ATTI PARLAMENTARI

XVII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **XXII-*bis***
N. **9**

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

(Istituita con deliberazione della Camera dei deputati del 25 settembre 2013)

(composta dai deputati: *Catania*, Presidente, *Allasia*, *Baruffi*, *Benamati*, *Berretta*, *Bordo*, *Borghese*, *Camani*, *Cariello*, Vicepresidente, *Caruso*, *Cenni*, *Donati*, *Fantinati*, *Gallinella*, *Garofalo*, Segretario, *Milanato*, *Mongiello*, Vicepresidente, *Rampelli*, *Russo*, *Senaldi*, Segretario, e *Taranto*)

RELAZIONE SUL FENOMENO DELLA CONTRAFFAZIONE SUL WEB

(Relatore: **on. Davide BARUFFI**)

Approvata dalla Commissione nella seduta del 23 marzo 2017

Comunicata alla Presidenza il 23 marzo 2017 ai sensi dell'articolo 2, comma 5, della deliberazione della Camera dei Deputati del 25 settembre 2013

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

RELAZIONE

PAGINA BIANCA

INDICE

1. INTRODUZIONE

Il fenomeno della contraffazione che si perpetra attraverso i sistemi telematici di *e-commerce* e via *web* in generale è forse uno dei più delicati e complessi nella prospettiva della definizione delle strategie di contrasto di tali fenomeni illeciti.

La contraffazione via *web* è sempre più rilevante per la crescita esponenziale delle transazioni commerciali via *internet*, che determina uno spostamento su tale mezzo delle forme di commercializzazione di molti prodotti contraffatti. Il fenomeno è già oggi molto rilevante e sempre di più lo sarà nel prossimo futuro e richiede perciò un'adeguata riflessione sulle forme di contrasto a tale fenomeno da predisporre.

La Commissione ha deciso pertanto di approfondire il tema, analizzando le modalità con le quali si manifesta oggi il commercio illecito di beni contraffatti con lesione dei diritti di proprietà industriale e la pirateria digitale particolarmente nel campo dei media audiovisivi in violazione del diritto d'autore, che si realizzano in forme svariate, palesi od occulte, nei siti e nelle piattaforme di *e-commerce* e nei *social forum* su *internet*.

In Commissione sono state pertanto svolte numerose sedute di audizioni con gli *stakeholders* del settore e le istituzioni competenti [(1)] e una missione di studio a Bruxelles per incontri con la Direzione CNECT della Commissione Europea.

Il quadro che è emerso da questa ampia ricognizione dei problemi e confronto con i soggetti più qualificati del settore, e che la presente relazione intende approfondire è molto complesso.

---

(1) Sono stati auditi: il 9-4-2015 il sostituto procuratore di Milano Tiziana Siciliano; il 17-6-2015 il procuratore aggiunto di Roma Nello Rossi; il 20-01-2016 il sottosegretario alla Presidenza del Consiglio con delega ai rapporti con l'UE Sandro Gozi; il 27-01-2016 il Direttore della Polizia Postale, Servizio centrale della polizia postale e delle comunicazioni, Roberto Di Legami; il 03-02-2016 il Comandante delle Unità Speciali della Guardia di Finanza, Gennaro Vecchione e il Capo del III Reparto – Operazioni del Comando Generale della Guardia di Finanza, Stefano Screpanti; il 18-02-2016 l'avvocato Andrea Caristi e il professor Ferdinando Ofria; il 03-03-2016 il segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali – FAPAV Federico Bagnoli Rossi, il presidente della Federazione Industria Musicale Italiana – FIMI Enzo Mazza, il presidente di Business Software Alliance – BSA Italia Paolo Valcher; il 10-03-2016 il segretario generale di Indicam, Claudio Bergonzi; il 17-03-2016 il Comandante del Comando Carabinieri Tutela della Salute, Claudio Vincelli; il 04-05-2016 il direttore dell'Ufficio Legislativo e Rapporti Istituzionali della S.I.A.E. Paolo Agoglia, e il direttore della Divisione Licenze e Servizi centrali della S.I.A.E. Sergio Maria Fasano; il 18-05-2016 il Segretario generale della Federazione contro la Pirateria Musicale e Multimediale FPM, Luca Vespignani; il 25-05-2016 il presidente del Consorzio del commercio Elettronico Italiano – NETCOMM Roberto Liscia e il presidente dell'Associazione Italiana Internet *Provider* – AIIP Renato Brunetti; il 21-07-2016 il direttore generale di I.A.B. Italia *(Interactive Advertising Bureau)* Daniele Sesini; il 27-07-2016 il presidente di Confindustria digitale, Elio Catania; il 28-09-2016 il Comandante Generale della Guardia di Finanza Giorgio Toschi e il Capo del II Reparto Operazioni del Comando Generale della Guardia di Finanza Stefano Screpanti; il 05-10-2016 rappresentanti di *eBay Inc*.; il 06-10-2016 rappresentanti di EUROPOL; il 13-10-2016 rappresentanti di *Alibaba* Group; il 27-10-2016 rappresentanti di Facebook Italia; il 03-11-2016 rappresentanti di Interpol; il 10-11-2016 rappresentanti di Google; il 18 gennaio 2017 rappresentanti di *Amazon*.

Le caratteristiche intrinseche di *internet*, che costituisce uno strumento globale a forte impatto sovranazionale, la sua costante espansione ed evoluzione, nonché la stessa dimensione immateriale del commercio elettronico rendono estremamente difficile attivare efficaci forme di contrasto alla commissione di illeciti via *web*.

Il quadro normativo esistente, la cui dimensione in sede comunitaria ed internazionale condiziona inevitabilmente la disciplina in sede nazionale, appare molto lacunoso nonché datato.

La direttiva 2000/31/CE, fondamentale in tema di commercio elettrico, recepita in Italia dal decreto legislativo 9 aprile 2003, n. 70 recante « *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico* », che afferma il principio della neutralità della rete e una ampia irresponsabilità dei *provider* per i comportamenti illeciti dei fruitori dei servizi sulle piattaforme digitali, è stata concepita in un periodo nel quale i servizi offerti dai *provider* erano molto diversi e certamente più limitati rispetto alla situazione odierna, tenendo altresì conto della rapida evoluzione tecnologica e commerciale manifestatasi in un periodo di tempo che per il mondo digitale rappresenta quasi un'« era geologica » diversa.

Uno dei problemi oggi sul tappeto è quello di conciliare la libertà di rete e le esigenze di espansione del commercio elettronico, da un lato, con le legittime istanze di tutela dei titolari dei diritti di proprietà industriale del *copyright*, da un lato, e dei consumatori dall'altro, rispetto ai profili di responsabilità dei fornitori dei servizi telematici offerti sul mercato e per l'utilizzo degli spazi virtuali ceduti.

Le forme di tutela giuridica esistenti nell'ordinamento avverso la contraffazione via *web* sono state descritte come inadeguate dalle aziende e dai titolari del diritto d'autore che richiedono invece un maggiore coinvolgimento, in termini di controllo preventivo, da parte dei *provider* in ordine all'inserimento in rete di prodotti contraffatti o di pirateria digitale. L'attuale sistema previsto dalla citata direttiva prevede oggi l'attivazione dei *provider* solo sulla base di segnalazioni da parte dei titolari di diritti di proprietà industriale o di diritti d'autore interessati o delle autorità competenti relative ad ogni specifica violazione al fine di rimuovere i contenuti illeciti. Tale sistema (c.d. procedura *Notice and Take Down*), pur essenziale, si è dimostrato spesso inefficace, nonché talvolta di difficile percorribilità. Tra i problemi segnalati: l'elevatissimo numero di violazioni; l'onerosità, anche economica, delle procedure da mettere in atto per i titolari di diritti; l'inefficacia delle tecniche di oscuramento dei siti.

Inoltre va considerato che le maggiori piattaforme commerciali operano su base globale, e come tali sono difficilmente soggette alla giurisdizione nazionale, per una carenza di strumenti di contrasto su base transnazionale.

Viceversa gli interventi di tipo proattivo, che prevedono un maggiore coinvolgimento dei *provider* in sede preventiva e non limitato al singolo caso, ma orientato ad impedire la reiterazione di attività illecite comunque realizzate (la c.d procedura di *Notice and Stay Down*, elaborata nell'esperienza americana), sono invocati dai titolari

di diritti come una nuova frontiera del bisogno di tutela per contrastare adeguatamente i fenomeni illeciti.

I contrasti tra aziende fornitrici dei servizi telematici e dei servizi connessi (in primo luogo nel settore pubblicitario), da un lato, e titolari dei marchi e soggetti titolari dei diritti d'autore e consumatori dall'altro, attengono ad una duplice sfera: quella ideologica anzitutto, relativa alla natura stessa di *internet* e alla liceità di controlli e atti limitativi della libertà di espressione e di commercio sulla rete; e naturalmente quella economica, relativa ai costi da sopportare per realizzare gli interventi di tipo preventivo, che contrappone le esigenze di tutela manifestate dai produttori e gli interessi dei *provider*.

L'approfondimento condotto dalla Commissione porta a ritenere opportuna, e in via generale preferibile, l'adozione di forme di coinvolgimento su base consensuale degli *stakeholders* del settore; intese volontarie per la definizione di comportamenti positivi volti a garantire il rispetto della legalità nelle transazioni commerciali, salvaguardare la libertà della rete e del commercio elettronico, tutelare i diritti di proprietà industriale ed intellettuale e tutelare maggiormente i consumatori.

Il quadro complessivo che emerge dagli approfondimenti svolti in Commissione evidenzia che il tema richiede, tuttavia, una serie di azioni positive volte ad adeguare la disciplina esistente ai grandi mutamenti intervenuti nel commercio digitale, al fine di rafforzare l'affidabilità complessiva del settore, per la quale la presenza di fenomeni diffusi di illegalità costituisce una minaccia al suo sviluppo e un grave nocumento per i titolari di diritti e i consumatori.

2. LA CONTRAFFAZIONE NEL QUADRO DELLO SVILUPPO DEL COMMERCIO ELETTRONICO

Nel corso delle audizioni in Commissione è emersa con chiarezza la dimensione del fenomeno dell'*e-commerce*, in rapporto alla crescita complessiva del « fenomeno *internet* » [(2)].

Nel 2015 sono stati 41,5 milioni gli italiani che hanno dichiarato di accedere a *internet* da qualsiasi luogo e strumento, vale a dire l'86,3 per cento della popolazione compresa tra gli 11 e i 74 anni; vi è una leggera flessione dell'accesso tramite computer (-2,5 per cento negli ultimi due anni), a fronte di un *trend* di costante crescita dell'accesso dai *device* mobili, con accesso da cellulari o *smartphone* per 32,7 milioni di individui (+45,3 per cento in due anni), 12,9 milioni da *tablet* (+83,6 per cento), 4,5 milioni da televisore (+63,2 per cento in due anni) e 6 milioni da *console* giochi (+33,7 per cento). Tra le categorie di siti frequentati dagli italiani, nel solo mese di dicembre 2015 l'82 per cento degli utenti italiani ha dichiarato di aver navigato su piattaforme per la condivisione di video e film, per un totale di 24 milione di utenti [(3)].

Con specifico riferimento al commercio elettronico, si rileva che su un totale di circa 14 mila miliardi di euro di PIL prodotti

(2) Dati tratti dall'audizione del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam.

(3) Rilevazioni *Audiweb*, citate nell'audizione del Segretario generale della FAPAV, Federico Bagnoli Rossi, il 3 marzo 2016.

nell'Unione europea nel 2016 quasi il 5 per cento è stato prodotto dal commercio *on line;* le previsioni al 2020 prevedono un aumento esponenziale del 50 per cento, per un valore stimato al 7,5 per cento del totale del PIL realizzato nell'UE [4].

In ambito europeo *leader* del commercio elettronico è la Gran Bretagna, con il 30 per cento del totale, seguita da Germania e Francia, ciascuna con il 25 per cento del totale. Il settore merceologico di maggior peso è quello dell'abbigliamento e beni correlati.

L'Italia ha solo il 3 per cento del totale dell'*e-commerce* UE, per un valore stimato di beni e servizi acquistati nel corso del 2016 pari a circa 16 miliardi di euro. Il ritardo dell'Italia rispetto ai grandi Paesi europei è ascrivibile, da un lato, al fenomeno del *digital divide* e dell'insufficiente diffusione della banda larga sull'intero territorio nazionale e, dall'altro, ad una scarsa propensione all'acquisto con metodi di pagamento virtuali e, in generale, all'acquisto non fisico. La fascia di utenti privilegiati in Italia è compresa tra i 25 e i 45 anni. Tuttavia il commercio elettronico è in crescita anche in Italia, dal momento che sono stimati in 19 milioni i consumatori che comprano *on line*, pur se la presenza di imprese in rete è ancora limitata: sono circa 40.000 quelle italiane che vendono prodotti sul *web*, a fronte delle 200.000 in Francia e delle 800.000 in Europa [5].

Il totale di consumatori che si rivolgono all'*e-commerce* (c.d. *e-shoppers*) è stato stimato in circa 1,7 miliardi di persone nel 2015 su base globale. La Cina vanta oltre 500 miliardi di euro di fatturato nel commercio *on line* mentre tra i primi dieci Paesi al mondo per volume di acquisti *on line* solo tre (quelli citati) sono europei.

Nel campo dei *social forum*, il numero di persone che si collegano almeno una volta al mese alla piattaforma di Facebook è di circa 1 miliardo e 700 mila persone, mentre gli utilizzatori di Instagram sono 500 milioni (con 28 milioni di utilizzatori in Italia di Facebook e 9 milioni di Instagram) [6].

Nel campo musicale i dati mostrano che oggi ben il 50 per cento del fatturato della musica nel mondo (41 per cento in Italia) è rappresentato dal digitale, nelle sue varie forme (*download*, *streaming*, modelli basati sulla pubblicità e sull'abbonamento) [7].

In Italia il settore degli audiovideo ha raggiunto un valore, nel 2015, di circa 14 miliardi di euro (con oltre 170.000 addetti), mentre il cinema in sala, pur cresciuto del 10,78 per cento rispetto al 2014, ha registrato un incasso totale pari a 637 milioni di euro, con 99 milioni di presenze, il settore televisivo e l'*home entertainment* hanno registrato un valore economico di 12 miliardi e 213 milioni di euro, per ricavi da *advertising*, canone, pay Tv e altre fonti, Home Video, OTT TV, vendita di dispositive audio e video, ecc.), con quasi 96 mila addetti nel 2014. Il settore digitale o del *broadcasting* è dunque rilevantissimo in termini economici e la lotta alla pirateria digitale un target di grande rilevanza sociale ed economica. Il mercato digitale – nuove piattaforme ed operatori hanno accresciuto l'offerta di servizi

(4) Fonte: *E-commerce Europe*.

(5) Dati tratti dall'audizione del Presidente del consorzio NETCOMM Liscia del 25 maggio 2016.

(6) V. audizione del 27 ottobre 2016 con il responsabile dei rapporti istituzionali per Italia, Grecia e Malta di *Facebook*, Laura Bononcini.

(7) V. audizione del 18 maggio 2016 di Luca Vespignani, Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale FPM.

all'utenza, sia per il « *download* » (EST), che per lo « *streaming* » (VOD), che con servizi in abbonamento (S-VOD) – pesa oggi per il 7,1 per cento del settore audio-video, con un +38,9 per cento nel 2014 rispetto al 2013 e un giro d'affari stimato a 25 milioni di euro [8].

Alla creazione di una vera e propria piazza commerciale telematica globale, è seguito inevitabilmente lo sviluppo di forme di commercio illegale *on line*, con merci contraffatte in violazione dei diritti di proprietà industriale o prodotti di pirateria digitale in violazione del diritto d'autore.

Le stime OCSE riferiscono di un aumento del fatturato dell'attività di contraffazione *on line* maggiore rispetto alla crescita del fatturato del commercio elettronico internazionale legale, dovuto anche dalla presenza di organizzazioni criminali internazionali che hanno orientato proprio sul versante della contraffazione parte dei propri interessi criminali. La contraffazione si presenta oggi non più solo come un fenomeno localizzato, quanto a produzione e distribuzione, solo in aree geografiche specifiche ma, al contrario, un'attività largamente organizzata a carattere transazionale che si rivolge ad una platea mondiale di consumatori.

Nell'audizione con INDICAM del 10 marzo 2016 [9] è stato riferito come la contraffazione *on line* cresca, ogni anno, a livello mondiale, del 15,6 per cento, con un costo per l'economia stimato in 1.800 miliardi di dollari; per l'Italia il costo della contraffazione per l'economia è stimato dal CENSIS in perdite per le imprese italiane nei vari settori industriali per circa 6,5 miliardi di euro, con 104.500 unità lavorative perse (per contraffazione e pirateria) [10]. Tra i beni più a rischio di contraffazione vi sono il *fashion* (abbigliamento e accessori) e l'elettronica di consumo, oltre ai farmaci e ai prodotti alimentari [11].

3. LA DANNOSITÀ DELLA CONTRAFFAZIONE SUL WEB

Gli effetti nocivi della contraffazione e della pirateria digitale sono ben noti alla Commissione, che nel corso di questa legislatura ha più volte esaminato la questione sotto il profilo di danni economici alle aziende, di sostegno indiretto alla criminalità organizzata, per la quale la contraffazione costituisce un settore rilevante di attività, di sfruttamento del lavoro in nero, di evasione fiscale, di inganno per i consumatori, di ostacolo allo sviluppo e alla competitività del mercato, di freno all'innovazione e alla creatività nei settori produttivi [12].

---

(8) Dati dell'indagine « Italia Creativa » raccolti da Ernst & Young, citati nell'audizione del Segretario generale della FAPAV, Federico Bagnoli Rossi, il 3 marzo 2016.

(9) Audizione del 10 marzo 2016 di Claudio Bergonzi, segretario generale di Indicam.

(10) Dati citati nell'audizione del 3 marzo 2016 con il Segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali (FAPAV), Federico Bagnoli Rossi.

(11) V. Audizione del 5 ottobre 2016 con Andrea Rota, Senior *Director Global Brand Protection* e Stefan Krawczyk, *Associate General Counsel and Head Government relations International* di *eBay Inc*.

(12) V. analisi delle conseguenze socio-economiche della contraffazione contenute in: Doc. XXII-*bis*, n. 1, Relazione su possibili proposte normative in materia penale in tema di contraffazione (relatore Mario Catania), approvata il 4 agosto 2015; Doc. XXII-*bis*, n. 2, Relazione sulla contraffazione nel settore tessile: il caso del distretto produttivo di Prato (relatrice: Susanna Cenni), approvata il 4 agosto 2015; Doc. XXII-bis, n. 3, Relazione sulla contraffazione nel settore calzaturiero (relatore: Filippo Gallinella), approvata il 4 agosto 2015; Doc. XXII-*bis*, n. 4, Relazione

L'Italia, la cui economia è tipicamente vocata alla manifattura, anche attraverso un prezioso tessuto di piccole medie imprese, è particolarmente colpita dal fenomeno.

La falsificazione dei marchi e dei prodotti e la pirateria digitale, oltre ad una grave distorsione complessiva dell'economia e agli effetti sociali negativi ben noti, determina una lesione particolarmente marcata proprio ai prodotti di qualità che costituiscono l'essenza del « *made in Italy* ». Si tratta di prodotti ad alto valore aggiunto, che hanno i propri elementi qualificanti, rispetto alle produzioni di altri Paesi, nello stile e nel *design*, ad esempio dei prodotti dell'abbigliamento, oppure nella qualità dei prodotti dell'agroalimentare.

Un elemento importante che favorisce il commercio illecito *on line* è rappresentato dalla facilità con cui può essere praticato e dalle dimensioni dei profitti rispetto ai rischi che le organizzazioni criminali che gestiscono tale attività illecita corrono concretamente.

È un dato evidente come, anche in forza della spinta del *web*, la contraffazione da fenomeno locale e quasi artigianale sia approdata, negli ultimi decenni, ad una dimensione di fenomeno transnazionale; non può sorprendere che a cavalcare tale fenomeno siano anche potenti organizzazioni criminali internazionali. Queste ultime hanno l'interesse a diversificare le attività illecite svolte nei settori tradizionali (traffico di stupefacenti, traffico di armi, sfruttamento della prostituzione, tratta degli emigrati, estorsioni, ecc.) – per i quali vi è un forte contrasto, da parte delle autorità competenti, ed un elevato allarme sociale – rivolgendosi verso nuovi campi di attività, quali la contraffazione, ove l'opinione pubblica è senz'altro meno avvertita della grave pericolosità sociale ed economica del fenomeno e il contrasto delle Istituzioni è stato storicamente meno pressante.

