quanto l'effetto di reddito positivo consente al consumatore di modificare le proprie scelte. Nel caso dei beni inferiori la curva di domanda è inclinata negativamente rispetto al reddito L'effetto può essere rappresentato graficamente tramite una curva di domanda di Engel. Come è noto, le curve di domanda rispetto al reddito (R) differiscono a seconda il tipo di bene (x) richiesto. La celebre legge di Engel enuncia che "più povera è una famiglia, maggiore è la proporzione della sua spesa totale che deve essere destinata all'acquisto di generi alimentari", ed, inoltre, "più ricca è una nazione più piccola è la proporzione di generi alimentari nella spesa". Quanto asserito indica che all'aumento del reddito la gente cambia la proporzione in cui domanda i vari beni. Le forme delle curve

[7] Per maggiori approfondimenti, si veda: Ofria F, Cava A. (2010). *La merce nell'epoca della sua riproducibilità contraffatta. Un'analisi economica e socio-culturale*. Messina: C.I.R.S.D.I.G, vol. N. 42, p. 1-39

engeliane di domanda dipendono dal coefficiente engeliano di elasticità(e_r), il quale è calcolato dal rapporto tra la variazione relativa o percentuale del bene ($\frac{\Delta x}{x}$) e la variazione relativa o percentuale del reddito ($\frac{\Delta R}{R}$):

$$e_r = \frac{\Delta x}{x} / \frac{\Delta R}{R}$$

Che può esprimersi, anche, come il rapporto tra la propensione marginale al consumo ($\frac{\Delta x}{\Delta R}$) e la propensione media al consumo ($\frac{x}{R}$).

$$e_r = \frac{\Delta x}{\Delta R} / \frac{x}{R}$$

Come è possibile rilevare nel *Fig. 1,* il valore assunto da e_r ci dà informazioni circa la natura del bene in questione:

- se $e_r \succ 1$, si tratterà di un bene di lusso, oppure, di un nuovo bene introdotto sul mercato. Così, se il reddito aumenta dell'1% la domanda del bene aumenta più dell'1%, e il consumatore spende una frazione sempre più alta nell'acquisto di beni di lusso. Viceversa, nel caso di diminuzioni del reddito (lungo la curva D_3 fino al punto *F*, $e_r \succ 1$;

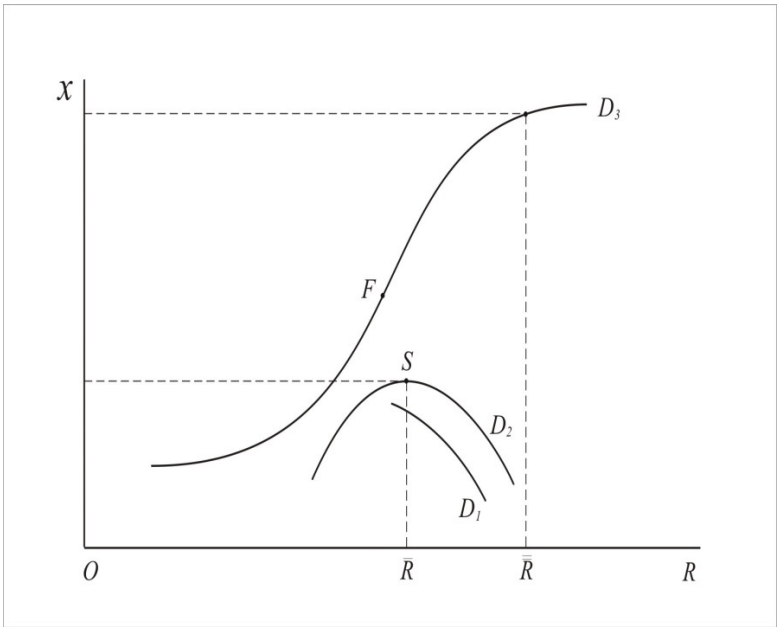
- se $0 \prec e_r \prec 1$, varia, si tratterà di beni di prima necessità, ovvero, di beni normali. Pertanto, all'aumentare del reddito, il consumatore spende una frazione più piccola di esso nell'acquisto di tali beni (lungo la D_2 della fig. 1 fino al punto *S*, $0 \prec e_r \prec 1$);

- se $e_r \prec 0$, si tratterà di un bene inferiore: il consumatore diminuisce la quantità del bene all'aumentare del suo reddito (lungo la curva D_1, $e_r \prec 0$).

In sostanza, le curve D_2 e D_3 evidenziano l'esistenza di un livello di saturazione, geometricamente rappresentato dalla linea orizzontale tratteggiata. Nel caso D_2, parleremo di saturazione assoluta: una volta arrivato al livello di reddito $\bar{R}$, il consumatore, anziché aumentare, diminuisce la quantità domandata del bene. Nel caso D_3, ci troviamo di fronte ad una saturazione relativa: al crescere del suo

reddito, la famiglia aumenta la quantità domandata del bene, ma superato il livello di reddito $\bar{\bar{R}}$ essa tende a stabilizzare i suoi consumi. Infine, il caso D_1è quello in cui all'aumentare del reddito, la famiglia diminuisce la quantità domandata del bene. In particolare, com'è noto, i beni inferiori sono quelli che assorbono larga parte della spesa dei consumatori aventi reddito molto basso. Ad esempio, nell'immediato dopo guerra i contadini del Mezzogiorno d'Italia, non potendosi permettere di acquistare la carne, per sopperire alle loro esigenze proteiche, domandavano solo legumi (bene inferiore). L'aumento del loro reddito negli anni successivi ha fatto sì che questi ultimi abbiano potuto sostituire i legumi con la carne.

Figura 1



STUDIO LEGALE
Caristi

Avv. Andrea Caristi

Via V. Monti, 8 – 20123 - Milano
Tel 02.46712581 - Fax 178.27.28.840
Via Cratemene, is. 312 98122 - Messina
Tel. 090.6406665- Fax 0906406665
email: avv.caristi@gmail.com - pec: caristi@pec.it

Commissione Parlamentare di inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo

La Contraffazione ed *Internet*.

Alcuni aspetti problematici e spunti di risoluzione.

In riscontro alla richiesta indirizzata da codesta Spettabile Commissione ai propri consulenti di far pervenire spunti di riflessione e contributi sulle tematiche afferenti il contrasto della contraffazione, con il presente, breve, lavoro si evidenzieranno alcuni "nodi" critici e problematici che le peculiarità del mezzo *internet* - ed il suo attuale sistema di *governance*[1] - frappongono ad un efficace e celere contrasto dei fenomeni di contraffazione e pirateria *online*.

1. La Contraffazione e la Pirateria in *Internet*.

Parallelamente alla distribuzione di merci contraffatte (per altro, usualmente prodotte in paesi ove la manodopera ha un costo minore che nell'area UE) attraverso i canali tradizionali - quali gli operatori, compiacenti od ignari, della normale rete commerciale e l'ambulantato - negli ultimi anni ha assunto rilievo crescente l'offerta fraudolenta di prodotti usurpativi attraverso il *web*.

La diffusione ormai capillare delle connessioni private alla rete, anche attraverso i dispositivi mobili e quindi lungo l'arco dell'intera giornata, e la maggiore diffusione ed accettazione, anche nel nostro Paese, dell'*e-commerce* quale strumento ordinario di acquisto di beni e servizi, ha inevitabilmente comportato una crescita esponenziale, quantitativa e qualitativa, dell'utilizzo del *web* quale canale di distribuzione di beni illeciti.

[1] Il "cuore" di *Internet*, costituito dal DNS (*Domain Name System*), è sotto l'autorità dell'ICANN, società *non-profit* di diritto privato statunitense, che si autodefinisce come "*an internationally organized, public benefit non –profit company*", la quale persegue una rappresentatività globale e multipla (*multistakeholder).*

L'utilizzo di *internet* quale veicolo privilegiato di diffusione di beni imitati trova ragione, in particolare, in alcune caratteristiche peculiari del *medium* stesso che, in forza soprattutto dei complessi profili di transnazionalità che caratterizzano la *governance*[2] della rete, rendono spesso problematiche le azioni di contrasto e di *enforcement* di provvedimenti giudiziari od amministrativi di tutela dei diritti lesi.

Per altro, come già accennato più sopra, i beni contraffatti generalmente provengono da mercati con manodopera a basso costo[3]. Con tale premessa, è di tutta evidenza come la rete *internet* – specie con riguardo alla distribuzione di prodotti di dimensioni fisiche ridotte – si imponga quale mezzo privilegiato di azzeramento della distanza geografica tra produttori-distributori di beni usuprativi ed i consumatori finali.

Inoltre, sovente, la vendita di prodotti contraffatti avviene all'insaputa ed in danno degli stessi consumatori che, impossibilitati dalla distanza geografica dal venditore ad una verifica *de visu* del prodotto e della sua regolarità, credono invece di acquistare merce legittima; altre volte, invece, specie tra le fasce di consumatori di più giovane età, l'acquisto di prodotti imitativi costituisce – specie con riferimento ai settori della moda e delle *luxury goods* - una scelta deliberata al fine di acquisire, ad un costo sensibilmente minore, beni che riecheggino, seppur in forma adulterata, il prestigio degli originali.

Particolare allarme ha destato, poi, la possibilità di reperire ed acquistare, attraverso *internet,* prodotti che possono essere venduti solo attraverso canali regolamentati (es. i farmaci) fattispecie che è stata oggetto di particolare attenzione da parte del Consiglio Nazionale Anti Contraffazione (CNAC) venendo inserita tra le priorità e le *best-practice* del Piano Nazionale Anticontraffazione.[4]

Le tipologie, poi, delle condotte contraffattive perpetrabili per mezzo di *internet*, o rese più agevoli dal suo utilizzo, spaziano dall'offerta di prodotti contraffatti in senso classico – costituita dall'immissione nel mercato di prodotti recanti il medesimo

[2] Il concetto di *governance* gode di una certa fortuna in relazione ad ambiti normativi, in prevalenza internazionali, caratterizzati dalla parallela e non gerarchizzata azione di soggetti diversi, di natura e vocazione disparata in una costellazione di spinte e rappresentazioni di interesse (Krisch e Kingsbury, 2006,1)

[3] Ministero per lo Sviluppo economico – Dipartimento per l'impresa e l'internazionalizzazione – Direzione Generale per la lotta alla contraffazione – Ufficio Italiano Brevetti e Marchi – Guida operativa a l sistema della proprietà intellettuale in Italia – p. 118

[4] PIANO NAZIONALE ANTICONTRAFFAZIONE - Macro-priorità, migliori pratiche e indicazioni per l'orientamento delle azioni future in materia di lotta alla contraffazione pagg. 79-89

marchio, confezione e descrizione utilizzata dal produttore originale – ad altre rese possibili dalle caratteristiche specifiche del mezzo i*nternet*.

E' opportuno evidenziare difatti che, con riferimento specifico alla contraffazione a mezzo *internet*, ormai viene pacificamente inclusa nel concetto di contraffazione anche, e forse soprattutto, ogni forma di sfruttamento "parassitario" del marchio altrui.

Il riferimento di cui sopra va, ad esempio, all'utilizzo del nome commerciale altrui quale nome a dominio[5], alla riproposizione del marchio altrui quale veicolo di attrazione di visitatori verso le proprie pagine *web*, alla variegata costellazione di attività compiute in spregio dei diritti di proprietà intellettuale altrui quale, a titolo esemplificativo, la messa in circolazione, sotto forma di *download* di *file*, di brani musicali protetti dalle norme sul diritto d'autore.