3.1. Le caratteristiche del commercio *on line* che favoriscono la contraffazione.

Rispetto alle forme tradizionali della contraffazione la commissione di illeciti tramite il *web* è agevolata da una serie di fattori [13]:

• la possibilità per gli autori degli illeciti di nascondere o simulare la propria identità sul *web*; per superare il limite dell'anonimato e della « aterritorialità digitale » sono necessarie onerose forme di cooperazione internazionale;

• l'ampia scelta di « punti vendita virtuali », costituiti dalle piattaforme digitali e dai siti *internet* di commercio elettronico, che consente una pericolosa dissimulazione tra prodotti veri e falsi, stante il ricorso per questi ultimi a immagini tratte dai cataloghi ufficiali;

• la relativa « sicurezza » delle transazioni illecite, sia sul piano economico, sia su quello distributivo-logistico, in quanto il controllo

---

sulla contraffazione nel settore dell'olio di oliva (relatrice Colomba Mongiello), approvata il 17 settembre 2015; Doc. XXII-*bis*, n. 5, Relazione sulla contraffazione nel settore della mozzarella di bufala campana (relatore: Paolo Russo), approvata il 23 settembre 2015.

(13) V. audizioni della Guardia di Finanza del 3 febbraio 2016, con il Comandante delle Unità Speciali, Gennaro Vecchione e il Capo del III Reparto – Operazioni, Stefano Screpanti e del 28 settembre 2016 con il Comandante Generale della Guardia di Finanza, Giorgio Toschi.

sul territorio può essere facilmente eluso dalle piccole spedizioni che interessano i consumatori finali;

• la tendenza alla transnazionalità dei traffici di merce contraffatta [14]; gli apparati informatici che ospitano le vetrine *on line* dei falsi sono in massima parte localizzati in paesi esteri e dispersi in una fitta rete di indirizzi e punti di snodo virtuali, la cui ricostruzione è molto complessa;

• una sorta di « territorialità digitale », in quanto gran parte delle transazioni di prodotti contraffatti non ricadono nella giurisdizione italiana ma avvengono su scala transnazionale, il che implica una sostanziale assenza di territorialità dei traffici che sfruttano la rete « estero su estero », e dove sia i venditori che i *server* sono ubicati all'estero; poiché sia la produzione dei beni contraffatti che l'immissione sul mercato digitale avviene in contesti non soggetti alla giurisdizione italiana, sono evidenti le grandi difficoltà delle autorità di polizia e dei titolari di diritti a porre in atto efficaci azioni di contrasto;

• il frazionamento tra la fase di produzione della merce contraffatta e della vendita su *internet* aumenta le difficoltà di contrasto: l'eventuale individuazione dei responsabili di siti o piattaforme informatiche illecite non comporta anche l'individuazione dei canali di produzione e stoccaggio della merce illegale.

Il profitto è diverso nel caso di vendita di merci contraffatte o di pirateria concernente le opere dell'ingegno: mentre per le prime è rappresentato dal prezzo di vendita pagato per la merce contraffatta dall'utente dell'*e-commerce*, nel caso del *download* spesso le opere sono messe a disposizione degli utenti gratuitamente, in quanto i siti illeciti traggono profitto essenzialmente dai proventi pubblicitari derivanti dalla gestione del sito.

3.2. L'assenza di una *governance* mondiale di internet.

Un altro fattore che contribuisce a rendere difficoltosi gli interventi di contrasto alla contraffazione sulla rete è costituito dalla assenza di una *governance* mondiale di *internet* e dell'ambiente digitale globale. L'assenza di un'autorità di regolamentazione internazionale contribuisce a far sì che le istanze di tutela degli interessi non trovino un interlocutore unico e sovraordinato tra operatori ISP, aziende e consumatori interessati cui rivolgere le istanze da parte dei titolari dei diritti che si ritengano lesi.

Il modello di *governance* della rete è diffuso e largamente privo di una regolamentazione a livello internazionale. L'attribuzione dei domini e degli indirizzi IP è affidato ad un organo che opera secondo la normativa degli USA – l'ICANN – che attribuisce i domini di primo livello e i *root server*. Per quanto riguarda specificatamente il contrasto alla contraffazione, è stato rilevato in audizione [15] come la

(14) V. Audizione del 28 settembre 2016 con il Comandante Generale della Guardia di Finanza, Giorgio Toschi.

(15) V. audizione del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam.

prassi di consentire la registrazione di domini generici (ad es. siti con nomi di specie di prodotti alimentari) possa essere in controtendenza rispetto all'esigenza di tutelare beni in cui non conta il genere, ma la specificità delle produzioni nazionali e geografiche, come rilevato dall'Osservatorio UE sugli *IP infringements*. La dimensione meramente comunicativa o commerciale delle attività in rete non consente di valutare questi aspetti dal punto di vista della prevenzione della commissione di illeciti, che non attengono alla sfera di competenza dell'ICANN. In questo senso occorre altresì interrogarsi circa i modelli di *governance* con l'adozione di approcci non solo *top-down,* ma anche *bottom-up,* finalizzati ad introdurre forme di controllo dal basso, che nel settore della contraffazione coincidono con la titolarità di interessi lesi e nella tutela degli interessi del consumatore.

Per questo motivo in ambito comunitario è stata posta la questione di una maggiore regolamentazione del settore. La Commissione UE ha ritenuto in proposito che una delle priorità della sua azione in merito di comunicazione digitale, sia la creazione di un Digital Single Market (DSM), nel quale realizzare un'armonizzazione delle regole nazionali attualmente vigenti, per la costituzione di un vero unico mercato digitale.

I temi affrontati in sede comunitaria sono il superamento delle barriere in tema di protezione dei dati, l'armonizzazione delle aliquote dell'imposta sul valore aggiunto, la riforma delle regole nelle telecomunicazioni, la protezione del *copyright* rispetto alle nuove tecnologie digitali, il superamento del fenomeno delle transazioni transnazionali (c.d. *cross border selling)*, vendite effettuate in *server* posti fuori dei confini nazionali, che rendono più conveniente il commercio elettronico effettuato fuori dai confini nazionali.

3.3. La complessità dell'azione investigativa di contrasto.

Alla diffusione della contraffazione nell'ambito del commercio elettronico corrisponde la difficoltà di un efficace contrasto da parte delle Istituzioni competenti, per le motivazioni in precedenza descritte.

A fronte di un impegno che la Commissione ha potuto valutare come massimo da parte delle forze di polizia e della magistratura, che ha portato a risultati significativi, si deve rilevare che la natura immateriale e globale della rete costituisce un terreno oggettivo di grande difficoltà operativa per chi deve predisporre le azioni di controllo e contrasto alla contraffazione.

Il rafforzamento della collaborazione informativa e operativa delle forze dell'ordine a livello internazionale è pertanto decisivo per una lotta efficace contro le caratteristiche transnazionali della contraffazione.

Al proposito va ricordato che, con il decreto legislativo n. 34 del 2016, è stata recepita la decisione del Consiglio dell'Unione europea n. 465 del 13 giugno 2002, che permette alle autorità giudiziarie e alle forze di polizia di almeno due Stati membri di creare *team* comuni incaricati dello svolgimento di indagini penali in ambiti specifici e per una durata di tempo limitata. Oggetto di attività è qualunque reato

che, a giudizio dell'autorità giudiziaria procedente, richieda il compimento di indagini complesse sul territorio di più Stati membri. Gli atti compiuti dalle squadre comuni sono acquisiti direttamente nei fascicoli processuali delle indagini in corso in ciascuno Stato partecipante, senza necessità di rogatoria.

Il ricorso alle rogatorie costituisce, infatti, uno dei punti deboli del contrasto in ambito transnazionale, per la lentezza e il costo di tali procedure.

L'altro canale attivo è quello della partecipazione alle iniziative di coordinamento internazionale sotto l'egida dell'Unione europea e degli organismi sovranazionali di Polizia: la partecipazione alle attività pianificate dell'International Crime Police Organization (Interpol) e dell'Organizzazione mondiale delle dogane, per una maggiore assistenza tra le autorità di Polizia e doganali [(16)]; la collaborazione con l'agenzia Europol, presso la quale è stato istituito l'Intellectual Property Crime Coordinated Coalition (IPC3), nuovo centro per la cooperazione in materia di lotta alla contraffazione, anche mediante lo sviluppo di sinergie con il settore privato e l'Università, sul modello di analoghe positive esperienze negli Stati Uniti d'America, promosse dall'International AntiCounterfeiting Coalition (IACC) e l'Ufficio europeo per la lotta antifrode (OLAF), nell'ambito dell'European Union *Policy Cycle* dell'Unione europea, progetto quadriennale per il contrasto delle fenomenologie criminali, tra cui anche la contraffazione.

A livello nazionale anche la frammentazione delle forze di polizia costituisce un problema per l'efficacia del contrasto alla contraffazione in generale, sul *web* in particolare. Il riparto di competenze tra le forze dell'ordine determina talvolta delle sovrapposizioni di ruolo: la polizia postale ha maturato una specializzazione nel *copyright*, particolarmente nel contrasto della pirateria musicale e cinematografica, con attenzione anche ad attacchi ad infrastrutture critiche, al crimine finanziario cibernetico, alla pedopornografia e al terrorismo, mentre la Guardia di finanza ha una competenza specifica, a carattere generale, in materia di contraffazione, con il Nucleo speciale frodi tecnologiche che assicura una costante attività di monitoraggio della rete, funzionale al contrasto dei crimini economico-finanziari che vengono perpetrati sul *web*, tra cui anche i traffici di merce contraffatta [(17)]; i Carabinieri hanno, infine, una specializzazione nelle sofisticazioni alimentari e nella filiera del farmaco. Ciò determina la necessità di raccordi operativi e, proprio per la contraffazione sul *web*, una duplicazione di strutture per l'analisi e l'intercettazione delle frodi *on line*. Ad esempio, nel corso delle audizioni, è emerso come nel settore della pirateria nell'audiovisivo, per il *card sharing*, vi siano interventi sia della Polizia postale che della Guardia di Finanza [(18)].

(16) Nell'audizione del 28 settembre 2016 il Comandante Generale della Guardia di Finanza, Giorgio Toschi, ha sottolineato l'importanza delle operazioni « Opson », « In our sites », « Wafers », « Pangea », « Silver Axe » e « Copycat », in materia di contraffazione e frodi alimentari e agroalimentari, commercio illecito *on line*, traffici di semiconduttori contraffatti, commercio illegale di farmaci, traffico di pesticidi dannosi per la salute, prodotti sportivi.

(17) Nell'audizione del 28 settembre 2016 il Comandante Generale della Guardia di Finanza Giorgio Toschi ha ricordato che tra il gennaio 2015 e il luglio 2016, i siti *internet* sequestrati/oscurati sono stati nel complesso 1.058, che si aggiungono ai 269 oggetto di analoghe misure cautelari nel 2014.

(18) V. audizione del 27 gennaio 2016 di Roberto Di Legami, Direttore della Polizia Postale, Servizio centrale della polizia postale e delle comunicazioni.

Un altro tema importante in materia di contrasto alla contraffazione sul *web* è quello della possibilità di effettuare, da parte delle forze dell'ordine, un'attività di scansione preventiva della rete. Per esempio, nel caso della lotta alla pedopornografia *on line*, la scansione è costante da parte della Polizia postale, perché la legge in materia già prevede che sia curato l'aggiornamento della *blacklist* delle piattaforme virtuali che ospitano questi contenuti.

La Guardia di Finanza [19] ha elaborato di recente la piattaforma « Co.li.bri. » (*counterfeiting on line brand inquiry*), sistema di controllo e monitoraggio anti contraffazione, che opera il monitoraggio dei canali di distribuzione commerciale *on line*, selezionando ed estraendo dal *web* elementi informativi rivelatori di condotte lesive dei diritti di proprietà intellettuale. Il sistema opera con un motore di ricerca « semantico » che, tramite apposite parole chiave, individua ed estrae inserzioni a rischio contraffazione nelle piattaforme di vendita *on line*.

Tenuto conto dell'enorme dimensione dell'ambiente del commercio digitale, è evidente che forme di razionalizzazione delle risorse e di raccordo con i titolari di diritti che effettuano le segnalazioni agli ISP nel settore degli IPR e DPI appaiono necessarie. Nel caso di fattispecie di reato quale il *cyberbullismo* o la pedopornografia, vi sono interessi pubblici alla tutela dell'ordine e della sicurezza pubblica e, quindi, un'attività d'ufficio è necessaria; in questo settore sono state già sviluppate forme di collaborazione tra le forze di polizia e gli operatori del *web*. Viceversa, nel caso di diritti patrimoniali di aziende titolari di marche, anche se un intervento pubblico trova fondamento nel fine di combattere forme di evasione fiscale, per evitare ingenti danni erariali per lo Stato, appare ragionevole che questa attività preventiva di monitoraggio della rete, di dimensioni ingenti per traffico sul *web* e molto costosa per i costi di gestione di sistemi tecnologici di monitoraggio preventivo, sia svolta anche nell'ambito del rapporto commerciale tra *providers* e aziende produttrici.

Un ulteriore problema in tema di efficacia dell'azione di contrasto, emerso nel corso delle audizioni in Commissione, è costituito dall'identificazione univoca dell'identità degli utenti/dispositivi a partire dagli indirizzi IP (*Internet Protocol address*). Gli strumenti investigativi sono limitati, in quanto, per rivelare i *nickname* e risalire all'identità del titolare, è necessario un provvedimento del magistrato, all'interno di un procedimento penale, che richieda in via autoritativa ai *provider* di consentire l'identificazione degli utenti/dispositivi, procedura che non consente di operare in tempo reale o sulla base di richieste da parte delle autorità amministrative competenti.

3.4. La formazione del consumatore.

Ad accrescere la pericolosità della contraffazione via *web* vi è anche l'atteggiamento condiscendente di una parte dei consumatori che acquistano in rete. Spesso nella scelta del consumatore *e-shopper* non vi è un'adeguata consapevolezza dell'illegalità e della pericolosità dell'operazione di acquisto di merce contraffatta in rete e dei danni

(19) V. audizione del 28 settembre 2016 con il Comandante Generale della Guardia di Finanza, Giorgio Toschi.

economici che tale acquisto può causare, da un lato, a fronte di un possibile vantaggio economico e sociale, legato al possesso di beni di presunto pregio altrimenti irraggiungibili. Il problema è più sensibile tra i giovani, dai quali il disvalore dell'acquisto fraudolento è meno percepito.

La Commissione sottolinea, al riguardo, la necessità di lavorare sul versante della educazione al disvalore della contraffazione, con una formazione, anche a livello scolastico, finalizzata a promuovere la legalità degli acquisti del consumatore.

In tale attività devono essere coinvolti i produttori, i titolari di marchi o dei diritti d'autore, con la promozione di campagne di informazione del consumatore ed iniziative di comunicazione rivolte ai consumatori e all'opinione pubblica [(20)].

In una ricerca realizzata nel 2013 dall'Associazione LIBERA con ANEC, ANICA, FAPAV e UNIVIDEO [(21)], ad esempio, si è evidenziato che il tasso di penetrazione della pirateria digitale in Italia è più alto nei giovani compresi tra i 14 e i 18 anni, con un'incidenza superiore al 70 per cento. Sempre secondo tale ricerca, solo metà degli studenti intervistati ritiene che scaricare o guardare copie non originali di film da *Internet* sia dannoso.

La Polizia postale e la Guardia di finanza hanno messo in campo progetti educativi con le scuole, per raggiungere ogni anno oltre 400 mila studenti e più di 1500 istituti scolastici [(22)].

4. LA TIPOLOGIA DELLA CONTRAFFAZIONE SUL WEB

Molteplici sono le forme della contraffazione sul *web* di marchi e altri segni distintivi o di pirateria digitale in violazione del *copyright*. La possibilità di rilevare le frodi e l'identificazione delle principali forme di accesso del commercio di beni contraffatti in rete, si differenzia in ragione delle diverse forme che il commercio elettronico ha assunto, in linea con il continuo processo di evoluzione della rete.

Esistono diversi tipi di commercio elettronico, gestiti da Commercial Service *Provider* (CSP), branca di attività molto rilevante all'interno della categoria generale degli *Internet Service Provider* (ISP), che, oltre ad offrire l'accesso a *Internet* con i relativi servizi

(20) Va ricordata l'iniziativa in tema di *educational, con* un *kit* per le scuole in cui si racconta il *backstage* di un film, una canzone, un prodotto audiovisivo o musicale, realizzata nel 2015 da FAPAV, ANICA, MPA e UNIVIDEO, come ricordata nell'audizione del Segretario generale della FAPAV, Federico Bagnoli Rossi, il 3 marzo 2016.

Vanno ricordate, al riguardo, le seguenti iniziative in tema di *educational* e sensibilizzazione: « Rispettiamo la creatività », realizzata da AFI, ANICA, FAPAV, MPA, NUOVOIMAIE, SIAE e UNIVIDEO, che ha raggiunto oltre 85.000 studenti tramite l'utilizzo di un *kit* didattico in cui si racconta il *backstage* di un film, una canzone, un prodotto audiovisivo o musicale, valorizzando il prodotto creativo; IO FACCIO FILM – Chi ama il cinema, non lo tradisce « campagna promossa da ANICA, FAPAV, MPA e UNIVIDEO, con l'obiettivo di valorizzare i lavoratori del comparto audiovisivo ».

(21) Ricerca *« Oltre la pirateria. I film, il cinema e i giovani: tra web, dvd e grande schermo »,* citata nell'audizione del 3 marzo 2016 con il Segretario generale della FAPAV, Bagnoli Rossi.

(22) Nell'audizione del 27 gennaio 2016 di Roberto Di Legami, Direttore della Polizia Postale, Servizio centrale della polizia postale e delle comunicazioni, sono stati citati i programmi « *Web* in cattedra », « Non perdere la bussola », « Buono a sapersi », « In strada come in rete », « Occhi in rete » e « Per un *web* sicuro ».

come gli ISP, offrono un pacchetto completo di Hosting e un insieme di software per l'*e-commerce*.

In sede normativa – ai sensi della direttiva sul commercio elettronico 2000/31/CE, nel decreto legislativo 9 aprile 2003, n. 70, che ha dato attuazione alla direttiva, e nell'articolo 1, comma 1, lettera *b*), della legge 21 giugno 1986, n. 317, e successive modificazioni – i soggetti operanti nel mondo digitale sono definiti « prestatori di servizi della società dell'informazione », ossia soggetti che conducono attività economiche svolgendole in linea (*on line*) e qualsiasi servizio della società dell'informazione prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi [(23)].

I *provider* specializzati nel commercio elettronico offrono servizi differenziati per modalità di transazioni e tipologia di utenti destinatari dei servizi: le fattispecie più rilevanti sono quelle del *Business to Business* (B2B), ovvero vendita di merci tra due realtà di *business* (aziende, enti pubblici o professionisti); del *Business to Consumer* (B2C), vendita di merci tra operatori di *business* professionali e consumatori (c.d. *e-shoppers)*; del *Peer to Peer* (P2P), ove una pluralità di clienti entra in contatto reciproco, vendendo, comprando o scambiando, segnatamente prodotti digitali dell'audiovisivo. [(24)]

I *provider* che hanno realizzato importanti piattaforme digitali per il commercio elettronico, si veda il caso di *e-Bay* o di *Alibaba*, forniscono spazi in rete sia a siti gestiti da venditori, che operano come intermediari tra i prodotti realizzati dalle aziende e i consumatori, sia a siti propri delle aziende manufatturiere, che vendono direttamente i propri prodotti; alcune di queste grandi piattaforme, ad esempio *Amazon*, sono divenuti essi stessi venditori dei prodotti, di cui acquisiscono la proprietà, destinati all'*e-commerce*, gestendo un'attività di intermediazione, con creazione di magazzini di deposito della merce, tra i produttori e i consumatori. L'accesso ai siti di vendita *on line* è peraltro disponibile attraverso i motori di ricerca, si veda il caso di *Google*, che attraverso la ricerca algoritmica delle merci e dei marchi mette in connessione venditori e compratori del settore dell'*e-commerce*, fornendo altresì servizi accessori, ad esempio pubblicitari. Accedono al commercio elettronico anche le cosiddette piattaforme del *web 2.0.*, i *blog*, i *wiki* e i *social network* (si veda il caso di *Facebook*), nei quali intervengono una pluralità di utenti in modo bi/multi direzionale, che nati ed operanti come forma di comunicazione sociale, hanno sviluppato importanti strumenti destinati al commercio, con l'assegnazione di account a soggetti dediti professionalmente al commercio.

Nel settore dei media audiovisivi operano i sistemi di *peer to peer*, *di file sharing o di downloading-uploading*, con i quali gli audiovisivi

(23) Per servizi a distanza si intendono i servizi forniti senza la presenza simultanea delle parti; per « via elettronica » si identificano i servizi inviati all'origine e ricevuti a destinazione mediante attrezzature elettroniche di trattamento, compresa la compressione digitale e di memorizzazione di dati, interamente trasmessi, inoltrati e ricevuti mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici; per « servizio a richiesta individuale di un destinatario di servizi » si intendono i servizi forniti mediante trasmissione di dati su richiesta individuale.

(24) Si ricordano anche: *Business to Employee* (B2E); *Business to Administration* (B2A); *Business to Machines* (B2M); *Business to Manager* (B2M); *Consumer to Business* (C2B); *Consumer to Consumer* (C2C); *Consumer to Administration* (C2A); *Government to Business* (G2B); *Government to Citizen* (G2C); *Government to Employees* (G2E); *Government to Government* (G2G*); Manager to Consumer* (M2C).

sono immessi sulla rete, nonché di *link sharing*, ad esempio *YouTube*, finanziati dalla pubblicità.

Infine molte delle piattaforme digitali più grandi offrono servizi integrati, si veda il caso di *Alibaba*, con la differenziazione delle piattaforme, alcune destinate ai consumatori, altre alle aziende, la predisposizione di servizi accessori (pubblicitari, di spedizione, ecc.) da società appartenenti alla *holding* di controllo.

Questa complessa situazione dell'offerta di commercio elettronico è molto rilevante per quanto attiene ai bisogni di tutela manifestati da parte dei titolari dei diritti, che a seconda del diritto da tutelare (IPR o DPI) e del tipo di supporto tecnologico, nella prassi che la Commissione ha potuto accertare, vedono diversamente soddisfatte le proprie segnalazioni relative alla lesione dei propri diritti. Su questo punto si rinvia al successivo paragrafo 7.1.

Esaminiamo ora le modalità con le quali la contraffazione si manifesta nei diversi segmenti di *e-commerce*, che è molto variegata.

4.1. Criteri per individuare i siti dediti alla contraffazione.

La possibilità di individuare siti illeciti dediti alla contraffazione è evidente nelle prassi di contrasto utilizzate dalle forze dell'ordine e dai titolari di diritti in una serie di casi.

A titolo esemplificativo si riportano alcuni dei casi più comuni.

Una forma molto frequente è rappresentata dalla vendita di merci con prezzi anormalmente bassi. È fisiologico che la vendita di merci sui siti possa avvenire a prezzi inferiori rispetto a quelli dei negozi fisici, per l'abbattimento dei costi di gestione (spese di esercizio dei locali, spese di personale, ecc.); quando il prezzo, però, è del tutto fuori mercato si è generalmente in presenza di merci contraffatte.

Un altro indice della presenza sui siti di merci contraffatte è rappresentato dalla vendita di prodotti non presenti nei cataloghi ufficiali dei produttori legali; in questi casi nel sito è apposto fraudolentemente un marchio su un prodotto contraffatto.

Altro elemento rilevatore della presenza di merci contraffatte è dato dalla eccessiva disponibilità, per quantità, di prodotti vendibili.

Fattispecie identiche a quelle realizzate sui prodotti presenti nei negozi, sono invece quelle della presenza di merci con marchi imitati o simili, ovvero di merci con etichette o *packaging* contraffatti, ovvero di merci con ricevute e scontrini contraffatti.

4.2. Fattispecie di siti illegali.

Dal punto di vista delle fattispecie più comuni di siti illegali dediti allo smercio di merce contraffatta, devono essere ricordati alcuni casi molto comuni [(25)]:

a) il c.d. *hacking* o *defacement* consiste in pagine di vendita di merci contraffatte che sono inserite in siti legali, intercettando le

(25) Un'analisi della tipologia di *e-commerce* illecito è contenuta in « Lotta alla contraffazione in *internet* – Metodologie, esperienze e risultati » a cura di Convey Srl e Patnet.it, pubblicato da Italia Oggi, del maggio 2014.

ricerche di consumatori inconsapevoli, che sul *web* ricercano merce legale in rete: si tratta di sistemi informatici che reindirizzano le ricerche dai siti legali a quelli illegali, senza che l'utente non esperto abbia contezza di essere reindirizzato su tali siti, e all'insaputa dei legittimi titolari di pagine *web* di siti legali o istituzionali [(26)]. Appositi programmi utilizzati dai contraffattori, in questi casi, sondano metodicamente su larga scala la vulnerabilità delle piattaforme informatiche che ospitano i siti legali, con il doppio obiettivo di ingannare gli utenti e di far aumentare il *page rank* dei siti illegali sui motori di ricerca. Fenomeno connesso è quello della sottrazione di identità a danni di utenti inconsapevoli, che divengono intestatari di siti di vendita illegale a loro totale insaputa, con un'azione di copiatura dei dati anagrafici relativi alla titolarità del sito per associarli ad altri siti illegali;

b) il c.d. *cybersquatting* consiste nell'accaparramento di siti da registrare presso l'ICANN (I*nternet Corporation for Assigned Names and Numbers*), che hanno nomi a dominio corrispondenti a marchi e altri segni distintivi altrui (insegne, ragioni sociali, nomi propri di personalità); si ha il *domain grabbing*, quando da domini esistenti abbinati a marchi generici si opera un'estensione illecita ad un TLD (*Top Level Domain*). Tali pratiche consentono, sia l'uso di tali siti per la commercializzare di prodotti contraffatti o per il loro uso in siti con elevato contenuto pubblicitario, sia per il successivo trasferimento oneroso di tali domini ai legittimi titolari. Esiste, in sede ICANN, collegata con il WIPO un istituto di arbitrato di riassegnazione dei nomi a dominio, che in alcuni casi ha dimostrato la propria efficacia come misura deterrente nei confronti dei titolari di attività illecite;

c) un'altra pratica illegale è quella di nomi a dominio avente un effetto di « *sounding* », sia nella scrittura (ad esempio introducendo storpiature dattilografiche – c.d. *typosquatting*) per realizzare una voluta confusione dei nomi), che per il suono inserito; altra modalità pratica è quella di riprodurre il nome del marchio mascherandolo con un suffisso (ad. es. *brandrealdiscount*; *brandheap*), così da ingannare consumatori inesperti, che confondono il sito illegale con quello legale, non considerando la presenza del suffisso;

d) più occulte sono le prassi che si avvalgono di soluzioni tecnologiche per orientare i consumatori ad accedere ai siti illegali, senza che questi ne siano avvertiti. È il caso dell'inserimento del marchio nei metadati del sito: il marchio non è inserito nel testo della pagina *web*, ma nel TAG del codice HTML e del c.d. *cloaking*, che consiste nell'inserimento di codici *javascript* invisibili agli utenti, ma segnalati dai motori di ricerca; in altri casi il marchio illegalmente utilizzabile è riprodotto i caratteri minimi nel corpo della pagina *web*;

e) altro uso illegittimo di marchi famosi si realizza con la c.d. *spam/injection* di *website* di terzi in messaggi pseudo-pubblicitari o in

(26) Il Nucleo speciale frodi tecnologiche della Guardia di Finanza nell'operazione « vetrine opache » del 2014 ha individuato 53 siti italiani dove erano state pubblicate pagine *web* che rimandavano ad alcuni portali di e-commerce di merce contraffatta ospitati su server esteri. I siti, riconducibili, in alcuni casi, a comuni o a scuole, erano stati violati all'insaputa dei legittimi titolari da *hacker* professionisti che sfruttavano con successo debolezze dei sistemi informatici, per pubblicare illegalmente pagine per la vendita di prodotti contraffatti.

siti o piattaforme ad elevata consultazione, al fine di intercettare i consumatori, deviandoli verso i siti illegali, aumentando in tal modo il *ranking* commerciale di tali siti: considerato che gli algoritmi di ricerca sul *web* privilegiano i siti maggiormente consultati da parte degli utenti, si ha la c.d. *keyword advertising* quando un sito usa illegittimamente, attraverso *keyword*, un marchio su cui non ha diritti, per aumentare la *page rank* del sito e approdare ai primi posti degli esiti delle ricerche sul *web*;

f) palesi e più facilmente controllabili sono invece gli inserimenti non autorizzati di un marchio in un sito o di un *link*, che rinvia ad un sito legale, non necessariamente per vendere via *web* merce di quel marchio, ma anche per sfruttarne la notorietà in sede di ricerca e dare valore commerciale al sito; tali fattispecie realizzano pratiche di concorrenza sleale e di utilizzazione non autorizzata di siti legali;

g) nel settore del diritto d'autore, segnatamente per gli audiovisivi, mentre la tecnica del *peer to peer* è segnalata in calo, in quanto il relativo protocollo è tracciabile e non criptato e quindi rintracciabile dalle forze di polizia, viceversa sono molto utilizzati i sistemi di *file sharing* illegale come quello del c.d. *cyberlocker* (servizi di archiviazione *web* che ospitano i file degli utenti e sono poi scaricati da utenti terzi, previo pagamento di un abbonamento di accesso al sito), e che consentono uno scambio molto più veloce dei *file*, nascondendo l'organizzatore dell'attività illecita dietro uno schermo societario e allocando i *file* pirata in *server* presso ISP internazionali.

Secondo uno studio dell'Istituto di ricerca IPSOS commissionato dalla FAPAV, citato nel corso delle audizioni in Commissione, la pirateria audiovisiva si può distinguere in pirateria « fisica », essenzialmente con acquisto di DVD contraffatti o copiati, in pirateria « digitale », con il *download*, lo *streaming*, il *peer to peer* o le copie digitali e in pirateria « indiretta », con condivisione di copie illegali tra amici e parenti. Più in generale, lo sviluppo di *internet* ha modificato le caratteristiche della pirateria audiovisiva, in quanto la riproduzione illegale su DVD venduti ai consumatori finali è in netto calo, mentre è in crescita esponenziale la disponibilità illecite di opere dell'ingegno su *internet* (27).

I ricavi dai « cyberlocker » sono stimati in quasi 100 milioni di dollari all'anno nel mondo (28).

Lo studio « Sala e Salotto 2014 » della società Ergo Research, in collaborazione con ANEC, ANICA e CINETEL, riporta che ogni giorno in Italia le visioni illecite di contenuti audiovisivi sono stimate in 1.239.000, a fronte di 1.035.000 visioni lecite (29).

(27) V. operazione *« Italian blackout »* condotta dalla Guardia di Finanza, su cui è stato riferito in audizione in commissione.

(28) Studio *« Behind the cyberlocker door: a report on how shadowy cyberlocker businesses use credit card companies to make millions »* citato nell'audizione del 3 marzo 2016 con il Segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali (FAPAV), Federico Bagnoli Rossi.

(29) Studio citato nell'audizione del 3 marzo 2016 con il Segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali (FAPAV), Federico Bagnoli Rossi.

In indagini della Guardia di Finanza [30] è stato ricostruito un legame diretto tra *cyberlocker*, che organizzavano « siti-vetrina » per la condivisione delle opere – ed *uploaders* della rete che caricavano illegalmente materiale tutelato dal diritto d'autore sulla piattaforma: i gestori del sito fidelizzavano i propri utenti coinvolgendoli nel traffico illecito, corrispondendo loro somme proporzionate al numero di *download* eseguiti sulle opere oggetto di condivisione caricate sulla piattaforma, con un guadagno per la vendita di abbonamenti di accesso al sito pari a 1,3 milioni di euro, a fronte di oltre 460 milioni di download illegali di file protetti dal diritto d'autore.

Per quanto riguarda la pirateria nel campo dei film è stato ricordato in audizione come il 58 per cento dei film sia reperibile illegalmente *on line* dopo i primi tre giorni di programmazione o prima dell'uscita stessa [31].

Secondo uno studio, condotto a livello comunitario dalla società indipendente TERA Consultants, la perdita di valore complessiva nel settore è stimata tra 34,5 e 47,1 miliardi di euro nel periodo tra il 2008 e il 2011, con una perdita complessiva di posti di lavoro quantificabile tra le 200 mila e il milione di unità nel quadriennio [32].

Il problema del *copyright* riguarda anche il *software*, che la legge sul diritto di autore equipara ad opere dell'ingegno. In audizione [33] è stato ricordato come la copiatura di prodotti informatici, in violazione della licenza che i prodotti *software* hanno per l'utilizzo all'interno di aziende, determini danni ingenti sia alle aziende produttrici, prevalentemente internazionali, sia all'indotto sviluppato da aziende italiane: un volume d'affari di circa 63 miliardi di euro in tutto il mondo di *software* piratato, con un tasso di pirateria del 29 per cento in Europa, del 47 per cento in Italia. Una diminuzione di 2,5 punti all'anno consentirebbe di recuperare più di 7.000 posti di lavoro e 5 miliardi di valore di attività complessiva.

Altro fenomeno da considerare è quello del c.d. *dark web* (o « rete oscura ») come parte del *Deep Web* (o rete sommersa o invisibile), ossia quella parte del *World Wide Web* non indicizzata dai comuni motori di ricerca ma raggiungibile attraverso *software* particolari che collegano *internet* e la « *Darknet* » (tra cui i più comuni sono Tor, I2P e Ferente). In particolare il *dark web* è usato per attività illegali. Nel corso di un'audizione svoltasi il 9 marzo 2017 la Guardia di Finanza ha illustrato efficacemente le caratteristiche del fenomeno [34].

Il *deep web* è un insieme di siti *internet*, pagine e contenuti *web*, che, non essendo indicizzati, non possono essere raggiunti dagli utenti attraverso i comuni motori di ricerca, ma solo conoscendo il *link* esatto o disponendo di sistemi identificazione (*username e password)*.

---

(30) V. audizione in Commissione del 16 ottobre 2014 del Comandante generale della Guardia di Finanza *pro tempore,* Capolupo.

(31) V. audizione del 3 marzo 2016 con il Segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali (FAPAV,) Federico Bagnoli Rossi.

(32) Studio citato nell'audizione del 3 marzo 2016 con il Segretario generale della Federazione per la Tutela dei Contenuti Audiovisivi e Multimediali (FAPAV), Federico Bagnoli Rossi.

(33) V. audizione del 3 marzo 2016 del Presidente di *Business Software Alliance* – BSA Italia, Paolo Valcher.

(34) V. audizione del Comandante Unità Speciali della Guardia di Finanza Gennaro Vecchione e del Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza, Giovanni Parascandolo e la relativa documentazione depositata in Commissione, pubblicata in allegato al res. stenografico.

Un dato interessante emerso nel corso dell'audizione citata è che i dati e le informazioni ospitate sul *deep web* rappresentano la quasi totalità dell'intero mondo *internet*, stimato in circa 400 miliardi di documenti complessivi, a fronte di poco più di 3,9-4 miliardi di pagine *web* contenute nel cd. *Surface (o Clear) Web*, indicizzate dai motori di ricerca: la maggior parte dei contenuti del *web* è quindi contenuta nel *deep web*.

Il *dark web* costituisce una piccola parte del *deep web* ma con caratteristiche tipiche di illegalità in quanto in esso possono annidarsi pericolose organizzazioni criminali, gruppi di *hacker*, cellule antagoniste o gruppi terroristici. In esso sono organizzati veri e propri « *marketplace* » che sebbene siano nascosti e non indicizzati, mutuano le caratteristiche espositive di consultazione dei siti di questo tipo dedicati al commercio legale. La Guardia di Finanza ha mostrato alla Commissione come nei *marketplace* del *dark web* siano in vendita una pluralità di materiali illeciti: droga, armi, materiale pedopornografico, documenti di identità rubati o contraffatti, numeri di care di credito, *mail list*, e prodotti contraffatti o piratati. Tali *marketplace* di merce illecita sono molto strutturati, in quanto sono garantiti da sistemi di *feedback* degli utenti basati sulla « credibilità » del venditore e sui quantitativi di prodotti ceduti, e le modalità di pagamento sono assiste da servizi di « *escrow* », ovvero accordi per i quali le somme relative alle merci vendute, prima di essere accreditate sui conti del venditore, sono trattenute da terze parti (solitamente gli amministratori del *marketplace*) fino al momento in cui l'acquirente conferma l'avvenuta consegna delle merci.

Il funzionamento dei *software* che consentono l'accesso al *dark web* è diverso da quello della rete tradizionale, in quanto la comunicazione tra *client* e *server* non è diretta, ma viene « rimbalzata » attraverso altri *server* denominati *relay* che fungono da *router* e rendono molto difficile se non impossibile poter intercettare l'origine, la destinazione e il contenuto dei messaggi e dei dati trasferiti.

Per quanto riguarda specificamente la contraffazione è stato riferito nel corso dell'audizione con la Guardia di Finanza come la minaccia appaia oggi ancora limitata, al contrario degli altri settori merceologici o attività illecite indicate.

I siti esistenti nel *dark web* nel settore della contraffazione sono utilizzati soprattutto per le vendite tra grossisti e non rispetto ai consumatori.

La pericolosità intrinseca di sistema è peraltro rappresentato dall'estrema difficoltà di svolgere attività repressiva rispetto a tale fenomeno. La mancata individuazione dei *client* e l'assenza di indicizzazione, e l'impiego di mezzi di pagamento virtuali rappresentati dalle cripto valute, rendono difficile individuare questi siti che vendono anche prodotti contraffatti. La tecnica di contrasto utilizzata dalla Guardia di Finanza consiste prevalentemente nell'attivazione di onerose procedure di acquisto simulato e operazioni sotto copertura per svolgere le relative attività investigative. Il fenomeno, pertanto, soprattutto in prospettiva, non deve esser sottovalutato [35].

(35) Nel settore della contraffazione, del contrabbando e dello smercio di stupefacenti, rilevante è stato il caso di « *Silk Road* », un sito di commercio elettronico chiuso nel 2013 dall'FBI negli Stati Uniti, e denominato dai media come l'« *Amazon* delle droghe ».

5. LA RESPONSABILITÀ DEGLI INTERNET PROVIDER NELLA NORMATIVA COMUNITARIA E NAZIONALE

L'azione di contrasto alla contraffazione nel commercio elettronico si fonda su una serie di interventi, descritti nel successivo paragrafo 7, che richiedono l'intervento dei *provider* e la cui realizzazione discende dalla responsabilità dei fornitori dei servizi tecnologici per le attività svolte.

La normativa comunitaria di riferimento riguarda due ambiti: in tema di diritti di proprietà industriale fondamentale è la richiamata direttiva sul commercio elettronico 2000/31/CE, recepita in Italia dal decreto legislativo 9 aprile 2003, n. 70, recante « *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico* »; in tema di diritti d'autore, con particolare riguardo ai media audiovisivi, la fonte essenziale è la direttiva 2010/13/EU sui servizi di media audiovisivi (Direttiva SMA).

5.1. I beni tutelati.

Alla base vi è la distinzione tra merci, tutelate dai diritti di proprietà industriale (IPR-*industrial property rights*) e opere dell'ingegno, tutelate dal diritto d'autore (*copyright*: DPI-diritti di proprietà intellettuale).

In generale occorre dire che la tutela degli IPR appare più difficoltosa rispetto a quella del diritto d'autore, per una serie di motivi: per una copertura diversa sul piano normativo, dal momento che la direttiva sul commercio elettronico, che prevede una limitata assunzione della responsabilità dei *provider*, offre in prospettiva, una tutela più limitata rispetto alla normativa in tema di media audiovisivi, ove nelle recenti proposte di modifica che di seguito si esamineranno sono stati previsti obblighi più stringenti a carico delle imprese digitali per evitare la commissione di illeciti; per la difficoltà di identificazione dei falsi e delle contraffazioni relative alle merci, che è già molto difficile rispetto ai prodotti « fisici » imitati con perizia, ma che lo è ancora di più su merci vendute in rete, che spesso non sono nella disponibilità degli ISP e per le quali i controlli hanno per oggetto semplici annunci di vendita *on line* delle merci, con complesse indagini volte ad identificare la sussistenza di licenze di vendita, l'identità degli operatori, e la liceità delle vendite; viceversa, i prodotti audiovisivi coperti da *copyright*, essendo in formato digitale, sono « merci » direttamente presenti nella rete dalla quale si scaricano: l'evoluzione di soluzioni tecnologiche, sempre più adoperate negli ultimi anni in base ad accordi intervenuti tra le piattaforme digitali e le grandi compagnie titolari dei diritti d'autore, permette di riconoscere immediatamente (in generale e in estratto) l'utilizzo non autorizzato di opere coperte da *copyright* (musicali, video, più in generale prodotti digitali) e di attivare forme di tutela o compensazioni risarcitorie.