Con particolare riferimento a queste ultime ipotesi, poi, se le stesse vengono perpetrate su scala sistematica, può parlarsi più propriamente di **pirateria**, la quale consiste nelle "*contraffazioni evidenti dei marchi, disegni e modelli registrati e le violazioni di altrui diritti di proprietà industriale realizzate dolosamente in modo sistematico*"[6].

2. Alcuni profili problematici comuni alle condotte usurpative perpetrate a mezzo di *Internet*. Il ruolo degli *Internet Service Provider* (*ISP*).

Che si tratti di una vendita *online* di prodotti imitativi, piuttosto che di ipotesi più insidiose, quali ad esempio, l'utilizzo occulto, o parassitario, del marchio altrui [7], la

[5] c.d. *Cybersquatting/Domain Grabbnig* - pratica maggiormente frequente, con riferimento al Tld ".it", agli albori del *web*, quando l'assegnazione del nome a dominio avveniva esclusivamente in forza del principio "*first come, first served*". Oggi, l'utilizzo di un marchio registrato quale nome a dominio .it è espressamente vietata sia dalle regole di *naming* sia dall'art. 22del C.p.i. ("*È vietato adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale un segno uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività di impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni.*). Rimane condotta problematica e rilevante con riferimento alle altre estensioni al di fuori della "giurisdizione" della *Naming Authority italiana.*

[6] art. 144 C.p.i. Dlgs 10.02.2005 n°30

[7] Questa ipotesi si realizza quando la denominazione altrui viene utilizzata quale *Meta tag* del proprio sito, al fine di incrementarne il volume di ricerca, e quindi le visite, sfruttando l'effetto traino del marchio, ovvero, ad esempio, quale parola chiave del sistema di annunci pubblicitari *Google Ad Words.* Proprio queste due ipotesi hanno visto contrapposte, innanzi il Tribunale di Palermo, sezione specializzata p.i., la *Maggiore Rent S.p.a* e *Sicily by Car S.p.a* e

maggior parte delle condotte usurpative, o contraffattive, perpetrate per mezzo della rete, presenta alcuni profili problematici comuni che si frappongono, sovente, ad una efficace azione di contrasto, sia da parte dello stesso danneggiato, nei limiti in cui potrebbe mettere in atto condotte di auto-tutela (inoltro di diffide stragiudiziali, azioni giudiziarie etc.), sia da parte delle Autorità.

Sotto un primo profilo, difatti, spesso è disagevole, se non impossibile, risalire in via diretta all'identità degli autori della condotta illecita, che possono contare, almeno *prima facie*, sull'anonimato.[8]

Sotto un secondo profilo, inoltre, la maggior parte delle attività illecite origina in regioni geografiche che ricadono al di fuori della giurisdizione degli organi di tutela nazionali e comunitari europei, con il conseguente rischio, sempre attuale, che la rete possa costituire un "porto franco" per le attività illecite.

Per altro, le attività usurpative possono essere consumate sia per mezzo di siti nella diretta disponibilità del contraffattore quanto, soventemente, per mezzo di piattaforme gestite da *ISP* [9]terzi.

Il riferimento di cui sopra va, a titolo di esempio, a realtà quali *Ebay,* piattaforma di aste e vendite *online Business to Consumer (B2C)* od *AliBaba*, piattaforma cinese di negoziazioni *Business to Business (B2B).*

La difficoltà nel pervenire all'identificazione dei responsabili e nel conseguire un adeguato *enforcemen*t dei diritti *online*, ha già indotto tanto gli *stakeholder* quanto le Autorità (su tutte il CNAC – Consiglio Nazionale Anti Contraffazione) ad individuare nel "terminale" distributivo della filiera contraffattiva, costituito dall'*Internet Service Provider* (*ISP)*, l'anello della catena sul quale concentrare l'interesse repressivo.

Al riguardo, occorre subito rilevare che il tema della responsabilità degli *ISP,* in ordine alle condotte perpetrare da terzi - in generale ed anche al di là del tema

Google Inc. La Maggiore lamentava l'utilizzo del proprio marchio "Maggiore" quale *Meta Tag* del sito della *Siciliy by Car* ed anche quale *keyword* della campagna *AdWords* di quest'ultima.

[8] L'esperienza investigativa ha ormai collaudato protocolli ed attività attraverso le quali la Polizia Giudiziaria può, in una buona parte di ipotesi, risalire all'identità degli autori di illeciti perpetrati *online* cfr. Procura di Milano -.Procedure Investigative sui primi accertamenti di Polizia Giudiziaria in Materia di Reati Informatici, cfr. Attività Investigativa in Internet –Arma dei Carabinieri . Studi anno 2012 cfr. *Internet Forensics* – Arma dei Carabinieri- Rassegna - 2009

[9] *Internet Service Provider*

specifico del contrasto alla contraffazione e pirateria *online* - è da tempo oggetto di un acceso dibattito in dottrina e non ha ancora trovato un orientamento uniforme e consolidato in giurisprudenza.

E' bene anticipare che, da sempre, è stata esclusa, tanto dogmaticamente quanto in ambito legislativo, l'ipotesi di "addossare" agli *ISP* un "*obbligo generale di sorveglianza*" o di "*ricerca attiva di fatti e circostanze che indichino la presenza di attività illecite*"[10], poiché si è ritenuta una tale misura in contrasto con il principio del libero sviluppo e della libera accessibilità della rete, oltre che, nell'abito specifico dell'*e-commerce*, in contrasto con la diffusione del commercio elettronico in chiave pro-concorrenziale.[11]

Si è da subito ritenuto, difatti che "*l'attribuzione agli ISP di un regime troppo gravoso di responsabilità finirebbe per inibirne o, almeno, ridurne l'attività con conseguenze facilmente prevedibili sullo sviluppo delle Rete e sulle enormi possibilità che la stessa fornisce sia nel campo dei rapporti economici che in quello dello sviluppo della personalità e della libertà di manifestazione del pensiero*"[12]

Con riferimento alla natura dei servizi offerti dagli *ISP*, il più elementare è costituito dalla stessa fornitura di accesso alla rete (c.d. *access provider*), propedeutica alla fruizione da parte dell'utente di tutti gli altri servizi da *Internet* quali quelli della navigazione sul *World Wide Web* od i servizi *email*.

Nel quadro normativo interno e comunitario, la legislazione di riferimento è costituita dal Dlgs. 9 aprile 2003 n. 70 emanato in forza della delega conferita al Governo dalla legge 1° marzo 2002 n. 39 (Legge comunitaria 2001) per l'attuazione della Direttiva n. 2000/31/CE («Direttiva sul commercio elettronico»).

La suddetta direttiva 2000/31 CE si è proposta di creare regole uniformi per il commercio elettronico e, in particolare, di fornire indicazioni comuni, relativamente alle regole da applicare alla prestazione di servizi delle società dell'informazione definiti come "*qualsiasi servizio prestato normalmente dietro retribuzione, a*

[10] Art. 16 Dlgs. 70/2003

[11] PIANO NAZIONALE ANTICONTRAFFAZIONE - Macro-priorità, migliori pratiche e indicazioni per l'orientamento delle azioni future in materia di lotta alla contraffazione pag. 21

[12] *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet Provider. Una sintesi di diritto comparato*, in Diritto dell'informazione e dell'informatica, 2000, pag . 836

distanza, per via elettronica, mediante apparecchiature elettroniche d'elaborazione (compresa la trasmissione digitale) e di memorizzazione dei dati e a richiesta individuale di un destinatario di servizi".

Già a livello comunitario, inoltre, è stato fissato il principio della divisione fra meri servizi d'accesso e servizi di fornitura/produzione di contenuti, con conseguente differenziazione di responsabilità.

In particolare, la direttiva, ed il Dlgs. 2003/70, tendono a non attribuire una responsabilità al prestatore, e quindi anche al *provider*, che si comporti da mero fornitore d'accesso[13], purchè "*non effettui una produzione propria di contenuti, non faccia selezioni di destinarlo e non metta in atto operazioni di filtraggio.*"

Parimenti, il citato Dlgs. 2003/70, distingue, tra i prestatori di servizio della società dell'informazione, tra quelli che compiono attività di semplice trasporto (art. 14, c.d. *mere conduit*), piuttosto che attività di memorizzazione temporanea (art. 15, c.d. *caching*) od attività di memorizzazione delle informazioni (art. 16, c.d*. hosting*).

In riferimento a tutte le suddette tre tipologie di prestazione di servizio, inoltre, il medesimo Dlgs. 2003/70, al successivo art. 17, ha escluso in radice che i medesimi fornitori di servizio possano essere assoggettati, come già anticipato, ad un "*obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano, né ad un obbligo generale di ricercare fatti o circostanze che indichino la presenza di attività illecite*".

Un altro aspetto che giova mettere in luce - sul quale si tornerà in prosieguo del presente lavoro e che costituisce, allo stato, il *punctum dolens* dell'individuazione nell'*ISP* del soggetto sul quale indirizzare le attenzioni repressive – è costituito dalla previsione di cui all' art. 16 lett b) in forza della quale l'*ISP* "*non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore…non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita*" e "*…non appena a conoscenza di tali fatti,* ***su comunicazione delle autorità competenti****, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*".

[13] c.d. *ASP* (*Access Porvider*)

Con riferimento alla "centralità" del ruolo degli *ISP*, perlomeno ai fini di un efficace contrasto delle attività contraffattive consumate attraverso "portali" di vendita, la stessa è già stata oggetto dell'attenzione del Consiglio Nazionale Anticontraffazione (CNAC), che, nel "Piano Nazionale Anticontraffazione", correttamente, ha differenziato due possibili posizioni, di rilevo, che gli *ISP* possono ricoprire con riguardo a fattispecie contraffattive.

Una prima ipotesi di rilievo è quella in cui l'*ISP* abbia un ruolo "*meramente tecnico, automatico e passivo*" e, pertanto, il prestatore del servizio "*non conosce né controlla le informazioni trasmesse o memorizzate*".

In relazione alla suddetta ipotesi, il CNAC: "*ritiene opportuno introdurre meccanismi di cooperazione che facilitino l'attività di repressione grazie alle informazioni di cui è in possesso l'ISP (ad esempio dovrebbe essere raccomandata una* ***clausola di esonero*** *di responsabilità dell'ISP nei confronti dell'utente registrato nel momento in cui venga richiesto all'ISP di fornire "inaudita altera parte" una serie di informazioni collegate all'utente registrato stesso quali il giro di affari intermediato, le informazioni sui mezzi di pagamento e tutte le informazioni rilevanti al fine di determinare l'ambito dell'illecito*)."

Con riferimento alle informazioni potenzialmente detenute dagli *ISP*, riguardanti gli autori di condotte illecite – anche al di là dell'ambito della contraffazione e delle lesioni dei diritti di proprietà intellettuale ma, in generale, con riferimento alle condotte illecite perpetrabili a mezzo *web* - è bene evidenziare un altro *punctum dolens*.

I fornitori di servizio difatti, necessariamente, sono in possesso di informazioni che, anche ad un livello meno "pervasivo" di quelle oggetto della clausola di esonero ipotizzata dalla CNAC, sono essenziali al fine di pervenire all'identificazione dell'autore di una condotta illecita, quali ad esempio i *file* di *log* contenenti il relativo indirizzo IP.

Al riguardo, in primo luogo, occorre osservare - con riferimento, in particolare, alle piattaforme di *e-commerce*, *social networking o search engine* - che nessuno dei

maggiori operatori è italiano, od opera attraverso *server* collocati sul territorio nazionale italiano, o ha una sede legale in Italia. Il riferimento, ad esempio, va a realtà quali *Ebay*, per *l'e-commerce*, *Facebook*, per il *Social Networking, Google* e *Yahoo* quali *search engine, YouTube* per la diffusione di contenuti audiovisivi, realtà che, già esse sole, sono destinatarie di una quota rilevante di accessi alla rete.

Quanto sopra, comporta diversi problemi sotto il profilo dell'applicabilità delle normative interne, o comunitarie ed, in tema di *enforcement*, in ordine alla stessa sussistenza di giurisdizione.

Sotto quest'ultimo profilo, con specifico riguardo alle condotte contraffattive realizzate a mezzo *internet*, attraverso l'accessibilità di contenuti illeciti ai navigatori di un paese diverso da quello in cui è collocato il *server,* la Corte europea, nel caso *L'Orèa*l c. *Ebay*[14], ha stabilito, quale criterio dirimente in ordine alla sussistenza dell'obbligo di conformarsi alla normativa dell'Unione, l'integrazione dell'evidenza che "*l'offerta in vendita del prodotto contrassegnato da un marchio che si trova in uno Stato terzo è destinata a consumatori che si trovano nel territorio per il quale il marchio è stato registrato*».

E' bene anticipare, però, che nella suddetta ipotesi esaminata dalla Corte UE, l'illiceità della condotta di usurpazione di marchio, con conseguente asseverazione alla normativa comunitaria, è stata ritenuta sussistente solo in capo all'inserzionista, mentre la posizione del *provider "deve essere esaminata nella prospettiva……della direttiva 2000/31…in particolare…alla sezione…che riguarda la 'responsabilità dei prestatori intermediari nel commercio elettronico",* il che riconduce alla problematica già evidenziata in ordine all'art 16 lett b) del Dlgs 2003/70[15], di cui si dirà meglio nel prosieguo del presente lavoro.

Ciò premesso, ritornando al tema della comunicazione di informazioni da parte degli *ISP*, possono evidenziarsi due ostacoli che, allo stato, si frappongono, quantomeno a fronte delle richieste provenienti direttamente dalla parte lesa, e non dalle Autorità.

[14] C.Giust, UE, 12.7.2011, causa C-324/09

[15] in forza della quale l'*ISP* "*non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore…non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita*" e "*…non appena a conoscenza di tali fatti,* ***su comunicazione delle autorità competenti****, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*

Al riguardo, è bene evidenziare che la possibilità che la parte privata compia, in autonomia - anche in previsione di un successivo intervento delle Autorità alle quali potranno essere fornite informazioni più complete circa la fattispecie illecita ed i suoi autori, rendendo possibile un intervento più celere ed incisivo – attività di auto-tutela dei propri diritti lesi, nell'ambito del contrasto alla contraffazione *online*, non può in alcun modo riguardarsi quale secondaria, essendo invece, l'auto-tutela in via stragiudiziale, il rimedio più celere e di minor costo sociale.

Un primo ostacolo – frequentemente riscontrato nell'esperienza pratica di chi scrive – è la negazione *sic et simpliciter*, da parte dell'*ISP*, della sussistenza in capo al medesimo, dell'obbligo di attenersi alla normativa interna italiana, in tema di tutela della riservatezza dei dati (Dlgs. 196/03) ove è disciplinato il regime della comunicabilità dei dati degli utenti e degli esoneri di responsabilità in capo al comunicante.

Per fare un esempio su tutti, il più noto ed utilizzato *search engine*, *Google*, solo a seguito della acquisizione massiva di foto ritraenti il territorio nazionale italiano, nell'ambito del lancio del servizio *Street View*, ha ricevuto un ordine[16] da parte dell'Autorità Garante dei Dati Personali Italiana finalizzato alla individuazione, da parte della medesima *Google*, di un rappresentate stabilito nel territorio dello Stato italiano[17], successivamente individuato, da *Google Inc.*, nella controllata *Google Italy Srl.*

Successivamente, la medesima *Google* – in accordo al principio fissato dalla Corte UE, di cui più sopra, del criterio della "destinazione" verso il territorio comunitario con conseguente applicabilità della normativa – si è conformata tanto a successive prescrizioni della Autorità Garante italiana[18], quanto ad importanti pronunzie della Corte Europea, quale ad esempio quella in tema di c.d. "diritto all'oblio"[19].

E' bene evidenziare, che in tema di contrasto alla contraffazione ed alla pirateria, il ruolo del *search engine* è tutt'altro che marginale, considerando che la presenza negli

[16] provvedimento Autorità Garante per la protezione dei Dati Personali n. 1759972 del 15 ottobre 2010
[17] art 5 lett b) Dlgs 196/03
[18] Autorità Garante per la Protezione dei Dati Personali – doc. n. 3738244 - Approvazione protocollo di verifica che disciplina le attività di controllo da parte del Garante sulle prescrizioni impartite a *Google* il 10 luglio 2015 – 22 gennaio 2015
[19] Corte di Giustizia UE, sez. grande, sentenza 13/05/2014 n° C-131/12.

indici di ricerca del medesimo costituisce, senz'altro, la miglior garanzia di raggiungibilità di un qualsiasi contenuto *web*, ivi compresi quelli aventi natura usurpativa.

Nello specifico, poi, della violazione di diritti di proprietà intellettuali relativi contenuti multimediali audiovisivi, assumono rilievo centrale realtà quali *YouTube* – facente capo anch'essa a *Google Inc* - che, notoriamente, ha resistito in un procedimento civile intentato nei suoi riguardi, innanzi il Tribunale di Roma, da *Mediaset S.p.a.* e finalizzato alla rimozione di contenuti audiovisivi della predetta *Mediaset*, tutelati dal diritto d'autore, dal portale *YouTube*.[20]

Giova evidenziare, infine, che l'assoggettamento effettuato da parte di *Google Inc.* alla normativa italiana e comunitaria, ha riguardato e riguarda solo i servizi offerti nelle lingue europee ed attraverso nomi dominio recanti estensioni geografiche europee (es. .it. .fr. es.) rimanendone al di fuori tutti quelli offerti direttamente da *Goole Inc.* attraverso il dominio *Google.com*.[21]

Per altro, in via incidentale, è bene evidenziare che le "modalità" attraverso le quali *Google* ha inteso conformarsi alla statuizione della Corte Europea in tema di oblio, destano non poche "preoccupazioni" – di cui si dirà meglio in prosieguo del presente lavoro - e sollevano potenti interrogativi in ordine al regime attuale di *governance* della rete e di volontà degli Stati di mantenere la propria autorità di fronte ad imponenti *corporation* private.

E' apparso subito evidente, difatti, come l'aver la Corte stabilito il principio che il *search engine* è responsabile per il mantenimento nell'indice di "*contenuti non più attuali*" o "*non più pertinenti*", con conseguente possibilità degli utenti di indirizzare, con banale attività stragiudiziale, eventuali richieste di rimozione direttamente al *search engine*, è stato interpretato da *Google* come l'essere investito del ruolo di "*arbitro privato della privacy*"[22]

[20] Tribunale di Roma – Reti Televisive italiane Sp.a. c. *YouTube Inc*, 29 ottobre 2009 r.g. 54218/08

[21] cfr. *The Advisory Council of Google – Report on the right to be Forgotten* – 5.5. *Geographic scope for delisting*

[22] "Diritto all'Oblio, *Google* dice no all'Europa"
L'Espresso, 28.09.2015 - http://espresso.repubblica.it/visioni/tecnologia/2015/08/26/news/diritto-all-oblio-google-dice-no-all-europa-1.226321

Alla pronuncia della Corte, difatti, è seguita da parte di *Google,* invece della mera ricerca, a fronte di eventuali richieste di rimozione, di elementi di verifica della fondatezza della richiesta, alla luce dei normali criteri di diligenza già previsti dalle leggi (es. nel nostro ordinamento agli art. 2043 c.c. e 1176 c.c.) e degli indici normativi e giurisprudenziali già esistenti, l'istituzione di un vero e proprio "comitato consultivo"[23] di esperti – che ha svolto anche "audizioni" pubbliche, quasi come fosse un organo statuale, per un lungo periodo, in vari luoghi d'Europa – al fine di decidere, essa stessa, i criteri applicabili.[24]

Il ruolo di *Google* - e di realtà affini - per altro, ai fini di interesse del presente lavoro, è da ritenersi centrale poiché oltre alle funzioni di *search engine* in senso classico, fanno capo alla medesima servizi quali *Blogger*[25], la già citata *YouTube, Google+*[26], tutte realtà attraverso le quali è possibile usufruire di spazi *web* – collocati su *server* al di fuori del territorio nazionale e comunitario – ed identificati da un dominio di terzo livello, il che rende impossibile identificarne il titolare attraverso la consultazione dei *data base* dei nomi a dominio[27] .

In tale scenario, di incerto riconoscimento da parte dei suddetti *player internet* della normativa e della giurisdizione interna e comunitaria, merita un cenno, in chiave comparativa, la nuove legge della Federazione Russa[28] in materia di protezione dei dati personali in seno alla quale, rigettando il principio del *safe harbor*[29], vengono fissati rigidi paletti in ordine alla possibilità delle *net company* estere di operare sul territorio nazionale.

In particolare, la suddetta, recente, normativa impone alle società estere che vogliano indirizzare servizi in lingua russa, o comunque verso i cittadini russi (es. nell'ambito di attività di *e-commerce)* che la "*registrazione, la sistematizzazione, il*

[23] https://www.google.com/advisorycouncil/

[24] "Diritto all'oblio e *Google*, un primo bilancio" - A. Caristi - *http://www.medialaws.eu/diritto-alloblio-e-google-un-primo-bilancio/*

[25] Piattaforma di personal *blogging* che consente all'utente di creare un sito sotto il dominio "www.nomeutente.bogger.com". E' evidente che un nome a dominio così formulato si sottrarrà alla possibilità di attribuirne la paternità attraverso le interrogazioni *whois* ed i dati dell'intestatario non potranno che essere comunicati dalla stessa *Google.*

[26] Piattaforma di *Social Neteworking* di Google.

[27] Per i domini ".it " accessibile all'indirizzo web: www.nic.it

[28] *Legge Federale russa n. 242 del 21 luglio 2014 – entrata in vigore il 1 settembre 2015*

[29] il c.d. *Safe Harbor* è un accordo in forza del quale può ritenersi lecito il trasferimento di dati transnazionale. In particolare, di recente, la Corte Europea ha dichiarato dichiarazione comunitaria di adeguatezza del livello di protezione garantito dalle organizzazioni aventi sede negli Stati Uniti d'America ed aderenti al c.d. accordo del "*Safe Harbor*",

salvataggio, l'archiviazione, l'aggiornamento e il recupero dei dati personali dei cittadini russi debbano essere effettuati solo in database situati nello Stato Russo".

Al riguardo, va evidenziato che, a fronte di provvedimenti normativi finalizzati ad una piena "sottomissione" degli operatori di *internet* alla sovranità statuale, il rischio paventato tra gli interpreti è quello di una "fuga" dei maggiori operatori da quei mercati che impongano regole troppo stringenti.

In riferimento all'ipotesi sopra citata, della nuove legge Federale Russa in materia di localizzazione di dati, deve evidenziarsi che, allo stato, non si registrano fenomeni di abbandono del mercato russo da parte degli operatori e, d'altronde, mercati di grandi dimensioni, quale appunto quello costituito dalla Federazione russa, o quale la stessa UE certamente è, difficilmente potrebbero *sic et simpliciter* essere abbandonati dai grandi *player* della rete senza che ne subissero essi stessi un nocumento.