Occorre, pertanto, trovare soluzioni, anche di carattere tecnologico, per assicurare una maggiore tutela alle aziende titolari di IPR.

Le difficoltà sono notevoli, atteso che l'azione intrapresa dalla Commissione UE per il Mercato unico digitale sembra incentrata più sulla tutela del diritto d'autore che su quella dei diritti di proprietà industriale: infatti, la proposta di direttiva del 14 settembre 2016 è relativa al mercato digitale e segnatamente, per quello che qui interessa, alle piattaforme digitali, e riguarda perciò solo il diritto di autore e non anche i marchi e gli altri segni distintivi dell'azienda; si esclude, invece, in tale sede, ogni modifica alla direttiva sul commercio elettronico.

Su queste questioni si rinvia al successivo paragrafo 7.1.

5.2. La normativa comunitaria in materia di commercio elettronico.

La direttiva 2000/31/CE riguarda gli *Internet Service Provider* (ISP), ossia quelle aziende che forniscono servizi *internet*: dal semplice accesso alla rete a servizi aggiuntivi, in particolare servizi di connessione, trasmissione, e memorizzazione di dati, anche ospitando siti. Il *provider* è quindi un intermediario della comunicazione, attraverso i cui *server* passa sostanzialmente ogni attività veicolata sulla rete, che collega i soggetti che intendono comunicare informazioni e gli utenti delle stesse.

Obiettivo della direttiva è quello di favorire lo sviluppo della rete, ragione per la quale i *provider* non sono ritenuti responsabili per i contenuti immessi dagli utenti se si limitano a far fluire il traffico in rete, svolgendo operazioni tecniche o passive sui contenuti veicolati, qualora non siano o non possano essere a conoscenza di eventuali contenuti illeciti appostati da utenti delle piattaforme. È il cosiddetto principio della « neutralità della rete » (*network neutrality*). Tale attività è considerata « di ordine meramente tecnico, automatico e passivo », in quanto il prestatore dei servizi non conosce né controlla le informazioni trasmesse o memorizzate.

Il decreto legislativo n. 70/2003, che ha recepito la direttiva in Italia, per la responsabilità degli ISP, distingue negli articoli 14, 15 e 16, tre diverse fattispecie di attività dei *provider*:

a) attività di semplice trasporto (*mere conduit*): il *provider* che trasmette in rete informazioni fornite da un destinatario del servizio o fornisce un accesso alla rete di comunicazione, non è responsabile delle informazioni trasmesse se non dà origine alla trasmissione, non seleziona il destinatario della trasmissione e se non seleziona nè modifica le informazioni trasmesse; rientrano in tale definizione i *network provider* che forniscono il solo accesso alla rete attraverso la dorsale *internet* e gli a*ccess provider* che forniscono il solo accesso alla rete attraverso *modem* o connessioni dedicate;

b) attività di memorizzazione temporanea (*caching*): il *provider* che, oltre alle prestazioni di *mere conduit*, memorizza automaticamente, in modo intermedio e temporaneo, le informazioni, al fine di rendere più veloce il successivo inoltro ad altri destinatari, non è responsabile delle informazioni trasmesse, se non modifica le infor-

mazioni, si conforma alle condizioni di accesso alle informazioni e alle norme di aggiornamento delle stesse, se non interferisce con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni e se agisce prontamente per rimuovere le informazioni memorizzate o disabilitare l'accesso, quando sia effettivamente a conoscenza della rimozione delle informazioni dal luogo dove si trovavano inizialmente sulla rete, o che l'accesso alle informazioni è stato disabilitato, oppure che un organo giurisdizionale o un'autorità amministrativa ne abbia disposto la rimozione o la disabilitazione;

c) attività di memorizzazione di informazioni (*hosting*): il *provider* che memorizza informazioni fornite da un destinatario del servizio non è responsabile delle informazioni trasmesse, se non è effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita; non è responsabile, per quanto attiene le azioni risarcitorie, se non è al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, se agisce immediatamente per rimuovere le informazioni o disabilitarne l'accesso. Se, viceversa, il servizio è svolto sotto l'autorità o il controllo del *provider* questi è responsabile. È questo il caso dei *content provider*, quando gli ISP oltre all'accesso sono anche autori dei contenuti pubblicati sui propri server; in giurisprudenza è stato ritenuto che i *content provider,* che forniscono contenuti, rispondono direttamente per gli eventuali illeciti commessi, applicando la normativa sulla stampa, che prevede la responsabilità civilistica del proprietario della pubblicazione e dell'editore in concorso con l'autore dello scritto. Se i contenuti sono immessi da terzi la responsabilità sussiste solo se il *provider* non consente di identificare l'autore del reato.

Questo assetto normativo implica pertanto per i *provider*:

• l'insussistenza di un obbligo di monitoraggio preventivo e generalizzato o generale di sorveglianza sulle informazioni, che il *provider* trasmette o memorizza, anche perché i contenuti trasmessi non sono di sua proprietà; nel caso dei *social network*, inoltre, tali contenuti costituiscono espressione del diritto costituzionale di manifestazione del pensiero, ai sensi dell'articolo 21 della Costituzione, e come tali non possono costituire oggetto di valutazione da parte del *provider*;

• l'esistenza di una responsabilità solo residuale del *provider*, in presenza di comportamenti dolosi;

• l'esistenza di obblighi di adeguata collaborazione con l'autorità giudiziaria o amministrativa, ai cui ordini si devono adeguare, nei casi indicati, rimuovendo i contenuti segnalati e fornendo senza indugio, a richiesta delle autorità, le informazioni in proprio possesso per identificare il destinatario dei servizi con cui vi siano accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite;

• l'esistenza di obblighi, in forza dei commi 2 e 3 dell'articolo 17, di informare senza indugio le autorità qualora il *provider* sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo cliente.

Una disposizione molto rilevante del decreto legislativo n. 70/2003 (e della direttiva) è quella di cui all'articolo 1, comma 2, lettera *d*), che esclude dall'ambito di applicazione di tale normativa le prestazioni di servizi della società dell'informazione effettuate da soggetti stabiliti in Paesi non appartenenti allo spazio economico europeo, esenzione rilevantissima se si considera il fatto che molte delle piattaforme mondiali più importanti sono extraeuropee: l'UE contribuisce solo al 4 per cento della capitalizzazione totale del mercato delle maggiori piattaforme *on line*, poiché la parte preponderante delle stesse ha sede negli Stati Uniti e in Asia [(36)].

Gli ISP, in buona sostanza, non hanno quindi l'obbligo di effettuare un monitoraggio preventivo del contenuto immesso *on line,* ma sono responsabili se non si attivano in caso di notifica.

È questa la cosiddetta procedura del *Notice and Take Down*, che la direttiva 2000/31/CE auspica sia introdotta da parte degli Stati. Allo stato risulta che solo la Finlandia, per il diritto d'autore, abbia adempiuto a tale previsione. In Italia alla procedura del *Notice and Take Down* fa testuale riferimento l'articolo 5 del Regolamento AGCOM del 680/13/CONS del 12 dicembre 2013. Tuttavia, un riferimento a tale procedura è implicitamente contenuto negli articoli 14, 15 e 16, del citato decreto legislativo n. 70/2003, allorquando prevedono che l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, possono esigere, anche in via d'urgenza, che il *provider* impedisca o ponga fine alle violazioni commesse [(37)]. Nella prassi tale procedura è attivata spesso su segnalazione dei titolari dei diritti tutelati, siano essi IPR o *copyright*, a prescindere da un intervento delle autorità competenti.

Uno dei problemi che è emerso nel corso dell'audizioni in Commissione rispetto alla normativa vigente è rappresentato dal fatto che la distinzione giuridica relativa ai *provider,* contenuta nella direttiva sul commercio elettronico 31/2000/CE, risulta oggettivamente obsoleta e, di fatto, superata dall'evoluzione dei servizi offerti sulla rete. Nei meno di vent'anni intercorsi tra il periodo di elaborazione ed approvazione della direttiva – un tempo enorme stante l'evoluzione tecnologica e commerciale dell'ambiente digitale – i servizi forniti dagli ISP sono divenuti estremamente più articolati e sofisticati, in molte direzioni.

In generale, il ruolo sociale ed economico delle piattaforme *on line* è oggi estremamente diversificato, in quanto forniscono mercati di *e-commerce*, motori di ricerca, sistemi di pagamento, *social media*, siti per la condivisione di contenuti e di video, ecc., piattaforme pubblicitarie *on line*, piattaforme di distribuzione di applicazioni, servizi di comunicazione, piattaforme per l'economia collaborativa, ecc.

(36) V. comunicazione della Commissione COM(2016) 288 final del 25.5.2016 « Le piattaforme *on line* e il mercato unico digitale Opportunità e sfide per l'Europa ».

(37) Sul punto della lacunosità della normativa comunitarie nazionale si vedano le considerazioni critiche del Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale (FPM), Luca Vespignani, espresse in audizione il 18 maggio 2016.

Nella rete operano una serie di soggetti che agiscono sempre più in base a schemi di attività che non rientrano nelle tre classificazioni individuate dalla direttiva sull'*e-commerce* e che non possono essere rubricati in un ruolo meramente neutrale o passivo, quale quello svolto all'origine da società di telecomunicazioni che si limitavano a stabilire la connessione tra domini ed utenti (ad esempio gestione dei *server*, connessioni fisiche, algoritmi di ricerca, ecc.).

Si tratta invece di un ruolo attivo nella gestione, selezione e organizzazione dei contenuti creativi. Si parla ormai comunemente di realtà digitali definite come OTT (*Over The Top*), ossia imprese che forniscono attraverso *internet* servizi variegati, con contenuti video e applicazioni di tipo « *rich media* », quale, ad esempio, le pubblicità che appaiono sulle pagine di siti *web* mentre li si visitano e che dopo una durata prefissata scompaiono: nella redazione del messaggio commerciale che accompagna il *link* pubblicitario o nella determinazione o selezione di tali parole chiave, i *provider* svolgono un ruolo attivo. Il profilo sul quale occorre riflettere è quello di un dovere di diligenza (c.d. *duty of care*) per gli intermediari di questo tipo, dal quale consegua la responsabilità per la predisposizione di comportamenti positivi di contrasto.

Per questi operatori va affrontato il problema se si possa continuare ad applicare un'esenzione sostanziale di responsabilità come quella prevista dalla direttiva sull'*e-commerce*, che non prevede un obbligo di sorveglianza.

Nel corso dell'audizione del 20 gennaio 2016 con il sottosegretario alla Presidenza del Consiglio con delega ai rapporti con l'UE, Sandro Gozi, è stato sottolineato come l'aspetto più controverso nell'applicazione del regime di responsabilità degli intermediari sia quello riguardante proprio « *la corretta qualificazione di hosting provider, a seconda che rivesta nel caso concreto un ruolo meramente passivo rispetto a quando fornisce anche servizi diversi dal mero stoccaggio delle informazioni* ». Si tratta di un aspetto giuridico molto complesso, che richiede una migliore e più chiara interpretazione.

Va pertanto aggiornata una riflessione circa l'applicazione di norme differenziate in ragione delle specifiche tipologiche degli ambienti digitali e dei corrispondenti profili di responsabilità.

A titolo di esempio, è stato approfondito in audizione il ruolo di uno dei colossi del settore, *Google*, che oltre ad essere primario motore di ricerca è altresì importante operatore di pubblicità *on line*, sia attraverso *keywords* sul motore di ricerca, sia attraverso un programma di erogazione di *banner* su siti terzi che entrano nei programmi di *Google* [38].

Le piattaforme hanno conosciuto un'evoluzione legata all'andamento del mercato: ad esempio in Commissione è stato illustrato da *eBay Inc*., nata come piattaforma per la vendita di prodotti di seconda mano, come l'80 per cento delle inserzioni mondiali oggi disponibili sulla piattaforma sia effettuata da parte di venditori professionisti di merci nuove [39].

---

(38) V. audizione del 21 luglio 2016 di Daniele Sesini, Direttore generale di I.A.B. Italia.

(39) V. audizione del 5 ottobre 2016 con Andrea Rota, *Senior Director Global Brand Protection* e Stefan Krawczyk, *Associate General Counsel and Head Government relations International* di *eBay Inc*.

Un altro esempio che la Commissione ha avuto modo di approfondire nel corso delle audizioni è quello di *Alibaba*. Il gruppo nel suo complesso presenta una diversificazione di attività che copre il ciclo completo del mondo dell'*e-commerce*: piattaforme dedicate al mercato cinese, a quello mondiale e altre riservate alle esportazioni delle imprese mondiali in Cina o nella regione ASEAN (*Taobao.com,* di tipo B2C-*business to consumer*) e C2C (*consumer to consumer*), *Tmall,* di tipo B2C, *Tmall Global*, *AliExpress*, *Lazada*); una piattaforma di pagamenti *on line* (*AliPay*); una rete logistica (*CAINIAO*) per la consegna dei prodotti acquistati; servizi e raccolta di dati di *cloud computing* per gli esercenti (*Alibaba Cloud*); piattaforme di contenuti digitali e contenuti di intrattenimento, per la diffusione di servizi a livello transfrontaliero [(40)].

In audizione *eBay Inc.* ha riferito del superamento dei problemi riscontrati con titolari di marchi famosi nel settore della moda e degli accessori (sia per lamentata contraffazione che per la vendita di tali merci al di fuori dai canali di distribuzione tradizionali, con conseguente aumento del contenzioso legale) con la sottoscrizione, nel 2011, di un *memorandum* di intesa promosso dalla Commissione UE sulla lotta alla contraffazione *on line*, firmato anche da altri primari operatori (quali *eBay, Amazon, PriceMinister, Allegro*, ecc.) e da marchi prestigiosi (*Burberry, Lacoste, Chanel, Nike, Luxottica, Moncler, Procter & Gamble, Adidas*, ecc.). Questi accordi volontari, se da un lato segnalano la bontà della via pattizia tra le parti per affrontare il problema alla luce delle mutate condizioni, dall'altro evidenziano implicitamente come il quadro delle regole comunitarie e nazionali risulti fortemente datato.

Queste realtà sono dunque emblematiche di quale sia il ruolo delle piattaforme digitali oggi e come occorra guardare alla dimensione complessiva delle *holding* di controllo per valutarne il ruolo e la potenzialità in termini di intervento a tutela della affidabilità degli standard di sicurezza per la tutela dei consumatori e dei diritti delle aziende produttrici. Basti pensare che gli attuali maggiori *player* operanti nel settore delle piattaforme commerciali (es. *Alibaba* e *Amazon*) non esistevano o erano stati appena costituiti nel momento di entrata in vigore della direttiva.

Il tema in discussione tra gli *stakeholders* e presso le istituzioni comunitarie è dunque il seguente: poiché le piattaforme svolgono un ruolo sempre più importante, in termini di accesso alle informazioni e ai contenuti, ciò comporta necessariamente l'assunzione da parte loro di maggiori responsabilità.

Va peraltro considerato, in termini economici ed occupazionali, che mentre l'industria manifatturiera in Italia impiega poco meno di 6 milioni di lavoratori, gli addetti degli intermediari del *web* sono molto più limitati, circa 220.000 unità [(41)], pur a fronte di profitti dell'economia digitale molto rilevanti e in costante crescita. Da tale

(40) V. audizione di Eric C. Pellettier, Vice Presidente e capo degli affari istituzionali internazionali e di Rodrigo Cipriani Foresio, Direttore esecutivo per Italia, Spagna, Portogallo e Grecia di *Alibaba Group* del 13 ottobre 2016.

(41) Il dato nelle attività manifatturiere, per il 2015, pari a 5.481,942 addetti, è tratto dal Rapporto sulla competitività dei settori produttivi dell'ISTAT; il dato degli addetti nell'« economia digitale », tratto dall'indagine svolta da IAB Italia ed Ernst & Young per il 2015, aggrega i settori della raccolta pubblicitaria via *internet,* servizi accessori ADV, tecnologia, servizi professionali ed *e-commerce*.

considerazione discende il fatto che in sede normativa europea ed internazionale si debbano contemperare gli interessi in gioco, costituiti dal complesso imprese-lavoratori delle due realtà, senza contare gli effetti sistemici della contraffazione in termini di danni erariali e di ordine pubblico causati agli Stati.

Il punto di equilibrio da raggiungere è quello di utilizzare soluzioni tecnologiche condivise, idonee a conseguire la salvaguardia di tutti gli interessi coinvolti, senza contrapposizioni di natura ideologica: da un lato, le libertà essenziali di espressione e di opinione; da un altro, la libertà e il valore dell'espansione del commercio *on line;* dall'altro lato ancora la tutela delle corrette regole dell'impresa e dei consumatori e del diritto d'autore, negli ambiti rispettivamente dei diritti di proprietà industriale e del *copyright*.

La Commissione europea sta lavorando su questo aspetto, ma occorre sottolineare che non sembra ancora maturata una visione netta ed innovativa dei problemi sul tappeto.

In una comunicazione del 25 maggio 2016 della Commissione europea si legge che: « *l'attuale regime di responsabilità relativo ai prestatori intermedi di servizi, definito dalla direttiva sul commercio elettronico, è stato concepito in un'epoca in cui le piattaforme on line non presentavano le caratteristiche e la portata che hanno oggi, ma ha creato un ambiente normativo tecnologicamente neutro che ha sensibilmente agevolato il loro sviluppo* ».

Nel maggio del 2015, la Commissione europea ha avviato un'indagine di settore sul commercio elettronico di beni di consumo e di contenuti digitali, nell'ambito della strategia per un mercato digitale unico, al fine di delineare il quadro delle tendenze di mercato e di individuare le problematiche di concorrenza presenti sui mercati europei, evidenziando le potenziali barriere alla libera concorrenza e le pratiche commerciali potenzialmente restrittive della stessa. I risultati dell'indagine, frutto dell'analisi dei dati di circa 1.800 imprese e di circa 8.000 operatori di *e-commerce* di numerosi settori merceologici, sono stati pubblicati in una relazione preliminare del 15 settembre 2016, sottoposta a una consultazione pubblica (si prevede che la Commissione pubblichi una relazione finale nel primo trimestre del 2017).

Di questo orientamento prudenziale circa la revisione della direttiva sull'*e-commerce* della Commissione europea, la nostra Commissione ha preso atto nel corso dell'incontro con la Direzione CNECT – Direzione generale per comunicazioni, network, contenuto e tecnologie – a Bruxelles il 27 e 28 giugno 2016. Nel corso dell'audizione la vicedirettrice Bury ha affermato che: « *quando si parla di Notice and Stay Down bisogna procedere con cautela, perché alcuni contenuti sono chiaramente illegali, ma abbiamo tante zone grigie e per questo dobbiamo stare attenti al nostro intervento, perché è necessario garantire la libertà di espressione del contenuto, ma anche la libertà di fare ricorso nel caso in cui il contenuto venga ritirato.* »

Nelle proprie audizioni la Commissione ha avuto modo di approfondire il punto di vista delle imprese digitali (ISP), che nelle posizioni delle associazioni di categoria, hanno ribadito l'adesione ai cardini della direttiva sull'*e-commerce*, e che, pertanto: « *l'unico ruolo che i prestatori di servizi di comunicazione possono attualmente*

rivestire ai sensi della normativa vigente è quello di recepire ordini di autorità competenti e dare loro corso. Non possono intervenire prima o sostituirsi a esse »[(42)].

Sul tema del superamento del principio del *Notice and Take Down* verso le forme preventive del *Notice and Stay Down* si rinvia al successivo paragrafo 8.

5.3. La normativa comunitaria in materia di diritto d'autore per i media audiovisivi.

L'altro complesso normativo comunitario rilevante anche per la contraffazione è quello relativo al diritto d'autore, segnatamente per il settore degli audiovisivi.

La direttiva 13 del 10 marzo 2010 (cosiddetta direttiva SMA), che ha sostituito le direttive 89/552/CE, 97/36/CE e 2007/65/UE, recepite in Italia dal decreto legislativo n. 44/2010, concerne la fornitura di servizi di media audiovisivi. La Commissione d'inchiesta, nel corso della citata missione svolta a Bruxelles[(43)], ha potuto confrontarsi sul tema dell'aggiornamento in corso di tale normativa UE, con un nuovo approccio per le piattaforme digitali *on line* che operano nel settore: la Commissione europea, nel quadro della strategia per il mercato unico digitale, ha effettuato, il 25 maggio 2016, una Comunicazione sulle piattaforme digitali e ha proposto un aggiornamento della direttiva 13/2010[(44)], formalizzato con la proposta di direttiva COM(2016) 287 final 2016/0151 (COD) del 25 maggio 2016, nonché, successivamente, la proposta di direttiva, del 14 settembre 2016, sul diritto d'autore nel mercato unico digitale COM(2016) 593-2016/0280 (COD).