Una volta delineato il superiore quadro di incerta applicabilità della normativa nazionale, ed essendosi già evidenziata la "riluttanza" dei principali *player* della rete a conformarsi *sic et simpliciter* alle normative statuali – in un evidente "braccio di ferro" per la sovranità, che riguarda non solo l'esempio sopra esaminato di *Google*, ma anche realtà quali *Facebook*[30] e gli altri grandi *player* della rete - è possibile evidenziare il secondo ostacolo (essendo il primo ostacolo, come già detto, costituito da un "precario" riconoscimento della legislazione e della giurisdizione interne) che, comunque, si incontra richiedendo, privatamente, agli *ISP* informazioni circa l'identità dei propri utenti al fine di tutelare un diritto.

Al riguardo è bene evidenziare che a differenza di *Google* – che si conforma, seppur con le limitazioni ed i profili problematici già evidenziati alle normative comunitarie, ma mantiene il principale centro di imputazione delle proprie attività negli Stati Uniti d'America – società quali ad esempio *Facebook* o *Yahoo*, hanno proprie articolazioni europee o italiane, costituite rispettivamente da *Facebook Ireland Ltd* e *Yahoo italia Srl* (la quale, comunque fa da tramite verso *Yahoo Ireland Ltd*), le quali, ordinariamente, riscontrano eventuali richieste di comunicazione di dati in conformità alla normativa italiana e/o europea.

[30] causa c-362714 *Maximillian Schrems / Data Protection Commissioner*

Orbene, in base all'esperienza professionale di chi scrive, è possibile affermare che ogni richiesta indirizzata ad un *ISP* – anche a quelli nazionali - finalizzata alla comunicazione di dati dei propri utenti al fine di tutelare un diritto, viene riscontrata negativamente sull'assunto che l'*ISP* "*non ha diritto di comunicare a terzi richiedenti i dati dei propri utenti, ma di avere al contrario un preciso obbligo a non fare nulla in questo senso, salva diversa disposizione delle Autorità.*"[31]

Il superiore assunto, esemplificativo di un indirizzo generalizzato, ad avviso del sottoscritto è ascrivibile alla **infelice formulazione** dell'art. 24 lett f) del Dlgs. 196/2033 ("*casi nei quali può essere effettuato il trattamento senza il consenso*") il quale dispone che "*il consenso non è richiesto quando il trattamento … con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento …".*

Il primo profilo di problematicità della suddetta norma è costituito dalla circostanza che la stessa configura una **facoltà** ("*casi nei quali **può** essere effettuato il trattamento senza consenso*") ma non istituisce un **obbligo**, in capo al titolare del trattamento, di comunicare i dati quando necessari a fini di investigazione difensiva – che, è bene ricordare, può anche essere "preventiva"[32] - o, comunque, di tutelare un diritto in giudizio.

In secondo luogo, la non esatta comprensione dei termini tecnici utilizzati in seno al Dlgs. 196/2033, quali "trattamento", "diffusione", "comunicazione" – pur se definiti all'art 4 ("definizioni") - ha condotto, spesso, da parte dell'*ISP,* ad interpretazioni fuorvianti di quanto disposto dall'art 24 let f) del Dgls. 196/03.

[31] dalla comparsa di costituzione di un *ISP* in giudizio afferente la comunicazione a terzi di dati dei propri utenti al fine di far valere un diritto.

[32] Art. 391-nonies. C.p.p (Attività investigativa preventiva. "1. L'attività investigativa prevista dall'articolo 327-bis, con esclusione degli atti che richiedono l'autorizzazione o l'intervento dell'autorità giudiziaria, può essere svolta anche dal difensore che ha ricevuto apposito mandato per l'eventualità che si instauri un procedimento penale.2. Il mandato è rilasciato con sottoscrizione autenticata e contiene la nomina del difensore e l'indicazione dei fatti ai quali si riferisce."). La norma no specifica se il procedimento debba riguardare l'indagato o la persona offesa dal reato e, pertanto, deve ritenersi possano validamente conferire mandato in tal senso anche le persone offese dal reato al fine di acquisire ogni elemento utile a dimostrare la sussistenza del medesimo.

E' stato sostenuto, difatti, da parte di un *ISP*, nel denegare la comunicazione alla parte lesa di dati dei propri utenti che: "*il riferimento all'art 24 lettera f) del Codice per la protezione dei dati personali è del tutto inconferente in quanto riguarda l'ipotesi completamente diversa in cui, al fine di una propria tutela azionata o da azionarsi in sede giudiziale, il titolare del trattamento dei dati utilizza i medesimi dati senza avere ottenuto il preventivo consenso del soggetto cui dati si riferiscono*"[33] e cioè, in altri termini, al solo fine di tutelare un diritto leso del medesimo *ISP* titolare del trattamento.

Quanto sopra è avulso da ogni lettura reale della norma. In primo luogo, la stessa è rubricata "*Casi nei quali può essere effettuato il trattamento senza consenso*" ed il termine trattamento, così come definito al precedente articolo 4 del medesimo Codice, include "*la comunicazione*" la quale, a sua volta, è definita al medesimo articolo come "*il dare conoscenza dei dati personali a* ***uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati****, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*".

In secondo luogo è esplicito nel dettato dell"art 24 lettera f) del Codice per la protezione dei dati personali il riferimento facultizzante allo "*svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397".*

Proprio quest'ultimo riferimento all'attività di investigazione difensiva, consente di riferire di un'altra, singolare, interpretazione della norma effettuata dagli *ISP*. Si ritiene, difatti, che possano, eventualmente, essere riscontrare, anche senza il preventivo "filtro" dell'Autorità Giudiziaria, le sole richieste provenienti dal difensore dell'indagato, e non già quelle provenienti dal difensore della potenziale persona offesa che esplichi attività di indagine difensiva alla ricerca di elementi a sostengo di eventuali notizie di reato.

Riguardo tutto quanto precede, non vi è chi non veda come – sia in tema di contrasto alla contraffazione *online* sia, più in generale in ordine alla tutela da tutti gli illeciti perpetrabili a mezzo *internet* – dovrebbe esservi il massimo interesse sociale affinché le parti direttamente interessate – come per altro avviene in ogni altro

[33] dalla comparsa di costituzione di un *ISP* in giudizio afferente la comunicazione a terzi di dati dei propri utenti al fine di far valere un diritto.

ambito dell'ordinamento – possano, anche autonomamente, attivarsi al fine di tutelare i propri diritti ed acquisire gli elementi utili a sostegno delle proprie ragioni.

In ambito *internet*, tale esigenza diventa ancor più pregnante in considerazione della circostanza che, differentemente da altri ambiti della vita sociale, la maggior parte delle attività vi avviene in forma, almeno *prima facie*, anonima.

Al riguardo, è bene evidenziare che in nessun modo, ed in nessun luogo dell'ordinamento, l'anonimato è riguardato quale un valore da preservare.

Al contrario, sono numerosi gli indici normativi che riguardano con forte sfavore le attività compiute in forma anonima, che si tratti della proposizione di una denuncia all'Autorità Giudiziaria, della quale non può difatti farsi utilizzo[34], al circolare per le strade col volto travisato, piuttosto che all'obbligo, sussistente in capo ad ogni cittadino, di recare sempre con sé un documento d'identità potendo, in casso contrario, essere persino trattenuto fino a ventiquattro ore, per fini identificativi, dalle Forze dell'ordine.

Per altro, il concetto cui in dottrina e nella stampa, ci si riferisce a difesa dello *staus quo* esistente, è quello della "libera accessibilità ad una rete aperta", oltre che della libertà di espressione e manifestazione del pensiero (art. 21 Cost.).

Al riguardo, è bene evidenziare che chi scrive dissente fortemente da una tale impostazione del problema dell'anonimato in rete. In primo luogo, il diritto alla libera manifestazione del pensiero, non ha mai – e non ha, allo stato, al di fuori della rete – tutelato la manifestazione "in forma anonima" di qualsivoglia pensiero. Al contrario, anche al di fuori delle stringenti regole vigenti nell'ambito dell'editoria - ove si prevede, tutt'ora, la responsabilità oggettiva, per omesso controllo, del direttore di una pubblicazione - l'ordinamento ha sempre visto con particolare favore l'attribuibilità di qualsivoglia esternazione ad un soggetto determinato o determinabile.

Analogamente, non si vede come il non poter operare in forma anonima possa costituire una compressione o compromissione del "libero accesso alla rete". Non vi è

[34] Artt 330 e 240 c.p.p.

chi non veda come, sulla rete come in ogni altro ambito sociale, si è responsabili delle proprie azioni e, seppur identificati od identificabili, nulla si teme, o si deve temere, se non si compiono attività antigiuridiche, né più né meno che nelle ordinarie attività di vita *offline*.

In tale ottica, ed in piena armonia col complesso dell'ordinamento, **potrebbe, pertanto, valutarsi una riformulazione del disposto di cui al suddetto art. 24 del Codice per la protezione dei dati personali, nel senso di mutare la facoltà, attribuita al titolare del trattamento (nella specie di interesse, gli *ISP*) in un** obbligo di comunicazione, nelle ipotesi già previste di necessità di far valere un diritto in giudizio ovvero - ma l'una ipotesi è funzionale all'altra - al fine di compiere attività di investigazione difensiva, in tutti i casi che appaiano non manifestamente infondati.

Per altro, sebbene con solo riferimento specifico agli operatori di *e-commerce*, la stessa Corte Europea ha già evidenziato che: "*se è certamente necessario rispettare la protezione dei dati personali, resta pur sempre il fatto che, quando agisce nel commercio e non nella vita privata, l'autore della violazione deve essere chiaramente identificabile*".[35]

Come di vedrà meglio in prosieguo, però, il nodo dell'identificabilità dell'utente *internet* è di più vasta portata ed investe ogni potenziale condotta illecita, anche al di là dell'ambito dell'*e-commerce* e del contrasto alla contraffazione ed alla pirateria *online.*

Parimenti, in ottica *de jure condendo*, il superiore obbligo ipotizzato dovrebbe essere accompagnato, con riferimento alle richieste finalizzate alo svolgimento di attività di investigazione difensiva, alla specifica indicazione della circostanza che lo stesso sussiste anche in caso di investigazioni difensive preventive nell'interesse della parte lesa.

Chiaramente, la previsione di un siffatto obbligo, **non potrà fare insorgere alcun automatismo tra la formulazione della richiesta ed il suo**

[35] C. Giust. UE, 12.7.2011, punti 135-144 della decisione.

eventuale riscontro positivo, con buona pace di polemiche[36] già sollevate da parte del "popolo della rete"[37] in ordine ad una proposta di novella, di segno simile ma non coincidente con quella sopra formulata, in relazione, però al già citato art. 16 del Dlgs 70/2003, articolo di cui si è in parte già detto e di cui si dirà meglio in prosieguo.

Già in seno al Piano Nazionale Anti Contraffazione, difatti, si era individuata l'urgenza e la necessità di "*adeguare anche la nostra legislazione interna (in particolare il Decreto Legislativo 9 aprile 2003 n. 70 di attuazione della Dir. 31/2000/CE), allo scopo di fornire una tutela effettiva contro ogni attività che venga ad interferire con ciò che i diritti IP concretamente rappresentano nella realtà economica e sociale. In tal modo garantendo un equilibrio di interessi che non penalizzi oltre il necessario i gestori dei servizi web e che nello stesso tempo protegga le imprese contro confondibilità e parassitismo, e gli utenti contro ogni inganno e ogni pregiudizio alla loro salute e alla loro libertà di scelta.*"

Tale necessità di adeguamento, in particolare, si era tradotta nella proposta di legge n. 5524 del 20 maggio 2012 di "*Modifica degli articoli 16 e 17 del decreto legislativo 9 aprile 2003, n. 70, in materia di responsabilità e di obblighi dei prestatori di servizi della società dell'informazione*"

In particolare, nel suddetto progetto di novella,[38] si disponeva, con riferimento all'art 16 del Dlgs. 70/2003, che l'esenzione di responsabilità in capo all'*ISP* per eventuali contenuti illeciti operasse solo se il medesimo "*non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione,* ***avvalendosi a tal fine di tutte le informazioni di cui disponga, comprese quelle che gli sono state trasmesse dal titolare del diritto violato***".

La suddetta proposta di riforma è stata però ritirata, a seguito, anche, delle sollevazioni della stampa, che ha criticato aspramente il suddetto provvedimento, in

[36] "Polemica sulla legge anti-pirateria, versione italiana" – IlSole24ore – 23 gennaio 2012 -

[37] che, nella specie, ha avuto come "portavoce disinteressato" i maggiori *player* dell'internet mondiale cfr. Sole 24 ora articolo già citato: "*L'edizione in lingua inglese di Wikipedia ha deciso di manifestare il suo dissenso attraverso l'oscuramento per 24 ore delle sue pagine e ha trascinato con sé una lunga lista di sostenitori, come Google, Yahoo e altri.*"

[38] http://nuovo.camera.it/_dati/leg16/lavori/stampati/pdf/16PDL0060220.pdf

maniera anche molto vigorosa[39], presentando l'esplicitazione dell'obbligo da parte del *provider* di tener conto anche delle segnalazioni degli interessati, come un "bavaglio messo al web".

Ad avviso di chi scrive - pur consapevole di assumere una posizione "impopolare" - la maggior parte delle polemiche sollevate a fronte delle proposte di regolamentazione del *web* e, segnatamente, a quella di cui sopra, nascono da una profonda incomprensione dei meccanismi base di funzionamento dell'ordinamento.

A proposito del c.d. "emendamento Fava", ad esempio, si è detto con la massima serietà sulla stampa, che lo stesso costituiva un'"*inaccettabile forma di privatizzazione della giustizia*" nonché definendolo "*Irresponsabile, anacronistico, anti-europeo e liberticida*"[40].

In realtà, lungi dal "privatizzare la giustizia" il suddetto emendamento tentava di ovviare – con equo bilanciamento degli interessi in campo, ma con tecnica normativa incerta - ad un "privilegio" concesso agli *ISP* dall'art. 16 del Dlgs. 70/2003 e tutt'ora in vigore ove si afferma, come già accennato ad inizio di questo lavoro, che l'esenzione di responsabilità in favore dell'*ISP* opera se "*agisca immediatamente per rimuovere le informazione, su* ***comunicazione delle autorità competenti***".

Per altro, è opportuno evidenziare che la suddetta circostanza ("comunicazione delle autorità competenti) a rigore esorbita dalla Delega conferita al Governo con legge delega 1 marzo 2002, n. 39 .

Difatti, in seno alla suddetta legge delega, il Governo viene invitato, a disciplinare la responsabilità dei prestatori con riferimento all'attività cosiddetta di "*hosting*" attenendosi al principio e criterio direttivo che "*il prestatore non sarà considerato responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che egli…non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*"[41]

[39] "La Lega nord prova a mettere il bavaglio al web" – il Fatto Quotidiano – 20 gennaio 2012 - http://www.ilfattoquotidiano.it/2012/01/20/fava-sopa-italiana-nuovo-bavaglio-titolo-bozza/185352/

[40] "Sopa Italiano – La legge che minaccia il web" il Fatto Quotidiano 222 gennaio 2012

[41] Art. 31 legge delega 1 marzo 2002, n. 39 .

Non vi è chi non veda, pertanto, come la legge delega non contenesse alcun riferimento alla necessità che la rimozione di contenuti dei quali sia, comunque, nota l'illiceità avvenga solo *"su comunicazione dell'autorità*".

Al riguardo, è bene sgomberare il campo da un "equivoco" – che fa il paio con l'atteggiamento di *Google* di tema di diritto ad oblio, che lo induce ad istituire un "Comitato Consultivo" ed a ritenersi "arbitro privato" della fattispecie - e cioè che, nel nostro ordinamento, non rientri nelle generali facoltà di ognuno – ed in relazione ad ogni fattispecie ipotizzabile – il richiedere, già in via stragiudiziale, la tutela dei propri diritti indirizzandone richiesta all'autore della lesione od a chi, comunque, abbia un obbligo giuridico di attivarsi.

Per chiarire meglio quanto sopra esposto, sarà bene precisare - tornando, a titolo di esempio, alla condanna comminata a *Google* dalla Corte Europea in tema di oblio - come la Corte non abbia affatto "demandato " *Google* di individuare in autonomia quali richieste dei privati accogliere o respingere e non l'abbia affatto costituito quale "arbitro privato" della fattispecie.

Parimenti, la Corte non ha attribuito agli utenti nessun "diritto di censura " – come pure paventato dalla stampa – in merito al contenuto degli indici di ricerca del *search engine*, né li ha fatti destinatari di un diritto di ottenere, in via indiscriminata, la rimozione, a piacere, di contenuti.

Molto più prosaicamente, la Corte ha ritenuto *Google* responsabile per la pubblicazione nel proprio indice di contenuti non più attuali o continenti.

In altri termini – come conforme al normale schema di funzionamento degli ordinamenti giuridici - la Corte ha **riconosciuto un diritto** (nella specie quello del ricorrente Signor *Gonzales* ad ottenere da *Google* la rimozione dall'indice di una vecchia notizia di stampa che lo riguardava) parimenti riconoscendo, in capo a *Google*, la sussistenza del **corrispettivo obbligo** di provvedere alla rimozione.

E', difatti, nozione base del diritto che alla posizione giuridica soggettiva di diritto (potere) di un soggetto, non possa che corrispondere quella di dovere di un altro soggetto.

In altri termini, la Corte non ha addossato a *Google* l'obbligo di attivarsi – e decidere in autonomia – a seguito di ogni richiesta proveniente da un privato.

Difatti, è bene evidenziare che, in linea generale – ed in ogni ambito della vita sociale od economica – l'opportunità di attivarsi o meno a fronte di una richiesta stragiudiziale è già codificata, in linea generale e per giurisprudenza più che consolidata, nel nostro ordinamento, dal combinato disposto articoli 40 c.p. ("*non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo*") e 2043 c.c. ("*ogni fatto doloso o colposo che cagiona ad altri un danno ingiusto obbliga colui che ha commesso il fatto a risarcire il danno*").

E' di tutta evidenza, pertanto, che una volta definita – da una norma o da una norma così come interpretata da una Corte di ultima istanza - l'antigiuridicità ed illiceità di una condotta (es. il mantenere nell'indice di ricerca un contenuto obsoleto), la conseguente posizione soggettiva di dovere (l'obbligo in capo al motore di ricerca di rimuovere i contenuti obsoleti) e la corrispettiva posizione di diritto, e quindi di potere (es. il diritto del Signor *Gonzales* ad ottenere la rimozione dell'articolo) il dare seguito o meno ad una istanza stragiudiziale costituisca una mera valutazione di opportunità in capo al destinatario, da compiersi in base al parametro, già anch'esso codificato, di cui all'art 1176 c.c. (diligenza nell'adempimento delle obbligazioni).

Analogamente, il già citato "emendamento" Fava, non aveva istituito il diritto del privato di ottenere la rimozione dei contenuti asseritamene illeciti, *sic et simpliciter*. Aveva, semmai, posto rimedio ad un "privilegio" – "nascosto" nelle pieghe dell'art. 16 del Dlgs 70/2003 – ove tanto l'obbligo generale di cui all'art 40 c.p. quanto quello speciale di cui allo stesso Dlgs. 70/2003 *("..non è responsabile… purchè non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita*" *ergo,* se ne è a conoscenza è responsabile) sono subordinati all'essere avvenuta una "**comunicazione delle autorità competenti**".

Deve evidenziarsi, difatti, che la norma in questione tipizza tre ipotesi distinte, in relazione a tre fattispecie parimenti differenti, in ordine al verificarsi delle quali l'*ISP* può andare esente da responsabilità.

La prima è che "*non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita*" (art. 16 Dlgs, 70/2033 lett a) senza che nulla venga detto dal legislatore circa quale debba essere la fonte di tale conoscenza (ad es. l'Autorità piuttosto che il danneggiato stesso)

La seconda fattispecie, limitata a "*per quanto attiene ad azioni risarcitorie"* è che *" non sia al corrente di fatti o circostanze che rendono* ***manifesta*** *l'illicetià dell'attività o dell'informazione*". Ai fini risarcitori, pertanto, non è sufficiente che l'*ISP* sia a conoscenza dell'illiceità, ma è necessario anche che questa sia **manifesta.**

A rigore quindi, in astratto, in base al suddetto articolato normativo, chi lamentasse la illiceità di un contenuto *web*, allegando all'*ISP* elementi tali da rendergli nota la predetta illiceità, ma non tali da farla apparire "manifestamente" nota - residuando, in ipotesi, elementi di dubbio, al riguardo - potrebbe veder riconoscere la responsabilità dell*'ISP*, ma non ottenere il risarcimento del danno.

La terza ipotesi, invece, disciplina il **diverso obbligo di rimuovere i contenuti**, il quale si ingenera in capo all'*ISP* solo "su comunicazione dell'Autorità".

E' bene precisare, che è proprio il suddetto inciso "su comunicazione delle autorità competenti" a costituire la seconda eccezione allo schema generale ordinamentale in materia di responsabilità, essendo la prima costituita dal già evidenziato requisito della "manifesta illiceità" in ordine alla sussistenza di responsabilità risarcitorie.

E' bene ribadire, di fatti, che il Dlgs. 70/2003 – con riferimento, almeno, alle attività di *caching* ed *hosting providing*, e parziale esclusione di quelle di *mere conduit* – non esclude affatto la responsabilità dell'*ISP* che sia a conoscenza dell'illiceità del contenuto *web* (e difatti gli articoli 15 e 16 sono rubricati quali "Responsabilità nell'attività di…" e non già quali "Esclusione della Responsabilità .."), nulla dicendo circa la natura di questa fonte di conoscenza che, come normale che sia, per quanto già detto in precedenza può, pertanto, ben essere costituita dalle allegazioni della parte danneggiata.

In altri termini, la suddetta norma - con riferimento alla lettera b) dell'art 16 - è costruita come fosse il corrispettivo, inverso, di quelle che in diritto penale si

chiamano "condizioni obiettive di punibilità", laddove nelle predette ipotesi una condotta è sanzionabile solo al verificarsi di un "fatto esterno" estraneo alla sfera di controllo dell'agente, mentre nell'ipotesi di interesse, al contrario, è esclusa la sanzionabilità se, al verificarsi del fatto esterno (comunicazione delle autorità) si tiene una determinata condotta (rimuovere prontamente le informazioni o disabilitarne l'accesso).

Con buona pace di chi paventava "bavagli al *web*", pertanto, deve ritenersi che, già in base alla normativa attuale, l'*ISP*, anche qualora informato dal solo danneggiato dell'illiceità di un contenuto, versi già in posizione di responsabilità (con tutte le conseguenze che il *versari in re illicita* può comportare) e, qualora "manifestamente informato", sempre anche solo dallo stesso danneggiato, sia anche tenuto al risarcimento del danno.