Per quello che rileva ai fini della presente relazione, si segnala che nella Comunicazione, la Commissione, in continuità con la strategia per il Mercato Unico Digitale presentata nel maggio 2015, dà conto di come il parere di più di due terzi dei partecipanti alla consultazione pubblica tenuta dall'UE ritenga necessario, per categorie di contenuti illegali diversi, approcci strategici mirati, a livello di procedure di segnalazione e intervento e che, mentre i titolari di diritti richiedono l'adozione di procedure *Notice and Stay Down*, gli intermediari digitali ritengono che l'attuale esenzione dalla responsabilità sia adeguata.

La questione è delicata, sia dal punto di vista politico che imprenditoriale. La comunicazione dà conto che alcune piattaforme *on line,* intervenute nella consultazione, hanno espresso il timore, nel caso di provvedimenti ampliativi della responsabilità degli ISP anche nel caso di illeciti, di una violazione della direttiva sul commercio elettronico.

---

(42) V. affermazioni del Presidente di Confindustria digitale, Elio Catania, nell'audizione del 27 luglio 2016.

(43) V. resoconto dell'incontro con Claire Bury, Vicedirettrice generale DG CNECT–Direzione generale per comunicazioni, network, contenuto e tecnologie, sito internet Camera dei deputati, http://www.camera.it/leg17/1203 ?shadow–organo–parlamentare=2368&natura=M).

(44) La Commissione ha effettuato una serie di consultazioni pubbliche, sia sul diritto d'autore, sia, tra il 24 settembre 2015 e il 6 gennaio 2016, sul quadro normativo per le piattaforme, gli intermediari *on line*, i dati e il *cloud computing* e l'economia.

La Comunicazione, come già richiamato, pur dando conto che l'attuale regime di esonero dalla responsabilità degli ISP è stato concepito in un'epoca in cui le piattaforme *on line* non avevano le caratteristiche odierne, in un contesto tecnologico e di mercato molto diverso, riconosce che tale assetto normativo, definito come « tecnologicamente neutro », ha sensibilmente agevolato lo sviluppo del settore. Il rapporto, conclusivamente, prende atto del fatto che, nonostante nella consultazione siano state espresse alcune preoccupazioni su aspetti attinenti a tale disciplina, i principi in tema di responsabilità godono di ampio sostegno, esprimendo l'indirizzo che tale scelta sia « *fondamentale per lo sviluppo futuro dell'economia digitale nell'UE e per sbloccare gli investimenti a favore degli ecosistemi di piattaforme* », senza la previsione allo stato di modifiche alla direttiva sull'*e-commerce*.

In tema di contrasto a illeciti veicolati nell'ambiente *web* la Comunicazione ritiene necessario, considerando anche gli sviluppi futuri tecnologici, migliorare la protezione degli utenti, garantire parità di condizioni, e stimolare un comportamento responsabile da parte degli intermediari, al fine di rafforzare la fiducia nell'ambiente delle piattaforme *on line*. Il punto 2), in particolare, richiede una condotta responsabile delle piattaforme *on line* in tema di tutela dei minori (es. video pornografici, abusi sessuali sui minori, ecc.), e di contrasto ai messaggi di incitamento all'odio (c.d. *hate speech*, in tema di siti apologetici di atti di violenza, di terrorismo, di discriminazioni razziali).

L'approccio concreto è duplice.

Da un lato la Commissione ha promosso azioni consensuali su base volontaria tra autorità e imprese informatiche finalizzate a garantire tale tutela: il codice di condotta con le imprese informatiche contro l'incitamento all'odio *on line*; il Forum dell'UE sui contenuti terroristici; la coalizione CEO (*Corporate Europe Observatory*) per rendere *internet* un luogo migliore per i bambini; da ultimo, il 6 maggio 2016, il Codice di comportamento tra Commissione e grandi aziende informatiche (cui hanno aderito *Facebook*, *Twitter*, *YouTube*, *Microsoft* e altre aziende informatiche) per l'adozione di procedure chiare ed efficaci di esame delle segnalazioni riguardanti l'incitamento all'odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l'accesso, oltre all'adozione di regole per gli utenti contro l'istigazione alla violenza e ai comportamenti improntati all'odio [(45)].

Dall'altro lato sono introdotte soluzioni normative per prevedere obblighi positivi di azione a carico degli ISP per prevenire determinate fattispecie illecite e per affrontare il tema del *value gap*, circa l'attribuzione dei profitti derivanti dall'utilizzo, anche non autorizzato, dei media audiovisivi.

Le modifiche alla direttiva SMA in tema di responsabilità, impongono alle piattaforme dedicate alla condivisione di video l'ob-

(45) Nella comunicazione si fa riferimento a giurisprudenza della Corte europea dei diritti dell'uomo in merito alla libertà di espressione, che distingue tra contenuti che « *offendono, scuotono o disturbano lo Stato o un qualunque settore della popolazione* », che rientrano nella libertà e quelli che contengono un vero e proprio grave incitamento alla violenza o all'odio, che invece gli Stati possono sanzionare o vietare.

bligo di prevedere mezzi per la tutela dei minori e contro l'incitamento all'odio, da attuare innanzitutto mediante la coregolamentazione; per quanto riguarda la tutela dei minori, la direttiva riveduta prevede l'allineamento delle norme di tutela per la radiodiffusione televisiva e per i servizi a richiesta. L'articolo 12 prescrive che i programmi che possono nuocere allo sviluppo fisico, mentale o morale dei minori, siano accessibili solo in maniera tale da garantire che gli stessi non possano, in condizioni normali, vederli o ascoltarli; ciò vale indipendentemente dal fatto che tali programmi siano trasmessi da emittenti televisive o proposti da un fornitore di servizi di media a richiesta; alla direttiva SMA è aggiunto un articolo 28-*bis*, che introduce l'obbligo per gli Stati membri di assicurare che i fornitori di piattaforme per la condivisione di video pongano in essere, preferibilmente mediante coregolamentazione, opportune misure preventive atte a proteggere i minori dai contenuti nocivi per lo sviluppo fisico, mentale o morale e proteggere tutti i cittadini dall'istigazione alla violenza o all'odio, con riferimento a discriminazioni per il sesso, la razza, la religione, l'ascendenza, l'origine nazionale o etnica. Si tratta di misure preventive, adeguate in base alla natura dei contenuti in questione, dei danni causabili, delle caratteristiche delle persone da proteggere, nonché dei diritti e degli interessi legittimi, compresi quelli dei fornitori della piattaforma per la condivisione di video e degli utenti che hanno creato e/o caricato contenuti, nonché dell'interesse pubblico, quali: meccanismi di segnalazione da parte degli utenti delle piattaforme di tali contenuti illeciti (dando comunicazione a questi del seguito dato alle segnalazioni); sistemi per verificare l'età degli utenti delle piattaforme; sistemi di controllo parentale.

Di particolare importanza è la norma che prevede, da un lato, che gli Stati membri non possano imporre ai fornitori di piattaforme misure più rigorose di quelle indicate, ma, dall'altro, possano imporre misure più rigorose in relazione a contenuti illeciti, fatto salvo il rispetto dei principi di cui agli articoli 14 e 15 della direttiva 2000/31/CE, o all'articolo 25 della direttiva 2011/93/UE. Questa norma, se pur generica, apre la strada, in linea teorica, alla possibilità di ampliare la responsabilità dei *provider* su altre fattispecie illecite.

Nella proposta di direttiva del 14 settembre 2016 sul diritto d'autore nel mercato unico digitale COM(2016) 593-2016/0280 (COD) va segnalata la richiamata questione del cosiddetto *value gap*, relativa ai profitti delle imprese digitali e dell'assegnazione dei ricavi derivanti per l'uso dei contenuti protetti dal diritto d'autore caricati dagli utilizzatori finali e messi a disposizione del pubblico. La questione era stata posta anche alla Commissione d'Inchiesta da parte delle associazioni nel corso delle audizioni. Il tema è quello, rilevante del rapporto tra ISP e titolari del diritto d'autore (che rappresenta un profilo di carattere generale applicabile in futuro anche rispetto ai titolari di IPR), dell'equità della ripartizione, tra i distributori e i titolari dei diritti, comprese le piattaforme *on line*, per il valore generato dalle nuove forme di distribuzione digitale [(46)]. La modifica alla direttiva in tema di pirateria digitale riguardante i media audio-visivi, prevede: « *la costituzione e l'applicazione di meccanismi di*

(46) Sul tema v. Comunicazione della Commissione « Verso un quadro normativo moderno e più europeo sul diritto d'autore » COM(2015) 626 final del 9.12.2015.

cooperazione su base volontaria che permettano, utilizzando un approccio "Follow the Money", di privare le persone che commettono violazioni commerciali dei diritti di proprietà intellettuale delle entrate provenienti da tali attività illegali ». A tal fine gli articoli 13, 14 e 15 della citata proposta di modifica della direttiva introducono, a tutela del diritto d'autore, obblighi positivi di intervento a carico degli ISP, che memorizzano e danno pubblico accesso ad opere caricate dagli utenti (*user generated content*). Compete a loro adottare, in collaborazione con i titolari dei diritti, misure, quali l'uso di tecnologie efficaci per il riconoscimento dei contenuti, per garantire il funzionamento degli accordi conclusi con i titolari di DPI per l'uso delle loro opere e impedire che queste ultime siano messe a disposizione in violazione dei diritti sulle loro piattaforme. Gli Stati membri provvedono a che i prestatori di servizi istituiscano meccanismi di reclamo e ricorso per gli utenti in caso di controversie e facilitano la collaborazione tra i prestatori di servizi digitali e i titolari dei diritti, al fine di definire le migliori prassi e l'uso di tecnologie adeguate e proporzionate per il riconoscimento dei contenuti, tenendo conto della natura dei servizi, della disponibilità delle tecnologie e della loro efficacia, alla luce degli sviluppi tecnologici [(47)]. Gli autori ed artisti devono ricevere, periodicamente e tenendo conto delle specificità di ciascun settore, informazioni tempestive, adeguate e sufficienti sullo sfruttamento delle loro opere ed esecuzioni da parte di coloro ai quali hanno concesso in licenza o trasferito i diritti, in particolare per quanto riguarda le modalità di sfruttamento, i proventi generati e la remunerazione dovuta. È inoltre previsto un meccanismo di adeguamento contrattuale a favore degli stessi, con il diritto di chiedere una remunerazione ulteriore se quella inizialmente concordata risulta sproporzionatamente bassa rispetto ai proventi e ai benefici originati in un secondo tempo dallo sfruttamento delle loro opere o esecuzioni.

L'introduzione di forme di ulteriori responsabilità per gli ISP in determinate fattispecie di illecito e la previsione di meccanismi per perequare il *value gap*, riguardano soltanto il diritto d'autore, anche se non si può escludere il fatto che, in forza di tale precedente, potrebbe poi, in una fase successiva, essere valutata l'introduzione di maggiori forme di tutela anche per i titolari di IPR.

6. LA RESPONSABILITÀ DEGLI INTERNET PROVIDER NELLA GIURISPRUDENZA

I contributi della giurisprudenza sono importanti per l'allargamento delle forme di tutela nel caso di fattispecie di contraffazione.

Nel senso di riconoscere le limitazioni alla responsabilità vanno ricordate tre sentenze della Corte di giustizia europea.

La sentenza del 23 marzo 2010 per il caso « *Google adwords vs Lvmh* », ha riconosciuto per il servizio della piattaforma la possibilità di

(47) Nell'audizione del 10 novembre 2016 *Google* ha criticato questa misura, ritenendo che un monitoraggio preventivo di *internet* alla ricerca di possibili contenuti illeciti costituisca una violazione del principio dell'assenza di un obbligo generale di sorveglianza per gli ISP sancito dalla direttiva *e-commerce* e un disincentivo all'implementazione di *partnership* e accordi di co-regolamentazione.

impiegare a scopo pubblicitario « *parole chiave corrispondenti a marchi altrui nell'ambito di un servizio di posizionamento su internet* » [(48)]: è stato precisato che per gli ISP valgono le limitazioni alla responsabilità dell'intermediario contemplate dalla direttiva sul commercio elettronico 31/2000/CE, in quanto le attività di tali operatori sono da ritenersi « *di ordine meramente tecnico, automatico e passivo* ».

Nella sentenza del 12 luglio 2011 « L'Oreal vs e-Bay » la Corte di Giustizia ha precisato che quando prodotti, che si trovano in uno Stato terzo – recanti un marchio registrato in uno Stato membro dell'Unione o un marchio comunitario e non commercializzati precedentemente nello Spazio economico europeo o nell'Unione – sono venduti *on line* da un operatore economico senza il consenso del titolare del marchio ad un consumatore che si trova nel territorio per il quale il marchio di cui trattasi è stato registrato, o sono oggetto di un'offerta in vendita o di pubblicità in tale mercato, il titolare del marchio può opporsi alla vendita, all'offerta in vendita o alla pubblicità in forza delle norme di cui all'articolo 5 della direttiva 89/104/CEE sul ravvicinamento delle legislazioni degli Stati Membri in materia di marchi d'impresa, come modificata dall'Accordo sullo Spazio economico europeo del 12 maggio 1992 o all'articolo 9 del regolamento (CE) del Consiglio 20 dicembre 1993, n. 40/94, sul marchio comunitario. È compito dei giudici nazionali valutare caso per caso se sussistano elementi pertinenti per concludere che un'offerta in vendita o una pubblicità che compare in un mercato *on line* accessibile in detto territorio sia destinata a consumatori che si trovano in quest'ultimo.

La sentenza « UPC Telekabel Wien contro Constantin Film Verleih ed altri », la Corte di giustizia ha riconosciuto il diritto dei giudici austriaci ad ingiungere alla Telekabel, fornitore di accesso ad *Internet* per il sito *Internet* kino.to, di vietare l'accesso a tale sito per la visione o il *download* di film senza il consenso delle società in possesso di diritti cinematografici, per violazione della normativa sul diritto d'autore.

In Italia, in sede civile, in senso ampliativo della responsabilità, devono essere ricordate due importanti sentenze che hanno stabilito che le piattaforme digitali che ospitano video caricati dagli utenti, non possono usufruire dell'esenzione di responsabilità (c.d. *safe harbor*), ma hanno invece un obbligo di attivarsi (c.d. *duty of care*) per la prevenzione di successive violazioni, considerando la natura sostanziale non di mero e semplice *hosting provider*, ma *hosting* di nuova generazione o *content provider*, essendovi un intervento attivo consistente nell'organizzazione e indicizzazione dei contenuti ospitati, con piani di sfruttamento pubblicitario rapportati alla tipologia dei clienti, con introiti rilevanti.

La prima sentenza, del 27 aprile 2016 emessa dalla Nona Sezione del Tribunale Civile Tribunale di Roma, ha condannato al risarcimento dei danni, per violazione del *copyright* televisivo, per uso illecito

(48) Nel caso di specie dal titolare di marchio Louis Vuitton era stata sostenuta la violazione del *trademark* nella pratica di far comparire il negozio di un rivenditore tra i *link* sponsorizzati, comparendo in cima alla classifica dei risultati quando un navigatore ricerca parole come « borsa » o « Louis Vuitton », pur non appartenendo il *brand* in oggetto al *merchant* in quanto questo tipo di utilizzo, secondo la sentenza della Corte europea, *« non viola il copyright dei marchi nel consentire agli inserzionisti l'acquisto di parole chiave corrispondenti ai trademark »*.

di programmi televisivi di *Mediaset*, la piattaforma digitale statunitense Break.com, *provider* che pubblicava contenuti caricati dagli utenti.

La sentenza del 17 luglio 2014 del Tribunale di Torino, sez. Tribunale delle imprese, ha emesso provvedimento cautelare nei confronti di *YouTube*, affinché la piattaforma si attivasse direttamente, utilizzando il sistema tecnologico di filtraggio *Content ID*, dopo una prima segnalazione inviata dalla società Delta TV, titolare del *copyright* relativi alla versione italiana di *telenovelas* che lamentava la presenza su *YouTube* di diversi episodi, per porre fine alle violazioni esistenti e prevenire nuove violazioni attuate mediante la pubblicazione (ad opera dello stesso soggetto o di terzi) dei medesimi contenuti, specificamente individuati dal titolare del diritto.

Un caso di grande risonanza presso l'opinione pubblica riguardante i *social network* e l'obbligo di porre in essere azioni positive è quello contemplato nell'ordinanza del 3 novembre 2016 del Tribunale di Napoli, su un reclamo presentato da *Facebook* contro una precedente ordinanza del 10 agosto 2016, che aveva disposto l'obbligo per alcuni social, tra i quali *Facebook*, a rimuovere video e commenti relativi ad un caso di una donna, poi suicidatasi, che aveva chiesto la rimozione dalla rete di materiale audiovisivo concernente propri rapporti sessuali.

In sintesi il Tribunale ha ritenuto che, anche se non sussiste un obbligo generale di sorveglianza e un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite per i soggetti che, come Facebook, forniscono un servizio di *hosting provider* rispetto a contenuti illeciti pubblicati negli spazi messi a disposizione dal *provider* medesimo – obbligo che non si rinviene nell'articolo 17 del decreto legislativo n. 70/2003 e che non può desumersi dalla disciplina generale della responsabilità civile – deve ritenersi sussistente una responsabilità per le informazioni oggetto di memorizzazione durevole od « *hosting* », ai sensi dell'articolo 16, comma 1, lettera *b)* del citato decreto legislativo, laddove il *provider* sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita e non si sia attivato per impedire l'ulteriore diffusione della stessa. Tale obbligo sussiste indipendentemente dal fatto che sia intervenuto un ordine dell'autorità ed anche nel caso in cui la richiesta di rimozione dei contenuti illeciti provenga dalla parte che assume essere titolare dei diritti.

Molto significativa per il contemperamento degli interessi dei *provider* e delle aziende titolari di IPR e DPI è la giurisprudenza degli Stati Uniti, che appare più aperta di quella della Corte di giustizia UE nel riconoscere la responsabilità degli ISP.

La normativa americana in tema di *copyright* (DMCA - *Digital Millennium Copyright Act*) prevede il criterio della « conoscenza effettiva » da parte degli ISP, quando il *provider* riceva una notificazione dal soggetto che lamenta una lesione del proprio diritto (IPR o *copyright*). In caso di inottemperanza l'ISP è responsabile, a titolo di concorso, dell'illecito. Se la notifica si rivela infondata il *provider* è sollevato da eventuali responsabilità civili verso il fruitore del servizio su *internet*.

La sentenza n. 10-15909, del 9 settembre 2011 della US Court of Appeals, Ninth Circuit, caso Louis Vuitton S.A. vs Akanoc Solutions,

Inc., società di *web hosting* in California che aveva fornito spazio *web*, banda e indirizzi IP a commercianti cinesi di prodotti contraffatti, ha condannato l'ISP a pagare a Louis Vuitton 10,8 milioni di dollari di danni, per *contributory trademark infringment* e *contributory copyright infringment*.

Nella sentenza Tiffany (NJ) Inc. vs *eBay Inc*., n. 04 Civ. 4607 (RJS) (S.D.N.Y. del 14 luglio 2008) è stato riconosciuto il ruolo di *eBay* nel ridurre la vendita di beni contraffatti, con la possibilità di ricorsi stragiudiziali da parte dei titolari di marchi e l'adozione non di comportamenti passivi ma di comportamenti proattivi, attraverso il programma VeRO [(49)], motore di ricerca antifrode oltre ad interventi manuali mirati.

Nella sentenza della Corte Federale della Virginia del 1º dicembre 2015, Cox Communications vs BMG Rights Management, società che gestisce diritti nel campo musicale, vi è stata la condanna dell'ISP al pagamento di 25 milioni di dollari in una causa di pirateria musicale, perché il *provider* non aveva ragionevolmente messo in atto una *policy* aziendale volta a dar termine alle violazioni poste in essere da propri abbonati, ritenendo che ciò configurasse una violazione volontaria del *copyright* ed escludendo l'applicazione della c.d. clausola « porto sicuro » del Digital Millennium Copyright Act americano. La sentenza segna un passaggio concettuale dal *Notice and Take Down* al *Notice and Stay Down*, ritenendo non sufficiente la semplice rimozione, ampiamente superabile con la reimmissione dei contenuti illeciti, ma richiedendo che l'ISP si attivi responsabilmente perché, una volta rimosso, il contenuto illecito non possa più essere caricato.

7. LE CARATTERISTICHE DEL MERCATO DEL COMMERCIO ELETTRONICO RISPETTO ALLA CONTRAFFAZIONE

7.1. L'incidenza delle diverse tipologie di commercio elettronico sull'efficacia del contrasto alla contraffazione.

Una questione particolarmente importante, emersa con chiarezza negli approfondimenti svolti in audizione nell'esaminare le modalità concrete di contrasto alle forme di contraffazione via *web*, è quella della differenziazione tipologica delle piattaforme e dei *provider*.

L'audizione con *Google* del 10 novembre 2016, ha mostrato con chiarezza come i problemi di approccio a strategie anti-contraffazione siano diversi a seconda del tipo di servizi offerti dall'ISP, con diverse strategie e una diversa efficacia dei risultati ottenuti [(50)].

Si devono distinguere le piattaforme di *hosting*, pubblicitarie e non, dai motori di ricerca e dai *social network*.

Le piattaforme di *hosting* pubblicitarie sono piattaforme meramente commerciali, attraverso le quali soggetti terzi promuovono i propri beni e servizi. Rispetto ad esse le forme di tutela preventiva sono più efficaci, in quanto l'accesso ad esse è condizionato ad

(49) *Verified Rights Owner (VeRO) Program.*

(50) V. audizione del 10 novembre 2016 del responsabile delle relazioni istituzionali di *Google* Enrico Bellini, e di Marta Staccioli, del *Litigation Counsel* per Italia e Grecia di *Google*.

accettazione del *provider* che può quindi svolgere forme di controllo proattivo.

Nel caso di *AdWords* e di *Google Shopping*, ad esempio, servizi che permettono la pubblicizzazione di annunci *on line* per la vendita di beni o servizi, *Google* ha riferito in audizione che la propria *policy*, obbligatoria per gli inserzionisti all'apertura dell'*account*, vieta assolutamente, sia nell'annuncio sia nel rinvio a siti *web* di destinazione, la vendita e la promozione di articoli contraffatti, che contengono un marchio identico o imitativo di marchi legali ovvero violazioni del *copyright*. Inserzioni di questo genere non sono pubblicate dall'inizio. A tal fine è operativo, in sede preventiva, un sistema di *machine learning*, sistema di intelligenza artificiale che identifica i comportamenti contraffattori sulla base di modelli di rischio. In questo caso viene chiuso automaticamente l'*account* dell'inserzionista e ogni altro *account* connesso allo stesso dominio e sono raccolte le informazioni sugli inserzionisti identificati come contraffattori, per prevenire e impedire tentativi futuri di riapertura di un account. Oltre a tali misure proattive permangono quelle reattive, vale a dire la rimozione su segnalazione degli interessati. I titolari di marchi possono segnalare a *Google* per *AdWords* la titolarità del segno distintivo o fornire una lista dei rivenditori autorizzati.

In tema di proprietà intellettuale ed industriale, i termini e le condizioni di accesso a *Facebook* ed *Instagram* prevedono esplicitamente il divieto di pubblicazione di contenuti che non rispettano i diritti di proprietà intellettuale altrui su *copyright* e marchi commerciali e l'impegno delle piattaforme a fornire gli strumenti necessari per la protezione di questi diritti. I formulari relativi alle segnalazioni con le quali si chiedono le rimozioni, sia per i contenuti non commerciali (pagine, profili, gruppi), sia per le inserzioni pubblicitarie, richiedono di dimostrare la titolarità dei diritti sui marchi e il diritto d'autore. Sono esaminati da *team* di persone operativo « h/24 » in tutto il mondo e, in caso di ripetute violazioni, l'*account* dell'utente viene disattivato.

Una differenza importante sussiste tra i contenuti caricati dai singoli utenti, per i quali si pone un problema di tutela della libertà di espressione, e gli annunci pubblicitari, che sono rivisti sia attraverso strumenti automatici, basati sulla ricerca di parole chiave (sia in tema di prodotti contraffatti, che di c.d. *hate speech* o messaggi discriminatori), che attraverso revisione effettuata da *team* di persone dedicati allo scopo prima della pubblicazione. *Facebook* ha annunciato in Commissione che tali strumenti saranno sviluppati anche per i gruppi, compresi i gruppi segreti.

Nelle piattaforme *web* che ospitano contenuti caricati da parte degli utenti, come video, audio o testi (nel caso del gruppo *Google*, ad esempio, ci si riferisce a *YouTube, Blogger* e *Google+*), per la tutela del *copyright*, oltre alla tutela di tipo reattivo su segnalazione vi è un intervento di supporti tecnologici a carattere proattivo, in grado di individuare preventivamente situazioni di violazione del *copyright*.

L'esempio di *YouTube*, che carica più di 800 ore di video al minuto in oltre 80 Paesi nel mondo, è emblematico. In *YouTube* opera un sistema di *machine learning* denominato *Content ID*, con un investimento di oltre 60 milioni di euro, che consente, in automatico, da un lato, di riconoscere i falsi, dall'altro per i detentori di diritti

di monetizzare, anche quando viene caricato da un privato. Il sistema *Content ID*, prima dell'*upload* di un video da parte degli utenti, confronta il file con milioni di file di riferimento, pari a circa 600 anni di contenuti, forniti dai detentori dei diritti legati da un accordo di *partnership* con *Google*; riconosce una musica caricata da un privato a supporto di un video o un video e, se il detentore di diritti intende monetizzare quella canzone, i ricavi pubblicitari di quel video su *YouTube* sono corrisposti alla casa discografica; altrimenti il titolare di diritti può chiedere di bloccare il video. *Content ID* gestisce circa il 98 per cento del materiale coperto da *copyright* su *YouTube*.

Soluzioni tecnologiche di questo tipo se da un lato contrastano la pirateria digitale, dall'altro costituiscono strumenti per una gestione evolutiva del diritto d'autore, funzionale a far diminuire il *value gap* tra titolari del *copyright* e operatori ISP, in quanto gli aventi diritto possono ricevere entrate anche se il contenuto protetto non è stato concesso in licenza all'*uploader*. È stato riferito in audizione che, non a caso, il 90 per cento delle richieste dei detentori di diritti si orienta per la monetizzazione.

Il problema è tecnologicamente diverso e molto più complesso per la tutela dei marchi e le contraffazioni di merci ove un sistema del genere, che esamina direttamente le opere dell'ingegno digitalizzate, non sembra applicabile. Su *YouTube*, allo stato, possono essere segnalati video o commenti che rinviano a siti che vendono beni contraffatti; su *Blogger post* e *Google* commenti o anche solo immagini e video di tipo analogo.

Tale tipo di piattaforme, come i *social network*, in quanto destinate ad ospitare anche libere opinioni, possono comportare, nel caso di richieste di rimozione, delicati problemi giuridici, la cui risoluzione non può comunque spettare ad un operatore privato, in quanto nell'ordinamento sono risolti in sede giudiziaria: si pensi a casi di vantata diffamazione in cui la pubblicazione *on line* di determinati contenuti viene inquadrata come libertà di espressione da parte dell'*uploader* e valutata come diffamatoria da parte di chi è destinatario od oggetto del messaggio.

I problemi maggiori si pongono, con tutta evidenza, nel caso di piattaforme non di *hosting*, ma di strumenti di ricerca sul *web*.

I motori di ricerca non sono venditori di merce, ma mettono in contatto venditori e clienti, senza responsabilità in questa attività, ai sensi della direttiva sull'*e-commerce*. Dalle audizioni svolte si evince come allo stato non siano state approntate azioni di tipo proattivo rispetto all'attivazione *ex post* su segnalazione da parte degli interessati, secondo il modello non privo di limiti del *Notice and Take Down*, per motivi derivanti dalla complessità tecnologica di un'operazione di filtraggio preventivo e dalla relativa onerosità.

Nel corso dell'audizione con *Google*, ad esempio, è stato riferito che su *Google Search* ogni giorno sono effettuate più di 3,5 miliardi di ricerche in tutto il mondo, rispetto a più di 60 miliardi di indirizzi sulla rete. I titolari di *copyright* possono effettuare le segnalazioni delle violazioni, ai sensi della direttiva sull'*e-commerce* in Europa e del *Digital Millennium Copyright Act* (DMCA) negli Stati Uniti e nel mondo, cui *Google* dichiara di rispondere in un tempo medio di 6 ore, con rimozione, tra novembre 2015 e 2016, di 898 milioni di risultati

dal motore di ricerca, ma con i limiti che un approccio *Notice and Take Down* presenta, soprattutto per la necessità di una segnalazione per ciascuna violazione.

Inoltre il sito, anche se non raggiungibile tramite il motore di ricerca, rimane sul *web*, a meno che non intervenga un provvedimento dell'autorità giudiziaria di oscuramento.

La tesi sostenuta da *Google* in audizione nel caso del motore di ricerca è che il servizio offerto sia « passivo », in quanto evidenzia quello che « *già si trova sulla rete, a prescindere dall'esistenza del motore di ricerca, il quale non ha l'opportunità e il potere di controllare i siti che si limita a indicizzare. Ovviamente, qualora segnalati secondo le normative applicabili, deindicizza siti che permettono attività illecite* ».

Si tratta di un punto focale della problematica in merito.

Il tema aperto è quello di valutare la possibilità di introdurre sistemi tecnologici in grado di riconoscere siti illeciti o *account* che si siano resi responsabili di comportamenti contraffattivi.

La ricerca effettuata dai *web searcher* avviene in base ad algoritmi, che costituiscono veri e propri segreti industriali, e che nel corso degli anni si sono evoluti dal riscontro di una mera presenza lessicale nei siti delle parole cercate, ad algoritmi di ricerca su base semantica e tenendo conto di altri elementi, tra cui il *page ranking*, ossia il tasso di frequentazione degli utenti dei siti. Tali algoritmi dei motori di ricerca sono in grado di recuperare sia i siti legali che quelli illegali, a meno che a loro non sia chiesta una selezione, attraverso opportune soluzioni tecnologiche, che porti all'esclusione dei siti illeciti.

È però vero che già oggi in questi algoritmi operano dei sistemi di filtraggio, per effetto di vincoli normativi, come emerso nell'audizione con *Google*, in grado di escludere la ricercabilità di siti in determinati settori illeciti [(51)]. Questo principio è stato introdotto anche nelle proposte di modifica delle direttive in tema di diritto d'autore e per i media audiovisivi illustrate nel paragrafo 5.3, in analogia a quanto previsto per l'*hate speech* e la tutela dei minori: si può infatti ritenere che le soluzioni tecnologiche adeguate siano disponibili.

In via generale, la definizione dei siti illeciti potrebbe avvenire con il supporto di associazioni rappresentative o consorzi dei produttori, non certo a livello di singole imprese e con l'onere di segnalazioni plurime o seriali – possibili al più solo per i grandi marchi, che non a caso hanno per tempo siglato accordi e messo in campo collaborazioni attive con le principali piattaforme. Appare auspicabile che, in casi di controversie sulle illiceità del sito, che talvolta può comportare problemi interpretativi, possa essere previsto un intervento delle autorità pubbliche competenti.

A fronte di atteggiamenti proattivi adottati dalle piattaforme globali è stato affermato in audizione che la maggiore pericolosità per la contraffazione *on line* è rappresentata dai siti specializzati in vendita di prodotti contraffatti (ad esempio nel campo farmaceutico) e dai nuovi media (quali i *social network*), che hanno un elevato

(51) V. intervento in audizione il 10 novembre 2016 di Marta Staccioli, del *Litigation Counsel* per Italia e Grecia di *Google*.

traffico di utenti e dove le difese, non essendo piattaforme principalmente vocate al commercio, sono minori [52].

Permane, peraltro, un rilevante problema, oltre che politico, anche di ordine economico: a chi porre in carico l'adozione, con relativi oneri, della miglior tecnologia esistente per l'eventuale monitoraggio preventivo.

Rispetto alla tutela del *copyright*, che, come ricordato, è più avanzata rispetto ai diritti di proprietà industriale, e che vede operare sul mercato grandi aziende (le c.d *major*) nel settore multimediale, particolarmente negli Stati Uniti, in grado di esercitare una pressione e un contrasto anche economico rispetto ai danni loro derivanti dalla pirateria digitale – ciò che indubbiamente ha indotto gli ISP all'adozione di soluzioni tecnologiche di tipo proattivo – la tutela degli IPR appare più arretrata.

Questa realtà è il frutto, da un lato, della presenza molto frammentata sul mercato globale delle aziende manifatturiere, alcune delle quali di dimensioni economiche ed organizzative piuttosto limitate, dall'altro, dell'indubbia difficoltà tecnologica di riconoscimento dei falsi e delle contraffazioni. Inoltre, giova ribadire, il quadro normativo esistente (DMCA e direttiva *e-commerce*) e il principio di neutralità della rete, sono indubbiamente favorevoli agli ISP per le ragioni storiche e logiche menzionate.

Caso ancora diverso è quello dei *social network*, che partendo da un'originaria e prevalente natura di *forum* di discussione e di manifestazione del pensiero nella vita di relazione sociale, ospitano oggi diffusamente anche attività commerciali, nella specie offerte di vendite, aste *spot* di merce o reindirizzamenti dalle pagine *social* a siti esterni di vendita. La realtà mostra come spesso tramite i *social* siano venduti prodotti contraffatti, con annunci che mirano ad intercettare i consumatori puntando sul basso prezzo della merce venduta come stimolo al contatto commerciale. È frequente rinvenire falsi siti sociali, orientati alla pubblicità o alla vendita di prodotti illegali: ad esempio gli *splogs, blog* apparentemente informativi, ma in realtà aventi contenuti pubblicitari, con i contenuti informativi copiati illegalmente da siti terzi o l'utilizzazione di *account* che utilizzano il nome di un marchio di proprietà di terzi. Altra fattispecie rilevante è quella dei gruppi « chiusi », visibili solo agli iscritti: anche in questo caso, a fronte dell'originario e diffuso utilizzo per lo scambio di opinioni e informazioni, si è andato diffondendo l'utilizzo, legittimo o meno, di commercializzazione di prodotti (scambio e vendita).

All'introduzione di forme di controllo preventivo è stato spesso opposto, in sede giuridica, il limite della tutela dei diritti di manifestazione del pensiero, propria dei *social*, in contrapposizione alle esigenze di tutela dei diritti, tra i quali quelli degli IPR e DPI.

In audizione è stata rilevata da INDICAM [53] la carenza di regolamentazione per tale ambiente, in cui « *la disponibilità di spazi che rechino visibilità a offerte palesemente in violazione non è un fenomeno isolato, ma è stimato al contrario in circa il 10 per cento del*

(52) V. audizione del 5 ottobre 2016 con Andrea Rota, *Senior Director Global Brand Protection* e Stefan Krawczyk, *Associate General Counsel and Head Government relations International* di *eBay Inc*.

(53) V. audizione del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam.

totale della contraffazione veicolata digitalmente ». Di qui la richiesta della definizione di un dovere di diligenza ulteriore rispetto a quanto previsto dalla direttiva sull'*e-commerce*.

7.2. La consapevolezza della necessità della lotta alla contraffazione presso gli *Internet Provider*.

Prima di esaminare in dettaglio le tecniche di contrasto, occorre soffermarsi sul fatto che, nelle dichiarazioni degli operatori dell'economia digitale auditi in Commissione, è emersa la consapevolezza dell'esistenza di un rilevante problema per l'affidabilità del commercio *on line* costituito dall'ingente traffico di merce contraffatta o dalla pirateria digitale.

A prescindere da una uguale forma limitata di responsabilità descritta nei paragrafi precedenti, le prassi applicative e gli accordi intercorsi tra ISP e aziende, finalizzati a prevenire o regolare i potenziali contenziosi legali con le aziende titolari di marchi o con i titolari di diritti d'autore che lamentino la lesione dei propri diritti da inserzioni di vendita poste illegalmente, rivelano un'evoluzione nelle tecniche di contrasto, con azioni finalizzate a controllare la regolarità delle vendite nel commercio elettronico. La maggiore o minore tutela accordata ai titolari di IPR e DPI consegue sia dalla tipologia dei diritti che si ritengono lesi, sia dalle forme di commercio elettronico e dal contesto informatico in cui ci si trova ad operare.

A tal fine la Commissione ha preso atto di una serie di iniziative assunte in tale direzione.

La piattaforma *eBay Inc*. vende più di un miliardo di oggetti a livello globale, con decine di milioni di nuovi oggetti in vendita ogni giorno, che non sono conosciuti fisicamente dall'ISP, ma solo attraverso le relative inserzioni pubblicate; in Italia accedono alla piattaforma più di 30.000 venditori professionali, con più di cento imprese che su *eBay* hanno conseguito un fatturato superiore al milione di euro, e circa 5 milioni di acquirenti. Nell'audizione dei rappresentanti di *eBay* è stato manifestato l'interesse della piattaforma ad operare per eliminare completamente la contraffazione, per almeno due ordini di motivi: per un motivo commerciale, in quanto il danno procurato agli utenti si traduce in una perdita di clientela per l'operatore ISP, e per un motivo economico, in quanto il sistema di garanzia per gli utenti di *eBay* fa si che in caso di insoddisfazione dichiarata dagli utenti la piattaforma subentri e rimborsi il costo dell'acquisto [(54)].

A tal fine è stato riferito che le regole definite dalla piattaforma impongono ai venditori la responsabilità di assicurarsi che gli oggetti messi in vendita siano genuini; in mancanza dell'assunzione di tale responsabilità le merci non sono ammesse alla vendita. Tre sono i livelli di controllo e di sicurezza: un livello proattivo, con un mix di tecnologie che identificano oggetti a rischio, sistemi di intelligenza artificiale che considerano i *pattern* di abitudini e di comportamento dei venditori correlati ad oggetti contraffatti, integrati da un esame

(54) V. audizione del 5 ottobre 2016 con Andrea Rota, *Senior Director Global Brand Protection* e Stefan Krawczyk, *Associate General Counsel and Head Government relations International* di *eBay Inc*.

condotto da *team* di persone; l'adozione del programma informatico di controllo *Verify right owners (VeRO)* in *partnership* con i detentori dei marchi (*right owners*) che presentano avvisi di *Notice and Take Down* in formato elettronico per eliminare merci contraffatte; l'utilizzo delle segnalazioni degli utenti *eBay* ha costituito un *Global asset protection team per* collaborare con le forze dell'ordine a livello globale. In audizione è stato riferito il dato che l'attività proattiva determina il blocco di più del 60 per cento degli oggetti contraffatti, mentre il restante 40 per cento dei casi avviene a seguito di segnalazioni dei *brand* o degli utenti.

Anche altre grandi piattaforme globali, ad esempio *Amazon* ed *Allegro*, stanno adottando sistemi proattivi analoghi. I rappresentanti di *Amazon* hanno riferito in audizione [(55)] che nel quadro della propria *policy* anticontraffazione, che i venditori sul proprio *marketplace* sono obbligati ad accettare prima di potersi registrare, particolare attenzione è data all'osservazione degli indicatori di prestazione (*key performance indicator*) per i venditori, come definiti nel *Memorandum of Understanding* siglato con la Commissione UE, consistenti nell'esame della percentuale di prodotti contraffatti posti in vendita, sull'accesso degli utenti a tali prodotti e nella percentuale di sospensioni e rimozioni di prodotti dalla piattaforma; è inoltre disponibile un programma anticontraffazione di « *product quality* », che prevede l'utilizzo di un sistema di « *predictive analysis* » attraverso tecnologia di *machine learning*, che analizza i dati e le segnalazioni pervenute, ad esempio individuando possibili connessioni tra nuovi *account* e *account* in precedenza coinvolti in casi legati alla contraffazione, con riferimento anche alla localizzazione, e particolare attenzione a categorie di prodotti sensibili per la salute del consumatore, come quelli dell'agroalimentare, al fine di cercare di prevenire l'inserimento di merci contraffatte.

Il controllo proattivo a carattere preventivo è più semplice quando i trader *on line* siano proprietari (piattaforme di *retail*) o abbiano in proprio rapporti di fornitura della merce che pongono in vendita nelle piattaforme digitali (*marketplace*), in quanto in questo caso il riscontro della tutela degli IPR può essere condotto non su annunci di vendita, ma direttamente sulla merce.