In altri termini, l'assenza di una "comunicazione dell'autorità" solleva l'*ISP* **solo** dall'obbligo di rimuovere il contenuto illecito, eventualmente anche se gli sia già nota la predetta illiceità.

E' bene precisare, anche in base all'esperienza professionale diretta di chi scrive, che la predetta comunicazione delle autorità, sovente, non può essere ottenuta, e proprio perché l'autore del contenuto lesivo quasi mai è direttamente identificato od identificabile.

Il riferimento di cui sopra, è a fattispecie tangenti il tema della contraffazione, quali ad esempio gli atti di concorrenza sleale (2589 c.c.) che non includano profili penalistici. In assenza di profili di rilevo penale, difatti, non sarà possibile compulsare l'Autorità Giudiziaria affinchè proceda alle investigazioni necessarie all'identificazione dell'autore della condotta.

E' bene evidenziare, per altro, che le stesse investigazioni spesso incontrano un ostacolo insormontabile nella previsione di un limite di dodici mesi, dalla data della comunicazione, per la conservazione dei "*dati relativi al traffico telematico, esclusi i contenuti delle comunica*zionI" (art. 132 co. 1, D.lgs 196/2003) da parte del fornitore.

Difatti, il predetto arco temporale (12 mesi) risulta spesso incompatibile con le reali tempistiche delle indagini preliminari. Pertanto, In prospettiva *de jure* condendo, potrebbe essere opportuno innalzare il predetto limite temporale di conservazione, quantomeno allineandolo a quello già previsto per i dati relativi al traffico telefonico che, di contro, è già di 24 mesi.

Chi scrive ha patrocinato, innanzi il Tribunale di Milano, sezione specializzata in materia di proprietà industriale ed intellettuale, un delicato giudizio cautelare, in materia di concorrenza sleale, particolarmente rappresentativo del rischio reale e concreto che la rete, almeno in parte, permanga quale "porto franco" delle attività illecite, poiché risoltosi in un sostanziale "vuoto di tutela".

Il ricorrente, produttore e distributore in proprio di apparecchiature elettroniche lamentava che, celandosi dietro un *nick name,* un concorrente denigrasse la sua attività tramite messaggi pubblicati sulle piattaforme di due noti *ISP* di rilevo internazionale.

La fattispecie era particolarmente delicata poiché i messaggi di interesse potevano essere ritenuti denigratori, solo ove fosse stato accertato che provenissero effettivamente da un concorrente potendo, in caso contrario, essere continenti con il c.d. diritto di critica.

Essendo necessario acquisire la prova che il *nick* celasse l'identità del concorrente, si chiedeva agli *ISP* di comunicare i dati in loro possesso relativi all'utenza corrispondente al predetto *nick*, ricevendo rifiuto in forza delle note ragioni di cui si è detto in precedenza.

Veniva pertanto investito il Tribunale, con domanda cautelare d'urgenza, affinché ordinasse direttamente agli *ISP* la rimozione dei contenuti denigratori ovvero, in subordine, ordinasse agli *ISP* di comunicare i dati identificativi degli utenti autori dei messaggi denigratori, al fine di potere agire in giudizio nei loro confronti.

Il Tribunale, quindi, con "*decisio diabolica*" rigettava entrambe le richieste del ricorrente. La prima, avente ad oggetto la rimozione direttamente ad opera degli *ISP* dei messaggi denigratori poiché: "*al momento non è dato sapere se le… dichiarazioni*

provengano da un'impresa concorrente ovvero da un consumatore, precondizione per valutare l'eventuale valore anticoncorrenziale di queste opinioni". La richiesta relativa ad ottenere dei dati di registrazione degli autori dei messaggi denigratori, di contro, veniva rigettata poiché: "*la richiesta di accesso ai dati appare esplorativa*" poiché , allo stato "*le circostanze appaiono allo insufficienti a dimostrare il buon diritto della ricorrente*"[42]

In altri termini, per provare l'anticoncorrenzialità dei commenti pubblicati da utenti "anonimi" di un *ISP* sarebbe stato necessario essere certi che il *nick* corrispondesse all'identità di un concorrente. E, per acquisire la predetta certezza in ordine all'identità dell'utente, sarebbe stato necessario essere certi dell'anticoncorrenzialtà dei commenti.

Non vi è chi non veda come pericolosi "vuoti di tutela", quale quello di cui sopra, costituiscano anch'essi un serio "*ostacolo al commercio legittimo*", anche in ottica "*pro-concorrenziale*".

E' di tutta evidenza, difatti, come il mero collocamento sulle piattaforme di maggiore visibilità (es. frequentemente *Yahoo Answers, Ebay, Tripadvisor etc.*), con conseguente elevata indicizzazione e visibilità sui motori di ricerca, di una serie di messaggi denigratori, da parte di un concorrente che abbia l'accortezza di mantenere la critica entro limiti continenti (qualora provenisse da un reale consumatore) possa cagionare agevolmente, e per un lungo lasso di tempo, un severo danno all'immagine ed alla reputazione del concorrente *target*.

Con riferimento al Dlgs. 70/2003, poi, va formulata un'ultima osservazione, in ordine ad una ulteriore disposizione ivi contenuta che esula dagli schemi normativi ordinari ingenerando, spesso, effetti paradossali.

E' bene premettere che, nel nostro ordinamento, non esiste un obbligo generale, da parte dei privati, di denunziare i reati all'Autorità Giudiziaria. Contrariamente all'opinione comunemente diffusa, difatti, non ogni condotta di tolleranza inerte, a fronte della commissione di un reato, costituisce "favoreggiamento" essendo al contrario, il mero silenzio del privato qualificato come "connivenza" non punibile.

[42] Tribunale di Milano – Sez. specializzata in materia di P.I.I. – 28.12. 2011 – r.g. 61372/11

Al contrario, ordinariamente, i soli soggetti obbligati a riferire all'Autorità Giudiziaria, sono quei soggetti dotati di qualifiche di rilevo pubblicistico, se non sono Pubblici Ufficiali in senso assoluto, quali ad esempio gli agenti ed ufficiali di polizia giudiziaria, per i quali sussiste obbligo di denuncia, ed i medici del sistema sanitario nazionale, per i quali sussiste l'obbligo di referto.

In tale ambito di rigida perimetrazione dell'obbligo di segnalare gli illeciti all'autorità giudiziaria, l'art. 17 del predetto Dlgs. 70/2033 dispone che: "*il prestatore è comunque tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza qualora sia a conoscenza di presunte attività o informazioni illecite*".

Sotto un primo profilo, operativo, la predetta norma genera, nella prassi applicativa, alcune distorsioni. Difatti, per così come viene interpretata da alcuni *ISP* la suddetta norma, può capitare che segnalando, ad esempio, la presenza sui *server* dell'*ISP* di un contenuto diffamatorio*,* la segnalazione venga inoltrata, *sic et simpliciter*, dall'*ISP* alla Procura della Repubblica ed all'AGCOM.

Entrambe le suddette segnalazioni sono del tutto inutili, già sotto un mero profilo procedurale, poiché la diffamazione è reato procedibile a querela di parte e la Procura non potrebbe, comunque, né avviare un procedimento di iniziativa né sollecitare il danneggiato in tal senso ed, ugualmente, l'Agcom, non ha alcuna competenza in tema di diffamazione.

Sotto un profilo ermeneutico, di contro, la suddetta previsione dell'obbligo di segnalazione induce a due interessanti osservazioni.

In primo luogo - anche alla luce di quanto premesso in ordine all'assenza, se non in capo a soggetti ben determinati, di un obbligo generale di denuncia – poiché gli *ISP* sono destinatari di uno specifico obbligo in ordine alla segnalazione alle Autorità di illeciti dei quali siano a conoscenza, non può in alcun modo sostenersi un loro ruolo – anche al di fuori delle ipotesi di *mere conduit* - totalmente "neutro" rispetto a quanto avviene sulle proprie piattaforme.

In secondo luogo, poiché alla comunicazione all'Autorità sono tenuti essi stessi, è ben chiaro che, in tale ipotesi, possano "*essere a conoscenza di presunte attività o informazioni illecite*" solo se informati direttamente da terze parti.

Difatti, non dovendo esercitare un obbligo generale di sorveglianza dei contenuti (art. 17 del Dlgs. 70/2003), al di fuori dell'ipotesi della scoperta "fortuita" di un illecito – non rimane che la possibilità che siano stati informati direttamente da un terzo – verosimilmente lo stesso danneggiato - coerentemente con quanto già argomentato in ordine alle previsioni di cui agli artt. 15 e 16 del medesimo Dlgs. 70/2003.

Quanto precede sembra smentire clamorosamente i timori che la "novella" proposta dell'On. Fava aveva ingenerato nell'opinione pubblica. Già allo stato, difatti, l'ISP non può rimanere inerte a fronte delle segnalazioni di condotte illecite che gli provengano dagli interessati ma, al contrario, è fatto destinatario di un obbligo di segnalarle alla autorità.

Per altro, verrebbe da chiedere ai denigratori dell'emendamento Fava, se quindi l'*ISP*, allo stato, è "l'arbitro privato" delle segnalazioni da ritenersi contenenti notizie di "*presunte attività o informazioni illecite*" dovendo, pertanto, inoltrandole alle autorità. E non sarà, pertanto, l'Autorità subissata di richieste a sola iniziativa dei privati che, col mero inoltro all'*ISP,* si assicureranno l'attivarsi delle medesime?

In realtà, come già evidenziato in precedenza, l'*ISP* non dovrà far altro che formulare una valutazione, secondo diligenza, delle segnalazioni che gli pervengano inoltrando quelle sole che lascino presumere la sussistenza di ipotesi illecite.

Giova evidenziare, per altro, che se per la sussistenza della mera responsabilità è necessario che l'*ISP* "*sia a conoscenza del fatto che l'attività o l'informazione è illecita*", mentre per la sussistenza di profili risarcitori è necessario che l'illiceità sia "*manifesta*", ai fini della sussistenza dell'obbligo di segnalazione all'Autorità, invece, sarà sufficiente che sia a conoscenza di "*presunte*" attività illecite.

Non vi è chi non veda come il generale regime della responsabilità degli *ISP*, in seno al Dgls. 70/2003 sia fonte di confusione, senza per altro tradursi né in un efficace strumento di ausilio nel contrasto delle attività illecite, né lasciando esenti gli *ISP* da

compiti gravosi ed, in molti casi , privi di utilità pratica, quali l'obbligo di segnalare all'Autorità GIudiziaria o Amministrativa ogni illecito presunto – senza distinzione tra illeciti penali o meramente civili o anche amministrativi .

Di contro, In prospettiva *de jure condendo*, **appare opportuno limitare il suddetto obbligo ad un limitato catalogo di reati specificamente individuati.**

Per altro, anche il suddetto obbligo di comunicazione all'autorità dei contenuti presumibilmente illeciti, così come formulalo, esorbita dalle direttive e principi della legge delega, nella quale di contro si chiedeva al Governo delegato di "*disciplinare le modalità con le quali i prestatori di servizi delle società dell'informazione sono tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi*".

Un ultima precisazione giova formularsi in ordine alla qualifica, quali *hosting provider*, che i maggiori operatori della rete (*Ebay, Google, Facebook, YouTube* etc.) attribuiscono a loro stessi ed, allo stato, viene loro ordinariamente riconosciuta nelle decisioni giudiziarie che li hanno riguardati.

E' già stato detto, che la sussistenza della predetta qualifica – in alternativa a quella, più gravosa in termini di obblighi e responsabilità dirette, di *content porvider* – è subordinata al verificarsi delle circostanze che il *provider* "*non effettui una produzione propria di contenuti, non faccia selezioni nel destinarlo e non metta in atto operazioni di filtraggio".*

Al riguardo, non può non evidenziarsi come la maggior parte dei servizi di "*memorizzazione di informazioni a richiesta di un destinatario del servizio"* siano forniti dietro accettazione, da parte dell'utente, di stringenti *policy* e condizioni di utilizzo[43], le quali prevedono una regolamentazione puntigliosa di ciò che è pubblicabile, ad avviso del gestore del servizio, ed includono sovente la possibilità di essere esclusi unilateralmente dal sistema, oltre a comportare, nella maggior parte

[43] A titolo esemplificativo, si veda "l'accordo per gli utenti" di *Ebay* ove vengono minuziosamente regolamentate le attività esperibili dai medesimi. Addirittura, nel predetto accordo, si prevede che: "*Quando fornisci ad eBay dei contenuti, concedi ad eBay una licenza d'uso perpetua, irrevocabile, senza limiti territoriali, a titolo gratuito e trasferibile (a più livelli) dei diritti d'autore, dei diritti di pubblicazione e dei diritti sulle banche dati di cui sei titolare in relazione a tali contenuti, in qualsiasi formato già esistente o futuro.*" - http://pages.ebay.it/help/policies/user-agreement.html#condizionimessainvendita

delle ipotesi, una "cessione di licenza d'uso"[44] o della titolarità dei diritti di proprietà intellettuale, da parte dell'utente, in favore dell'*ISP*.

Quanto sopra è vero tanto per le maggiori piattaforme di vendita *online*, quanto per ogni altro servizio di diffusione di contenuti a richiesta dell'utente, ivi comprese le piattaforme che concedono spazio per la pubblicazione di *Blog*[45] o siti personali.

In altri termini, l'utente non è libero di pubblicare qualsiasi contenuto – o di tenere qualsivoglia condotta – all'interno della piattaforma della quale entri a far parte ma, al contrario, il gestore del servizio impone limiti, regole e, sovente, compie una "selezione" dei contenuti pubblicabili, in conformità alle proprie *policy.*

In altri termini, non è affatto corretto definire gli spazi di pubblicazione forniti dai maggiori operatori come "lavagne bianche" sulle quali l'utente possa pubblicare il contenuto che meglio creda e nei confronti dei quali il gestore rimanga "neutro" e ciò, in prospettiva di un'evoluzione giurisprudenziale – o di una chiarificazione normativa - potrebbe indurre a ritenere i predetti operatori non più quali *hosting provider* bensì quali veri e propri *content provider*, in ragione della loro non completa "neutralità" in ordine ai contenuti pubblicati dagli utenti.

E difatti, in almeno un caso giudiziario, che ha visto coinvolto un noto motore di ricerca in ordine al servizio di "suggerimento" nella ricerca[46], il Tribunale di Milano[47] ha ritenuto che, sebbene la selezione delle parole da associare alla chiave di ricerca fosse effettuato da un *software*, in automatico, il fatto stesso che vi fosse una selezione comportava la qualifica del gestore del servizio quale *content provider*.

[44] sempre con riferimento ad Ebay, ad esempio: "*Quando fornisci a eBay dei contenuti, concedi a eBay una licenza non esclusiva, valida in tutto il mondo, perpetua (o per la durata dei diritti d'autore o di altri diritti sui contenuti), irrevocabile, a titolo gratuito e trasferibile (a più livelli) per l'utilizzo dei contenuti (inclusi, a mero titolo esemplificativo, la creazione e utilizzo di lavori derivati) e ci autorizzi a esercitare e utilizzare i diritti d'autore, i diritti sui marchi i diritti di pubblicazione e dei diritti sulle banche dati di cui sei titolare in relazione a tali contenuti, in qualsiasi formato già esistente o futuro.*"

[45] A titolo d'esempio, si segnala che nei "termini si servizio" della piattaforma *Blogger*, si precisa che: "Blogger può adottare le seguenti misure: 1.Rimuovere i contenuti. 2. Inserire una pagina di avvertimento prima dei contenuti in questione 3.Informare gli autori e gli amministratori tramite email o un messaggio sulla loro bacheca di Blogger 4. Pubblicare un messaggio in cui si informa che i contenuti sono stati rimossi. 5. Fornire un link a una copia dell'avviso di rimozione

[46] Il servizio di suggerimento nella ricerca affianca, alla parola chiave inserita dall'utente, un elenco di parole corrispondenti alle ricerche di maggior volume effettuate in relazione alla parola chiave di interesse, così come individuate da un software in base a criteri predeterminati. Tale accostamento "automatico" ha più volte dato luogo ad associazioni tra le generalità di un soggetto, ad esempio, e termini quali truffa o arrestato che, all'evidenza, possono cagionare una lesione dell'immagine. Di conseguenza il servizio è stato oggetto di numerosi procedimenti giudiziari.

[47] Tribunale di Milano,ordinanza 21-25 gennaio 2011

Invero, il suddetto provvedimento veniva reclamato ed, in tale sede, il Tribunale riteneva che: "*è la scelta a monte e l'utilizzo di tale sistema e dei suoi particolari meccanismi di operatività a determinare – a valle - l'addebitabilità… dei risultati che il meccanismo così ideato produce, con la … conseguente responsabilità extracontrattuale*" con la conseguenza che*, tout court*, "*non è applicabile alla presente vicenda la normativa contenuta nel D. Lgs. n.70/03, che inserisce esclusivamente l'attività di memorizzazione di informazioni fornite da altri.*"[48]

Infine, ad indicare come la giurisprudenza in tema di responsabilità degli *ISP* sia tutt'altro che consolidata, con pronuncia del 2013 emessa in seguito ad un giudizio avente oggetto simile a quello di cui sopra, il Tribunale mutava ulteriormente orientamento, collocando il suddetto servizio di suggerimento nella ricerca nell'ambito, di contro, delle attività di *caching*[49], ritenendo, in particolare che "*il servizio in questione si qualifica quindi come mero servizio di caching, cioè di memorizzazione temporanea di informazioni fornite dagli stessi utenti, senza alcuna responsabilità in relazione al loro contenuto a norma dell'articolo 15 del D. Lgs 70/2003 (cd. Decreto E-commerce). Pertanto, prima di un'esplicita richiesta dell'autorità giudiziaria, e in assenza di un obbligo di filtraggio preventivo da parte degli ISP, il provider non aveva il dovere di rimuovere i risultati delle ricerche automatiche in esame, asseritamente lesivi*"[50].

Un altro ambito, di grande interesse in tema, in particolare, di contrasto alla pirateria audiovisiva, è quello delle tecnologie di trasmissione c.d. *peer to peer* che consentono la trasmissione di *file* direttamente tra utenti, anziché da un sito *web* all'utente.

Al riguardo, giova evidenziare la pronuncia con la quale la Corte di Cassazione[51] ha stabilito il principio che "*L'utilizzo di tecnologie di trasmissione peer-to-peer (quelle cioè che consentono il trasferimento di file direttamente tra utenti, anziché dal sito web all'utente) non esclude la configurabilità del reato di cui all'art. 171, comma 1, lett. A-bis, L.D.A. (che punisce l'attività di chi metta a disposizione del pubblico attraverso internet opere protette dal diritto d'autore) da parte del titolare del sito web. E ciò sebbene, attraverso la tecnologia in questione, il titolare del sito non "detenga" mai*

[48] Tribunale di Milano, ordinanza del 24 marzo 2011
[49] Art. 15 Dlgs. 70/2003
[50] Tribunale di Milano, ordinanza del 25 marzo 2013
[51] Corte di Cassazione - 9 settembre - 23 dicembre 2009, n. 49437 – The Pirate Bay

nei propri database l'opera protetta, che al contrario si trova presso gli utenti, e da questi stessi trasferita ad altri soggetti."

In altri termini, in riferimento ad un servizio quale il *peer-to-peer* che, a rigore, andrebbe qualificato, ai sensi del Dlgs. 70/2033 quale *mere conduit*, la Corte ha focalizzato l'attenzione, piuttosto che ai profili di responsabilità scaturenti dal predetto Dlgs. 70/2003 – che incontrano le già note limitazioni – sulla sussistenza, ex art. 110 c.p., di un vero e proprio concorso nel reato.

In particolare, il suddetto concorso, ad avviso della Corte, può essere integrato, da parte del titolare del sito *web* che offra servizi di *peer-to-peer* purché: "*non si limiti a mettere a disposizione degli utenti il protocollo di comunicazione peer-to-peer, ma faccia qualcosa di più, come ad esempio indicizzare le informazioni che provengono dagli utenti, rendendo più facile l'individuazione delle opere magari attraverso un motore di ricerca.*"

Quanto sopra, è in linea con quanto da noi già argomentato in ordine alle attività dei maggiori fornitori di servizi della rete, in relazioni alle quali si è già contestato che, in presenza di *policy* di utilizzo stringenti, possa correttamente definirsi la relativa attività quale di *hosting providing*.

E' bene evidenziare che, in un contesto tutt'altro che chiaro e definito e caratterizzato dalle ombre già evidenziate sin qui, le politiche di contrasto della contraffazione perpetrata a mezzo di siti gestiti da *ISP* terzi, da ultimo, si è indirizzata verso la stipula di "protocolli di intesa" tra le associazioni rappresentative di interessi tutelabili, o le stesse Autorità nazionali, e gli *ISP* fornitori dei servizi.

Il riferimento che precede, va, ad esempio, al recente protocollo stipulato – in occasione di EXPO Milano 2015 – tra il Ministero per le politiche agricole, alimentari e forestali ed *Ebay*, finalizzato alla "*valorizzazione e promozione settore vitivinicolo su Ebay*". Il predetto protocollo, in particolare, prevede l'impegno di *Ebay* a "*rimuovere gli annunci quando vengono riscontrate violazioni relative ai vini DOP e IGP*"[52]

[52] https://www.politicheagricole.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/8489

Iniziative quale quella di cui sopra, e delle quali non si nega in alcun modo l'efficacia e la necessità – in un quadro "emergenziale" e caratterizzato da numerose lacune di alcune delle quali si è riferito nel corso del presente lavoro – non possono essere riguardate, ad avviso di chi scrive, come ad una risoluzione definitiva delle problematiche connesse alla "resposansabilizzazione" degli *ISP*.

Se, da un conto, protocolli ed intese, tra le entità statuali e gli operatori privati esteri, garantiscono un canale di dialogo tra gli stessi e ben dispongono ai fini di eventuali azioni di *enforcement*, che potranno contare sull' auto-responsabilizzazione collaborativa degli *ISP*, non può non rilevarsi come tutto ciò finisca con l'essere affidato più ad un *good will* degli operatori stessi che non alla necessaria autoritatività ed imperatività che l'*enforcement* di diritti dovrebbe possedere per propria natura.

In altri termini, accordi e protocolli sono sempre revocabili, da parte del sottoscrittore, e non possono sostituire un quadro normativo certo, efficace e dotato di tutta la *vis impositiva* che, allo stato, solo le normative statuali, o comunitarie, possono avere.

3. Il nodo della *governance* di *internet*

Invero, sin dalle origini del *world wide web*, la gestione della rete è sempre stata allettata da "ambizioni autoregolative", in parte scaturenti dalla necessità di colmare le lacune normative generate dalla rapidità della diffusione delle connessioni, in parte originatasi da una visione "libertaria" della rete, in contrapposizione alla sovranità degli stati ed al processo normativo tradizionale.