Nell'audizione con i rappresentanti della piattaforma cinese di *e-commerce Alibaba*, tra le principali al mondo, con una platea di 400 milioni di utenti stimata in Cina, la Commissione ha preso atto di affermazioni molto decise circa l'impegno di tale *holding* di assumere un ruolo di *leader* nella lotta alla contraffazione, attraverso l'uso di tecnologie innovative, la collaborazione con i detentori dei diritti, con i Governi e le autorità di polizia. È stato affermato espressamente che *« per Alibaba i prodotti contraffatti sono inaccettabili. Riteniamo che i marchi e la loro proprietà intellettuale debbano essere protetti. Alibaba è interessato a sostenere i produttori che innovano e investono nei loro stessi marchi. Non tolleriamo né condoniamo coloro che rubano la proprietà intellettuale di altri. Violare la proprietà intellettuale è un furto ed è dannoso per l'innovazione e l'integrità del nostro mercato.*

(55) V. audizione di Franco Spicciariello, *Senior Manager Public Policy* Italia, Federico Finzi, *Legal Director IT* e Zuzana Pucikova, *Senior Manager Public Policy* EU di *Amazon* del 18 gennaio 2017.

Non osserviamo soltanto leggi e regolamenti, ma assistiamo concretamente le autorità di polizia per la lotta ai contraffattori. Alibaba sta compiendo sforzi indipendenti per essere trasparente, creativa e proattiva. È riconosciuto che una lotta efficace alla contraffazione richieda uno sforzo congiunto dei detentori di diritti che vengono colpiti dalla contraffazione e dei partecipanti alle attività di e-commerce, come Alibaba » [(56)]. A tal fine, in Italia, il 24 agosto 2016, è stato siglato tra il Ministero delle politiche agricole - Ispettorato centrale della tutela della qualità e repressione frodi dei prodotti agroalimentari, e *Alibaba* un *memorandum* d'intesa per educare i consumatori e proteggere i diritti di proprietà industriale (denominazioni di origine protette ed indicazioni geografiche), in relazione ai più tipici prodotti italiani, come per esempio l'olio extravergine d'oliva toscano.

Lo stesso audito ha sottolineato che il problema dell'efficacia delle iniziative a contrasto della contraffazione è rappresentato in parte dalle stesse dimensioni del commercio *on line*, dal momento che a fronte di 1,5 miliardi di inserzioni, con più di 100.000 marchi che operano sulle piattaforme e oltre 7 milioni di operatori, è inevitabile che vi sia una parte di inserzioni contraffatte. È stato riferito in Commissione che il sistema anti-contraffazione adoperato da *Alibaba* ha la capacità di elaborare 100 milioni di dati al secondo, e consente di condurre delle scansioni proattive su circa 7 milioni di nuove inserzioni al giorno, esaminando le caratteristiche dei prodotti, quali marchio, prezzo, geolocalizzazione, identità del compratore e del venditore, *feedback* dei consumatori e altri elementi. Tale sistema, nel periodo agosto 2015-2016, ha portato all'eliminazione proattiva di più di 380 milioni di inserzioni. Sono stati altresì illustrati in Commissione il programma di Notice and Take Down adottato (sistemi *AliProtect* e *TaoProtect*), che consente ai detentori di diritti di proprietà di registrarsi sulle piattaforme di *Alibaba*, a prescindere dalla sussistenza di un « negozio digitale » sulle piattaforme e il programma di rimozione « in buona fede » *(Good Faith Programme*), riservato agli esercenti che hanno una « buona reputazione commerciale », che prevede una procedura semplificata di rimozione, che viene elaborata in tempi rapidi senza chiedere prove. Va rilevato, peraltro, che proprio su questa procedura in altra audizione [(57)] sono state avanzate perplessità in quanto riservato solo ad aziende che vantino un *rate* di successo nelle richieste di rimozione di almeno il 90 per cento, e come tale contestato dai titolari di marchi.

In tema di lotta alla pirateria digitale *on line* nell'audizione di *Google* [(58)] è emerso, infine, che accanto all'azione di contrasto alla pirateria digitale vi è una linea di tendenza aziendale, in una chiave evolutiva del diritto d'autore, volta ad accrescere sempre più i contenuti legali disponibili per gli utenti e aumentare la remunerazione per i detentori dei diritti d'autore. Uno studio del luglio 2016 *dell'Intellectual property office* del Regno Unito ha riscontrato come la

(56) V. audizione di Eric C. Pellettier, Vice Presidente e capo degli affari istituzionali internazionali e di Rodrigo Cipriani Foresio, Direttore esecutivo per Italia, Spagna, Portogallo e Grecia di *Alibaba Group* del 13 ottobre 2016.

(57) V. documentazione allegata al resoconto stenografico dell'audizione di del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam.

(58) Audizione del 10 novembre 2016 del responsabile delle relazioni istituzionali di *Google* Enrico Bellini, e di rappresentante dell'ufficio legale di *Google* Marta Staccioli.

percentuale di utenti che accedono illegalmente a film, musica e altri contenuti coperti da *copyright* è scesa al punto minimo mai registrato, in corrispondenza con il massimo utilizzo di piattaforme legali come *YouTube*, *Spotify* e *Netflix*. Pare questa una tendenza estremamente interessante per efficacia in quanto, promuovendo la diffusione legale di contenuti, in particolare audio-video, senza oneri diretti per gli utenti, accompagna un'evoluzione generale del mercato e favorisce l'incontro positivo tra domanda e offerta. Risolvendo peraltro a monte (pur con le menzionate criticità e opportunità di *value gap*) il contrasto della circolazione di contenuti illegali: in questo caso la pubblicità paga legalmente contenuti legittimamente diffusi, anziché sostenere illegalmente contenuti contraffatti.

Le ragioni dell'adesione delle piattaforme ISP alle iniziative anticontraffazione non sono solo di ordine etico, ma discendono anche da motivazioni reputazionali e quindi commerciali, per la necessità di tutelare le aziende e gli utenti nel loro utilizzo delle piattaforme e mantenere la fidelizzazione dei clienti [(59)]. Nell'audizione con *Amazon*, ad esempio, la *policy* di attenzione nei confronti del consumatore è stata definita significativamente come « *customerobsession* » [(60)].

8. LE MODALITÀ DI CONTRASTO ALLA CONTRAFFAZIONE NEL COMMERCIO ELETTRONICO

8.1. Dal *Notice and Take Down* al *Notice and Stay Down*.

Una delle prospettive al centro del dibattito internazionale in materia che la Commissione ha esaminato, è il passaggio da un mero atteggiamento di *Notice and Take Down*, ove gli ISP si attivano solo su segnalazione degli interessati, ad un approccio più coinvolgente degli ISP, definito *Notice and Stay Down*.

Il *Notice and Take Down* è una tutela successiva alla constatazione, da parte degli interessati (in genere i detentori dei diritti, ma anche i consumatori), della presenza in rete di merci contraffatte o di pirateria digitale, che in questo caso inviano una segnalazione all'ISP per farle eliminare. I limiti sono evidenti.

Tale procedura implica la necessità di inviare una segnalazione per ogni singola violazione rilevata, ed è quindi estremamente onerosa in quanto comporta il dispiego di un'ampia attività di monitoraggio e di contenzioso con gli ISP, causando elevati costi gestionali aziendali.

Il volume complessivo delle transazioni commerciali su supporto digitale, e la necessità di effettuare migliaia e migliaia di segnalazioni, implicano, di fatto, un'oggettiva impossibilità di combattere il fenomeno e una assoluta mancanza di tutela, particolarmente per le piccole e medie imprese, per i titolari dei beni tutelati dagli IPR o dai DPI.

---

(59) V. audizione del 27 ottobre 2016 con il responsabile dei rapporti istituzionali per Italia, Grecia e Malta di *Facebook,* Laura Bononcini.

(60) V. audizione di Franco Spicciariello, *Senior Manager Public Policy* Italia, Federico Finzi, *Legal Director* IT e Zuzana Pucikova, *Senior Manager Public Policy* EU di *Amazon* il 18 gennaio 2017.

La procedura di *Notice and Stay Down*, invece, fa seguire alla singola segnalazione da parte dei titolari di diritti IPR e DPI, che si reputano lesi da contenuti pubblicati o da merci commercializzate sul *web*, la rimozione dei contenuti da parte dell'ISP di tutte le fattispecie di quell'illecito, prevenendo ed impedendo la reiterazione dello stesso.

Nel *Notice and Stay Down* gli ISP sono tenuti, in presenza di una segnalazione su un determinato marchio contraffatto o opera dell'ingegno oggetto di pirateria, a realizzare sostanziali azioni positive, attraverso adeguati sistemi tecnologici, per eliminare situazioni di contraffazioni seriali, quali:

a) rimuovere tutte le copie dell'opera dell'ingegno scaricabile o gli accessi alla vendita *on line* di merci contraffatte, da tutte le URL alle quali le offerte di *download* o di vendita sono attingibili, anche se non indicate nella segnalazione dell'illecito da parte dei titolari di IPR o DPI;

b) impedire che ulteriori copie della stessa opera/prodotto siano caricate in futuro, utilizzando sistemi tecnologici di filtraggio e blocco, anche verso gli IP usati per violare diritti di IPR e DPI[(61)];

c) installare sistemi di monitoraggio per ricercare attività illecite, utilizzando le informazioni relative a quelle contenute nelle segnalazioni.

Il *provider* è quindi tenuto, in forza di un *duty of care*, che consegue proprio al fatto di essere stato informato dell'esistenza di un'attività illecita, in forza di una segnalazione, ad adoperarsi per impedire al medesimo contraffattore di continuare ad esplicare in qualsiasi forma il proprio commercio illegale, o ad altri di fare altrettanto per lo stesso contenuto.

È possibile immaginare che, se la segnalazione fosse effettuata non in maniera episodica, ossia per singoli illeciti dai singoli soggetti, ma in modo sistemico da parte di associazioni rappresentative o consorzi dei titolari di diritti, che agiscano a tutela di determinati settori merceologici e consentano l'individuazione dei casi più diffusi di falsi e contraffazioni subite dai propri aderenti, si potrebbe avere un'amplificazione della forma di tutela offerta e, per gli ISP, una base concreta e delimitata su cui applicare le soluzioni tecnologiche di ricerca automatica e preventiva degli illeciti.

Nel *Notice and Stay Down*, la segnalazione assume quindi un valore molto maggiore, non essendo limitato al singolo caso, ma costituendo un importante elemento conoscitivo di situazioni illecite, che pertanto non possono più essere ignorate dal *provider*; da tale conoscenza effettiva deriva una responsabilità oggettiva per gli ISP.

Di tali comportamenti proattivi è stata illustrata l'applicazione in Commissione, ad esempio nel campo dei *social network,* nel corso dell'audizione con il gruppo *Facebook*, titolare anche del marchio

(61) Nel corso dell'audizione di Luca Vespignani, Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale (FPM) è stato stimato che l'adozione del criterio del *Notice and Stay Down* in luogo del *Notice and take down,* il 90 per cento delle richieste di rimozione che oggi vengono mandate non verrebbero più inviate, perché la stragrande parte delle segnalazioni riguarda la stessa opera sullo stesso sito, con circa 2 milioni e mezzo di notifiche in meno inviate ogni anno.

Instagram. In tema di proprietà intellettuale ed industriale, i termini e le condizioni di accesso a *Facebook* ed *Instagram* prevedono esplicitamente il divieto di pubblicazione di contenuti che non rispettino i diritti di proprietà intellettuale altrui su *copyright* e marchi commerciali e l'impegno delle piattaforme a fornire gli strumenti necessari per la protezione di questi diritti. Come già ricordato, i formulari relativi alle segnalazioni con le quali si chiedono le rimozioni, sia per i contenuti non commerciali (pagine, profili, gruppi), sia per le inserzioni pubblicitarie, richiedono espressamente di dimostrare la titolarità dei diritti sui marchi e il diritto d'autore e sono esaminati da *team* di persone operativi « h/24 » in tutto il mondo. In caso di ripetute violazioni l'*account* dell'utente viene disattivato. [(62)] Altre misure di tipo preventivo, attraverso strumenti automatici, consentono di evitare la creazione di nuovi profili da parte delle stesse persone il cui *account* sia stato disattivato. Altro strumento utilizzato, sempre da *Facebook,* è costituito dall'associazione ai contenuti audiovideo inseriti dai titolari dei diritti di un'impronta digitale (c.d. *Fingerprint*) che consente, in caso di successivi caricamenti dello stesso contenuto da parte di utenti non legittimati, l'immediata conoscibilità di ciò da parte del titolare di diritti, che può chiederne la rimozione.

Il tema, con un approccio pragmatico, è dunque quello di valutare il contributo che le tecnologie per la protezione dei beni tutelati da marchi o da diritti d'autore possono fornire per combattere i fenomeni del falso e della contraffazione, con l'adozione di procedure rapide che diano seguito alle segnalazioni di illeciti.

Per l'adozione di procedure di *Notice and Stay Down* deve essere poi considerata con attenzione la sproporzione che si può determinare tra i danni ingenti che il *trading on line* di beni contraffatti causa alle aziende manufatturiere rispetto ai notevoli profitti, legittimamente conseguiti, che conseguono i *provider* nelle attività di *trading* elettronico, anche rispetto agli oneri economici da assumere per la realizzazione degli interventi di tipo proattivo.

8.2. L'oscuramento dei siti illegali.

Oltre alla rimozione dei contenuti derivante dal rapporto privatistico tra operatore ISP e titolari dei diritti lesi da attività contraffattorie, la modalità più utilizzata con l'intervento dei poteri pubblici è costituita dall'oscuramento dei siti illegali: si tratta di un blocco informatico dell'accesso in Italia alle pagine illecite, con informazione del consumatore circa l'illiceità delle transazioni e dei siti [(63)].

Tale misura può essere disposta sia in sede giurisdizionale, attraverso misure di sequestro disposto dall'autorità giudiziaria, che si attiva d'ufficio, sia in sede amministrativa, dall'Autorità *Antitrust*

(62) V. audizione del 27 ottobre 2016 con il responsabile dei rapporti istituzionali per Italia, Grecia e Malta di *Facebook*, Laura Bononcini.

(63) Nell'audizione del 25 maggio 2016 con il Presidente dell'Associazione italiana *Internet Provider* (AIIP), Renato Brunetti, è stato ricordato che tale possibilità consegue solo a provvedimenti disposti dall'autorità giudiziaria e non anche da parte dell'autorità amministrativa, in quanto il reindirizzamento ad un altro sito che contenga l'avviso dell'illiceità si configurerebbe come atto di indagine giudiziaria, perché quel sito è in grado di raccogliere tutti gli indirizzi degli utenti che hanno cercato di raggiungerlo.

(AGCM) per i beni oggetto di diritti di proprietà industriale e dall'Autorità per le comunicazioni (AGCOM), per il *copyright*, attivate non d'ufficio, ma su richiesta degli interessati.

È una misura che ha mostrato nell'applicazione limiti evidenti: il blocco, pur utile, è però superabile dai titolari dei siti illeciti deviando il traffico su altri indirizzi *internet* o mediante la creazione di nuovi siti nella rete. I siti illegali su *internet* operano peraltro secondo alcune caratteristiche ricorrenti: l'opacità dei meccanismi di attribuzione della titolarità delle risorse *internet* utilizzate; la parcellizzazione dei carichi di merce; il ricorso a sistemi di pagamento legali ed efficienti; l'adozione di tecniche di vendita idonee a trarre in inganno il consumatore.

Va poi ricordato che molti ordinamenti esteri non contemplano nella propria normativa ipotesi considerate criminose in Italia ed in Europa e non contemplano, ad esempio, la misura della confisca per equivalente. In caso di indagini da condurre su base sovranazionale l'assenza di una convenzione internazionale in materia, che preveda l'omogeneità delle sanzioni e forme di coordinamento delle forze di polizia e delle magistrature nazionali (sul versante, in particolare, delle misure cautelari e personali, dei sequestri preventivi dei siti e delle merci, delle sanzioni economiche definitive, come le confische) costituisce un serio problema, in un campo come quello della contraffazione sul *web*, per sua natura sovranazionale. Va ricordato al proposito che in sede di audizione presso la Commissione, il 17 giugno 2015, il procuratore aggiunto di Roma, Nello Rossi, ha auspicato che: « *si prenda atto che il web è diventato un nuovo ambiente in cui si moltiplicano i fenomeni criminosi, come è naturale, e si possa immaginare che i vari Stati si mettano d'accordo almeno su alcune linee guida, su alcune regole di cooperazione, su alcune ipotesi che vogliono contrastare in un certo modo. Come ho detto, la dimensione sovranazionale è fondamentale sul piano, appunto, dell'omogeneizzazione delle norme incriminatrici* »[(64)].

In sede giurisdizionale si ricorda che la Procura di Milano ha adottato, in materia di siti *web* dediti a forme di contraffazione, una prassi di contrasto[(65)] basata su decreti di sequestro ed oscuramento dei siti « in bianco », confermati in sede di riesame, che già contiene l'estensione ad altri siti aperti successivamente a seguito delle operazioni di reindirizzamento, senza necessità di ulteriori provvedimenti giudiziari, che potrebbe costituire una parziale soluzione a questo problema. I provvedimenti di sequestro riguardano in tal modo non solo il sito segnalato dall'avente diritto leso nei propri diritti di proprietà industriale, ma sono automaticamente estesi anche a qualsiasi altro sito che abbia denominazione simile, suono simile, e sia comunque riferibile a quello originario[(66)].

---

(64) Va altresì ricordato come il sostituto procuratore di Milano Tiziana Siciliano, nell'audizione in Commissione del 9 aprile 2015, abbia affermato che « *quello di internet è un problema « pazzesco », ben più grave e ben più serio della contraffazione di strada, perché è pressoché impossibile intervenire sulla fonte dell'offerta (provider all'estero, chiusura pressoché totale di chi detiene il potere di diffusione della comunicazione web).* »

(65) V. audizione del 9 aprile 2015 del Sostituto Procuratore della Repubblica del Tribunale di Milano, Tiziana Siciliano.

(66) Nell'audizione del 28 settembre 2016, il Comandante Generale della Guardia di Finanza, Toschi, ha richiamato l'operazione « Red Devils » del 2016 che ha permesso di ricostruire un vasto

In sede di audizione [67] è stata sostenuta la necessità, per quanto riguarda la disattivazione dei siti, di impedirne la riattivazione rafforzando la tutela attraverso il blocco congiunto dell'indirizzo IP con il DNS (*Domain Name System*) [68]. Il DNS è una funzione di *Internet* che trasforma un nome dell'URL in un indirizzo IP, attraverso la quale la rete arriva al *server* cercato.

In sede amministrativa devono essere ricordate le iniziative, in tema di diritto d'autore assunte da parte dell'Autorità di garanzia per le comunicazioni, e, in tema di diritti di proprietà industriale, da parte dell'Autorità Garante per la concorrenza e il mercato.

Sotto il primo profilo molto importante è il Regolamento dell'Autorità di garanzia per le comunicazioni (AGCOM) (del. 680/13/CONS) del 12 dicembre 2013, relativo alla tutela del diritto d'autore sulle reti di comunicazione elettronica, il cui articolo 2, comma 3 riguarda le violazioni via *web* di opere protette dalla legge sul diritto d'autore. La norma non concerne gli utenti finali che effettuano *download* o fruiscono in *streaming* di opere digitali, né le modalità di condivisione di tali opere in rete tra tali utenti (attraverso *file sharing* o *peer to peer).* Il titolare di un'opera digitale resa disponibile su una pagina *internet* in violazione della legge sul diritto d'autore presenta istanza all'AGCOM, qualora non sia pendente un procedimento presso l'autorità giudiziaria. Il procedimento (articolo 7) si svolge nei confronti del *provider* e, ove rintracciabili, verso l'*uploader*, i gestori della pagina o del sito. L'AGCOM può esigere, secondo criteri di gradualità, proporzionalità ed adeguatezza, che il *provider* impedisca la violazione o che vi ponga fine: se il sito che contiene la violazione è ospitato su *server* ubicato in Italia, l'AGCOM ordina la rimozione selettiva delle opere digitali o, in caso di violazioni massive, la disabilitazione dell'accesso a tali opere illecite (articolo 8, comma 3); se il sito è ospitato su *server* fuori Italia, l'AGCOM ordina al *provider* di semplice trasporto *(mere conduit)* la disabilitazione dell'accesso al sito (articolo 8, comma 4); in entrambi i casi l'AGCOM ordina al *provider*, ai sensi dell'articolo 71, comma 2-quater, lett. *a*) del Codice delle comunicazioni elettroniche, di reindirizzare automaticamente verso una pagina *internet* redatta secondo le modalità indicate dall'Autorità le richieste di accesso alla pagina ove è stata accertata la presenza dell'opera digitale illegittima. I *provider* devono ottemperare entro 3 giorni dalla notifica. In caso di inottemperanza (articolo 8, comma 7) l'AGCOM applica le sanzioni di cui all'articolo 1, comma 31, della legge 31 luglio 1997, n. 249 (sanzione amministrativa pecuniaria da lire 20 milioni a lire 500 milioni ovvero, nel caso di abuso di posizioni dominanti, la sanzione amministrativa pecuniaria non inferiore al 2 per cento e non superiore al 5 per cento del fatturato

traffico di merce illegale sviluppato attraverso un sito *internet* in apparenza assimilabile, per aspetto, prezzi di vendita, mezzi di pagamento e di spedizione proposti, a quelli degli *outlet* ufficiali di marchi di alta moda, poi oscurato su ben 90 *provider* di tutto il mondo, registrato in Olanda a nome di persona fisica residente in Francia, con l'indirizzo IP localizzato in Inghilterra e il beneficiario dei pagamenti con carta di credito residente in Cina.