In tale scia, l'allora Garante per la protezione dei dati personali Rodotà, in un suo articolo del 1998 relativo alla disciplina giuridica di *Internet* già affermava "*la necessità di mettere a punto una strumentazione adeguata alla nuova realtà che dev'essere regolata ... Nasce così la spinta verso forme di autodisciplina, verso un uso di strumenti contrattuali, che non hanno solo la funzione di colmare temporaneamente una lacuna, ma di identificare una diversa e più complessa strategia di regolazione*" con la conclusione che è "*l'integrazione delle fonti tradizionali esige l'intervento di discipline individuali (contratto) o di settore (codici di*

autoregolamentazione), che si presentano anche come la prima forma della disciplina giuridica (eventualmente in attesa di altre forme di intervento)".[53]

E' in tale ambito che, come accennato in apertura del presente lavoro, ha preso piede, in materia di regolamentazione della rete, l'idea di una *governance* sopranazionale della medesima, piuttosto che di una puntigliosa regolamentazione ancorata al tradizionale principio di territorialità.

Il concetto stesso di *governanc*e implica necessariamente un'azione non gerarchizzata di soggetti diversi e, per propria natura, non appare mai staticamente definibile ed assume, piuttosto, i tratti di un processo dal quale, man mano, possano evidenziarsi elementi di vaghezza e determinazione[54]

Caratterizzazione tipica della *governance*, difatti, è di essere un processo *multistakeholder*, finalizzato ad una rappresentanza il più possibile armonica di una pluralità di diversi interessi facenti capo a differentii soggetti.

Con la suddetta visione, fluida e globale della rete, però, convive una dimensione territoriale e statuale di livello locale. E' in atto, anzi, un parziale fenomeno di "zonizzazione" (*zoning*) della rete, con l'instaurarsi di vere proprie derivazioni nazionali, separate ed autonomamente caratterizzate in termini di contenuti, con il caso-limite costituito dalla Cina che, con la creazione del c.d. "*169 network*" ha istituito una vera e propria *enclave* nazionale di *internet*.[55]

Non può negarsi infine che agli Stati, singolarmente considerati, spetti ancora, in ultima analisi, il giudizio di bilanciamento finale tra la libertà dei contenuti della Rete ed i valori espressi dall'ordinamento territoriale.[56]

In seno alle Nazioni Unite, lo sforzo finalizzato al pervenire ad un modello di *governance* unitario della rete ha trovato concretizzazione nell'istituzione del *Working Group on internet governance* (WGIG), finalizzato all'istituzione di un tavolo stabile di elaborazione e discussione dei temi più rilevanti in materia.

[53] STEFANO RODOTÀ, *Anche il diritto insegue la società che corre, e cambia,* Telèma n. 11, 1998 http://www.fub.it/telema/TELEMA11/Telema11.html

[54] Andronico, 2009, 237

[55] Deibert, Palfrey et al. 2008)

[56] Benkler 200, 171

Un ulteriore istanza di dialogo, in seno al WGIG, è costituita dall'istituzione *dell'Internet Governance Forum*, concepito quale ulteriore istanza di dialogo e confronto rappresentativo e del quale, il 20 ottobre scorso, si è svolta la sessione italiana per i l 2015.[57]

Allo stato, quindi, il "governo" della rete continua ad essere sottoposto a due spinte opposte e di segno contrario. L'una "liquida"[58] tendente a una visione mai staticamente definibile che tende ad accantonare le forme più piene ed imperative del diritto in favore di un approccio *soft* ed autoregolativo.

La seconda ancorata alle tradizionali visioni di territorialità, statualità e certezza del diritto, riguardate come le sole che possano fornire effettiva tutela ed un quadro di valori stabili.

E' in tale ottica contraddittoria che si collocano provvedimenti quali l'adozione, da parte della Camera dei Deputati della "*Dichiarazione dei diritti di internet*" che, adottata con atto privo di collocazione nella gerarchia delle fonti, non può che avere una funzione di *moral suasion*, fungendo da eventuale criterio ermeneutica residuale, od, al più programmatica.[59]

Pur rispondendo all'intento, lodevole, di cristallizzare e fissare diritti che, altrimenti, rischierebbero di essere travolti dalla "liquidità" dell'attuale assetto della rete – soggetta, per altro, a continue evoluzioni tecniche cui la produzione normativa non riesce a tenere il passo - il suddetto atto non può, difatti, nell'attuale logica dell'ordinamento, essere sostitutivo di un atto normativo in senso pieno.

Non vi è chi non veda, per altro, la pericolosità intrinseca insita in una "abdicazione" di fatto dello Stato al suo ruolo di regolatore e garante dei conflitti, non potendo escludersi, laddove latiti il diritto che, piuttosto che istanze realmente democratiche e *multistakeholder*, si imponga la pura e semplice "legge del più forte"

[57] http://www.isoc.it/programmaIGFItalia2015
[58] Zigmunt Bauman "Vita Liquida" – Laterza, 2008
[59] http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

che, nella specie, è allo stato, agevolmente, individuabile nel volere ed interesse dei "colossi" della fornitura di servizi *web*.

Nel solco di un esercizio attivo della sovranità, si collocano, con riferimento ad attività illecite – quindi anche a quelle relative a fattispecie di contraffazione piuttosto che di i prateria – le azioni di "oscuramento" che le Autorità interne possono ordinare di operare agli *acces provider* in relazione a qui siti esteri per mezzo dei quali vengano compiute attività illecite.

Pur se non del tutto satisfattiva e risolutiva – poiché, come evidente, le attività illegali continueranno ad essere raggiungibili al di fuori della nazione ove operi l'inibizione – in assenza di un assetto più soddisfacente dei profili di transnazionalità della rete, il suddetto "oscuramento", appare quale rimedio da valorizzare.

Al riguardo, non può non evidenziarsi, però, come in forza della normativa esistente anche il predetto rimedio presenti aspetti problematici.

A rigore, difatti, la richiesta indirizzata a terzi (*access provider*) di inibire la trasmissione sul territorio nazionale di un sito, ha natura obbligatoria, esulando, pertanto, dallo schema tipico, ad esempio, del "sequestro preventivo " (art. 324 c.p.p) il quale, di contro, ha natura reale.

La Corte di Cassazione, con complessa argomentazione, ha ritenuto che "*uno speciale potere inibitorio è assegnato all'autorità giudiziaria dal D.Lgs. 9 aprile 2003, n. 70, artt. 14 e 16, di attuazione della direttiva 2000/31/CE relativa ai servizi della società dell'informazione.*" e che, pertanto, sussiste un potere inibitorio dell'autorità giudiziaria penale avente il contenuto di un ordine indirizzato ai *provider* di precludere l'accesso alla rete informatica *Internet* al solo fine di impedire la prosecuzione della perpetrazione del reato di cui all'art. 171 ter, comma 2, lett. a-bis)"

In conclusione, e quale ulteriore spunto di riflessione, si segnala che, al fine di consolidare il suddetto orientamento della Corte, in prospettiva *de jure condendo*, potrebbe essere opportuno prevedere il suddetto ordine di inibizione diretto ai *provider* espressamente, e normativamente, quale mezzo di inibitoria "tipico".

4. Conclusioni. Spunti di riflessione.

In conclusione, col presente lavoro, si sono messi in luce alcuni aspetti problematici che si frappongono, sovente, ad un'efficace azione di contrasto delle condotte illecite, e segnatamente alle azioni di contrasto della contraffazione e della pirateria *online*, formulando, ove ritenuto opportuno, spunti di riflessione ed indicazioni di possibili risoluzioni, anche in una prospettiva *de jure condendo*.

In particolare, sono state messe in luce le seguenti criticità, evidenziando, per ciascuna, il possibile rimedio individuato:

1) incertezza in ordine alla sussistenza della giurisdizione interna o comunitaria in relazione alle attività degli *ISP* aventi il loro centro di imputazione degli interessi in uno stato *extra UE*.

proposta di risoluzione: revisione critica di principi quali il c.d. *safe harbor* - per altro, di recente, dichiarato invalido dalla Corte Europea con riferimento al trasferimenti di dati verso gli U.S.A. – che spostano l'*enforcement* di diritti dal piano diretto dell'intervento dell'Autorità nazionale, o comunitaria, al piano della cooperazione internazionale.

2) infelice formulazione dell'art. 24 lett f) del Dlgs. 196/2033 ("casi nei quali può essere effettuato il trattamento senza il consenso") il quale dispone che "*il consenso non è richiesto quando il trattamento … con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento …".*

proposta di risoluzione: riformulazione del disposto di cui al suddetto art. 24 del Codice per la protezione dei dati personali, nel senso di mutare la facoltà, attribuita al titolare del trattamento (nella specie di interesse, gli *ISP*) in un **obbligo** di comunicazione, nelle ipotesi già previste di necessità di far valere un diritto in giudizio ovvero al fine di compiere attività di investigazione difensiva, in tutti i casi che appaiano non manifestamente infondati e, con riferimento alle richieste finalizzate

allo svolgimento di attività di investigazione difensiva, attraverso l'introduzione della specifica indicazione della circostanza che l'obbligo di comunicazione sussiste anche nella ipotesi di investigazioni difensive preventive nell'interesse della parte lesa.

3) previsione, all'art. 16 del Dlgs. 70/2003, del "privilegio" concesso agli *ISP*, costituito dalla sussistenza dell'obbligo di rimuovere contenuti illeciti solo "*su* ***comunicazione delle autorità competenti***".

proposta di risoluzione: eliminazione dal suddetto articolo dell'inciso "su comunicazione delle autorità competenti" il quale, per altro, esorbita dai principi direttivi attribuiti al governo in sede di legge delega 1 marzo 2002, n. 39 .

4) previsione, all'art. 17 del Dlgs. 70/2033, dell'obbligo, da parte degli ISP, di segnalare gli illeciti all'autorità giudiziaria, ("*il prestatore è comunque tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza qualora sia a conoscenza di presunte attività o informazioni illecite*") obbligo che, così come formulato, è fonte di incertezze distorsioni applicative.

proposta di risoluzione: circoscrivere il suddetto obbligo ad un limitato catalogo di reati, ed illeciti, specificamente individuati in conformità, per altro, ai principi direttivi della legge delega 1 marzo 2002, n. 39 .

5) L' art. 132 co. 1, D.lgs 196/2003 individua il termine di dodici mesi, dalla data della comunicazione , per la conservazione "*dati relativi al traffico telematico, esclusi i contenuti delle comunica*zionI" da parte del fornitore. Il predetto arco temporale (12 mesi) risulta spesso incompatibile con le reali tempistiche delle indagini preliminari finalizzata all'identificazione degli autori dei reati commessi per mezzo di *internet.*

proposta di risoluzione: potrebbe essere opportuno innalzare il predetto limite temporale di conservazione, quantomeno allineandolo a quello già previsto per i dati relativi al traffico telefonico che, di contro, è già di 24 mesi.

6) Lo speciale potere inibitorio assegnato all'autorità giudiziaria dal D.Lgs. 9 aprile 2003, n. 70, artt. 14 e 16 è fonte di dubbi ed incertezze interpretative, in ordine a

profili di sovrapponibilità od incompatibilità con l'istituto del sequestro di cui all'art 324. c.p.p., che ha natura reale e non obbligatoria.

proposta risolutiva: introdurre l'ordine di inibizione diretto all'*acces provider* e finalizzato ad impedire la trasmissione di siti sul territorio nazionale (c.d. oscuramento), quale mezzo di inibitoria tipico, eventualmente anche in seno al codice di procedura penale.

Con l'auspicio di aver utilmente contribuito al lavoro di Codesta Spettabile Commissione e di aver fornito utili spunti di riflessione.

Milano 14 dicembre 2015

Avv. Andrea Caristi

17STC0016560