Proposta avanzata il 3 marzo 2016 sia dalla FAPAV, nell'audizione del Segretario generale Federico Bagnoli Rossi, sia dal Presidente della Federazione Industria Musicale Italiana (FIMI), Enzo Mazza.

(67) Fonte: E-commerce Europe.

(68) V. audizione del 18 maggio 2016 di Luca Vespignani, Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale (FPM).

realizzato nell'ultimo esercizio), dandone comunicazione agli organi di polizia giudiziaria, ai sensi dell'articolo 182-*ter* della LDA, che richiama gli articoli 347 e seguenti c.p.p. circa le attività ad iniziativa della PG per la raccolta di elementi essenziali di reato. Avverso le decisioni dell'AGCOM è ammesso ricorso dinanzi al TAR (articolo 17) [(69)].

Il valore del Regolamento e l'efficacia dell'azione dell'Autorità, anche rispetto agli altri paesi europei, sono stati segnalati da molti dei soggetti adulti dalla Commissione.

Si deve anche all'adozione di tale provvedimento l'uscita dell'Italia dalla « *Watch List* » (Paesi sotto osservazione), stilata dall'Ufficio del Commercio USA (*Office of the United States Trade Representative*) dei Paesi non considerati convenienti per gli investimenti americani, a causa dello scarso contrasto della pirateria.

Sotto il secondo profilo, l'Autorità Garante per la concorrenza e il mercato (AGCM) è intervenuta per contrastare la contraffazione che riguarda IPR sotto il profilo della tutela del consumatore contro le pratiche concorrenziali scorrette, in particolare contro le pratiche ingannevoli per il consumatore inconsapevole, vietate dal decreto-legge 6 settembre 2005, n. 206 *Codice del consumo* (articoli da 21 a 23). Le pratiche ingannevoli consistono nel fornire informazioni non corrispondenti al vero, o incomplete, al consumatore riguardo la natura del prodotto, le sue caratteristiche principali, il prezzo, il professionista che lo commercializza ecc., inducendolo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso. L'AGCM, confortata dalla giurisprudenza del TAR del Lazio e del Consiglio di Stato, ha dato un'interpretazione ampia delle modalità con cui vengono veicolate ai consumatori informazioni ingannevoli, estendendole anche alle pratiche commerciali scorrette realizzate via *web*. In virtù di tale interpretazione, è stata fatta rientrare nella definizione di pratica commerciale ingannevole anche la presentazione e l'offerta, in particolare sul *web*, di prodotti contraffatti che esibiscono marchi conosciuti (tipicamente articoli di abbigliamento, accessori, pelletteria, ecc.) [(70)]. L'intervento si basa, dal punto di vista normativo, sugli artt. 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, di attuazione della direttiva 2003/31, che consente la sospensione provvisoria di pratiche commerciali illegali. Ai *provider* è intimato di cessare la diffusione delle informazioni ingannevoli, con un'inibitoria volta ad ottenere la sospensione dell'accessibilità dei siti limitatamente agli utenti della rete che si connettono dal territorio italiano.

Da parte delle aziende digitali, è stato rilevato, in audizione, che, mentre il blocco del DNS, che si sostanzia nella mancata prestazione del servizio di traduzione informatica del contatto, non contrasta con la libertà delle comunicazioni, viceversa il blocco sull'IP, che implica impedire la comunicazione, potrebbe costituire una limita-

(69) Sul Regolamento v. audizione con la SIAE del 4 maggio 2016.

(70) Nell'audizione in Commissione del 27 novembre 2014 è stato ricordato che *« l'esperienza maturata dall'Autorità in questo campo ha evidenziato che spesso al consumatore viene fatto credere, in modo non corrispondente al vero, che i prodotti commercializzati siano originali, facendo uso di siti che apparentemente, per la loro presentazione grafica, sembrano riconducibili al produttore stesso »*.

zione della libertà delle comunicazioni ai sensi dell'articolo 15 della Costituzione [71].

8.3. L'approccio *Follow The Money*.

Per i siti dediti ad attività illecite nel settore della contraffazione e della pirateria digitale, importante è l'approccio cosiddetto « *Follow The Money* ». Con tale denominazione si intende il contrasto ai prodotti della contraffazione o della pirateria digitale basato non solo sulla lotta in senso tecnico a tali fenomeni (identificazione di tali merci, oscuramento dei siti e sequestri da parte delle forze di polizia e delle autorità giudiziarie, ecc.), ma incentrato su attività finalizzate ad impedire la remunerazione economica di tale attività illecita, d'intesa con gli operatori finanziari di supporto alle attività di *trading on line*.

La *best practice* in materia è americana. Negli Stati Uniti, sin dal 2013, è stato concluso l'accordo *Payment Processor Initiative–Rogue Block Program* tra l'IACC (*International AntiCounterfeiting Coalition)*, associazione *non profit* che tutela i diritti di proprietà intellettuale ed industriale, e le aziende del mercato del credito, con la partecipazione dello *US IPR Enforcement Office*, facente capo direttamente alla Presidenza degli Stati Uniti [72].

L'accordo, di natura privatistica, prevede l'impossibilità, per i violatori dei diritti di IPR *(infingers),* di avvalersi dei circuiti di pagamento per l'acquisto di beni contraffatti, sulla base di uno scambio di informazioni tra titolari di diritti e piattaforme di pagamento. Queste ultime, ricevute le richieste di *delisting*, effettuano il blocco con le banche gestori dei conti correnti dei venditori di merce contraffatta, che ricevono il trasferimento di denaro dall'acquirente. L'accordo si basa su disciplinari di impiego delle carte di credito che gli utilizzatori delle stesse si impegnano a rispettare [73].

La strategia di contrasto basata sul *Follow the Money* è diversa nel caso di pirateria digitale in violazione del diritto d'autore e nel caso di violazioni dei diritti di proprietà industriale.

Nel primo caso, il principale obiettivo di contrasto è costituito dalla necessità di bloccare il finanziamento costituito dalla pubblicità; la strategia *Follow The Money* vera e propria riguarda il sistema dei pagamenti di merci contraffatte nel caso di violazione di IPR, poiché la fonte di approvvigionamento finanziaria per i venditori contraffattori sono le vendite stesse.

Per il *file sharing* o l'*upload-download* illegale di audiovisivi, ad esempio, è noto che il profitto per gli operatori non deriva tanto dall'operazione di scarico di film o musica, che spesso è gratuito, ma

(71) V. intervento in audizione del vicepresidente dell'Associazione italiana *Internet Provider* (AIIP), Paolo Nuti, del 25 maggio 2016. Va ricordato, peraltro, come nel caso della pedopornografia, dal 2006, viene disposto il blocco sia del DNS che dell'IP, mentre nel caso dei siti di gioco illegali richiesta dall'azienda dei Monopoli di Stato in forza di previsione della legge finanziaria 2006, il blocco riguarda solo il DNS.

(72) V. audizione del Presidente dello IACC, Robert Barchiesi, del 16 marzo 2017.

(73) Nell'audizione del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam, è stato riferito che l'accordo ha portato a oltre 14000 segnalazioni, con un blocco dei finanziamenti di oltre 7000 casi.

dalla pubblicità ospitata dai siti, in rapporto al numero di contatti e il *page rank* degli stessi. Intervenire, previ accordi tra ISP, titolari degli DPI e agenzie pubblicitarie, per concordare il divieto di inserzioni pubblicitarie (ad es. *banner* pubblicitari) su siti illeciti, favorendo la consapevolezza della pericolosità dell'inserimento di campagne pubblicitarie al buio su tutti i siti, basandosi solo sul criterio del *page rank*, può costituire una misura efficace per togliere la principale fonte di profitto per gli operatori illegali [(74)].

Anche nel settore della tutela degli IPR, l'esperienza americana, e parzialmente europea, mostra come una strategia perseguita per il *Follow the Money* sia costituita da intese definite tra titolari di marchi e segni distintivi, ISP e titolari di siti e società di gestione dei mezzi di pagamento elettronici (carte di credito, *internet banking*, ecc.), per bloccare, in presenza transazioni relative a merce contraffatta sul *web*, la possibilità di effettuare pagamenti *on line* per l'acquisto di tale merce, rendendo non attivabili i circuiti finanziari digitali riguardo ai siti interessati.

Già dal luglio 2014, d'altronde, la Commissione europea ha elaborato un piano d'azione per elevare la tutela dei diritti di proprietà industriale e del *copyright,* seguendo l'approccio *Follow The Money* [(75)]. Il piano d'azione comunitario definisce una serie di azioni volte a far sì che la politica dell'UE in materia di rispetto dei diritti di proprietà intellettuale (DPI) si concentri sulle violazioni su scala commerciale in materia di DPI nei paesi terzi e per arrestare il commercio di prodotti che violano i DPI:

- avviare un dialogo con le parti interessate (agenzie di pubblicità *on line* e prestatori di servizi di pagamento) inteso a ridurre gli utili provenienti dalle violazioni su scala commerciale via *internet*;

- promuovere la dovuta diligenza tra tutti gli attori coinvolti nella produzione di merci, svolgendo un *audit* responsabile delle catene di approvvigionamento, applicando la dovuta diligenza;

- aiutare le piccole imprese a far valere i loro diritti in modo più efficace migliorando le procedure giudiziarie e incentivare la cooperazione tra Stati membri, facilitando gli scambi di *best practices*;

- collaborare con i paesi *partner*, attraverso dialoghi e gruppi di lavoro, per individuare le principali debolezze dei loro sistemi di protezione dei DPI e IPR, con sondaggi periodici per individuare i « paesi prioritari » dove è opportuno concentrare gli sforzi dell'UE.

L'approccio ha incontrato il favore di molti operatori ISP: va ricordato come *Google* abbia dichiarato in Commissione l'adesione all'approccio di contrasto del tipo *Follow the Money*, segnatamente per quanto riguarda gli introiti pubblicitari, con l'annullamento di oltre 670.000 *ads* per violazione del *copyright* nel 2015, l'esclusione di 91.000 siti e dal programma *AdSense* e la chiusura di 11.000 *account*.

(74) La Guardia di Finanza ha riferito nelle audizioni in Commissione delle numerose operazioni svolte in questa direzione: operazione *Publifilm*, operazione *Match Off* e operazione *Cellular phone*, per il controllo delle inserzioni pubblicitarie sui siti.

(75) Comunicazione della Commissione COM(2014) 392 final, del 1º luglio 2014: *« Verso un rinnovato consenso sul rispetto dei diritti di proprietà intellettuale: piano d'azione dell'Unione europea »*.

8.4. Gli accordi tra i *provider* e le aziende.

Come richiamato più volte, importante nella realtà del mercato elettronico è la realizzazione di accordi tra gli *stakeholders* del commercio elettronico e le aziende produttrici per bloccare la vendita di merci contraffatte, coinvolgendo anche i fornitori di « *side services* »: dunque siti e piattaforme di *e-commerce*, *social network*, *web searcher* da un lato, titolari dei marchi dall'altro, ma anche trasportatori fisici dei prodotti (c.d. *shipping)*, il sistema pubblicitario *(c.d. advertising)*, il circuito finanziario dei mezzi di pagamento (c.d. *payment processing*: servizi interbancari, carte di credito, moneta elettronica, ecc).

Il tema della corretta reputazione sul mercato è stato sottolineato in audizione, rilevando che vi sia negli operatori della società dell'informazione « *un fortissimo interesse ad assicurare un elevato livello di reputazione del mercato digitale, perché questo ha una ricaduta certamente su tali operatori e anche sull'intero funzionamento del mercato* » [(76)].

L'Unione Europea ha promosso accordi con la partecipazione degli ISP in tema di lotta all'incitamento all'odio e tutela dei minori. Va ricordato al proposito il *Memorandum of Understanding* del 2011 in materia di collaborazione volontaria tra titolari di diritti e *internet platform*, promosso dalla Commissione UE-DG *Market*, firmato da vari operatori della rete e da vari titolari di marchi.

Il MoU si proponeva di regolare su base consensuale la collaborazione tra titolari di diritti IPR e DPI e piattaforme, prevedendo una cooperazione finalizzata a rendere attivi una serie di filtri indispensabili per un'efficiente lotta alla contraffazione *on line*. Il MoU è stato oggetto di critiche da parte di operatori del settore [(77)] per la mancanza di criteri efficaci e misurabili di intervento e di regole applicabili a tutti i fornitori coinvolti, lasciando ad ogni piattaforma la regolamentazione degli interventi volti a bloccare venditori identificati come *infringer* seriali.

Va ricordato che in Italia l'articolo 18 del decreto legislativo n. 70, del 9 aprile 2003, prevede l'adozione di codici di condotta da parte delle associazioni imprenditoriali, professionali o di consumatori, trasmessi al Ministero delle attività produttive ed alla Commissione Europea. Tali codici contengono ogni utile informazione sulla loro applicazione e sul loro impatto nelle pratiche e consuetudini relative al commercio elettronico. Attraverso tali strumenti potrebbero essere definiti, su base consensuale, comportamenti positivi per il controllo della assenza di forme di contraffazione nel commercio elettronico.

In tema di *copyright*, va ricordata, nel giugno 2014, la stipula di un Memorandum d'intesa tra la IAB (*Interactive Advertising Bureau*), associazione per la raccolta pubblicitaria sulla Rete, la FAPAV (Federazione per la tutela dei contenuti audiovisivi e multimediali) e la FPM (Federazione contro la pirateria musicale e multimediale), per regolamentare le modalità di spontanea rimozione di contenuti pubblicitari individuati in siti pirata. Nel caso di pubblicità che appare

(76) V. audizione del 27 luglio 2016 del Presidente di Confindustria digitale, Elio Catania.

(77) V. le considerazioni espresse in merito nel corso dell'audizione del 10 marzo 2016 di Claudio Bergonzi, Segretario generale di Indicam.

su siti che smerciano merce contraffatta, nella forma di *banner* pubblicitari, il danno è infatti duplice: da un lato si trae in inganno il consumatore, contribuendo a dare un'apparenza di affidabilità di tali siti, favorendone in tal modo la crescita di contatti e le prospettive di *business*, dall'altro si danneggia l'immagine delle aziende che investono in pubblicità, in quanto i loro marchi legali sono associati a siti ove si smerciano prodotti illegali [(78)].

Negli altri Paesi europei si segnalano: nel Regno Unito, il *Digital Trading Standards Group* (DTSG), attivo dal 2014, di cui fanno parte diversi attori dell'industria pubblicitaria, che utilizzano la *Infringing Website List* (IWL), gestita dalla *Police IP Crime Unit* della polizia inglese, con lo scopo di minimizzare il fenomeno della collocazione della pubblicità su siti illeciti; in Francia, un MoU, in preparazione da parte del Governo, in collaborazione con l'industria pubblicitaria, sostanzialmente analogo a quello siglato in Italia, con la redazione di una *blacklist* di siti [(79)].

Il tema del coinvolgimento delle agenzie pubblicitarie è particolarmente importante, soprattutto nel settore del *copyright*, visto che i profitti dei siti illeciti che violano i DPI derivano essenzialmente da questo segmento di attività. Il mercato pubblicitario in Italia ha avuto un volume di investimenti *on line* pari a circa 2,15 miliardi di euro nel 2015, con una crescita stimata al 2016 a 2,4 miliardi di euro [(80)].

È stato riferito nelle audizioni che spesso gli inserzionisti non sono a conoscenza di dove sia ospitata la pubblicità commissionata, dal momento che i *banner* pubblicitari sono gestiti con sistemi parzialmente o totalmente automatizzati (c.d. *spider* automatici). Gli inserzionisti, dunque, spesso comprano la pubblicità non su determinati siti, ma attraverso pacchetti complessivi rapportati al numero di visitatori. Il problema è dunque la collocazione di *banner* su siti illeciti attraverso sistemi automatici che analizzano determinati volumi di traffico e in base ad essi indirizzano la pubblicità sui siti di maggiore frequentazione da parte degli utenti. Le agenzie pubblicitarie possono e debbono essere chiamate, in chiave proattiva, a responsabilizzarsi nelle proprie scelte di collocazione, ad esempio filtrando e creando *blacklist* di siti che commercializzano prodotti contraffatti o piratati, impedendo così che tali siti ricevano le inserzioni pubblicitarie.

In tema di IPR va ricordata l'iniziativa « Carta Italia », sottoscritta dal MISE, dal Consorzio del commercio elettronico italiano (NETCOMM), cui aderiscono aziende, ISP, servizi bancari [(81)] e da INDICAM il 14 luglio 2015, che prevede lo sviluppo di *best practices* per contrastare la contraffazione *on line* ed impegni da parte degli aderenti per eliminare le merci contraffatte dai siti e dalle piattaforme di *e-commerce*. La Carta intende promuovere lo sviluppo di *best*

(78) Il problema di riconvertire gli investimenti pubblicitari dai siti illegali a quelli legali, stante i molti e forti investimenti pubblicitari sui siti illegali, è stato evidenziato nel corso dell'audizione dalla Federazione contro la Pirateria Musicale e Multimediale (FPM) del 18 maggio 2016. Il Segretario Generale della FPM, Vespignani, ha riferito peraltro della scarsa applicazione del MoU, in quanto molte delle pubblicità veicolate su « siti pirata » è risultata essere stata gestita da agenzie non aderenti alla IAB.

(79) V. audizione del 21 luglio 2016 del Direttore generale di IAB Italia, Daniele Sesini.

(80) V. audizione del 21 luglio 2016 di Daniele Sesini, Direttore generale di I.A.B. Italia.

(81) Per la specifica degli aderenti al Consorzio v. sito *internet* NETCOMM- http://www.consorzionetcomm.it/ Associazione/Chi-Siamo/Soci/

practices dirette a contrastare il fenomeno della contraffazione *on line*, con adesione aperta a tutti i soggetti della filiera produttiva e distributiva operanti in Italia ed, in particolare, i *merchants* operanti *on line* e le piattaforme di *e-commerce*, i titolari dei diritti di proprietà industriale, i produttori licenziatari e le associazioni dei consumatori.

Il Consorzio Netcomm, aderente ad Ecommerce Europe, associazione europea del commercio elettronico, ha creato diversi *trustmark* (sigillo Netcomm, sigillo Business Partner, sigillo Ecommerce Europe Trustmark, sigillo Netcomm Gold), la cui funzione è di assicurare che i soggetti licenziatari, siano essi *merchant* (venditori di prodotti o servizi propri o di terzi *on line*) o piattaforme (mercato *on line* gestito da un soggetto titolare, su cui operano diversi venditori), svolgano un'attività di commercio trasparente e conforme alle leggi (c.d. *compliance*), al fine di rafforzare l'affidamento dei consumatori acquirenti *on line*.

Tra i principi fissati nel documento si segnalano:

• l'impegno per i *merchants* a garantire l'autenticità dei prodotti offerti in vendita sui rispettivi siti e per gli ISP a far sì che le condizioni di accesso alle piattaforme da parte dei venditori prevedano che questi ultimi assicurino che i prodotti offerti *on line* non siano contraffatti, verificandone l'originalità prima dell'offerta sulla rete, anche attraverso controlli nella filiera distributiva a monte dell'offerta;

• il riconoscimento che i prodotti non autentici possano essere individuati, a seguito dell'analisi del contenuto dell'offerta e/o della descrizione del prodotto, ovvero a seguito dell'analisi del comportamento generale del venditore e dall'insieme delle informazioni che lo riguardano;

• l'impegno degli aderenti alla Carta di cooperare tra loro e con il MISE, al fine di individuare e quindi porre in opera come *best practices*, misure conformi per individuare le offerte relative a prodotti non autentici prima della loro pubblicazione e prevenire il ripetersi di tali offerte;

• la definizione di una procedura di segnalazione, da parte dei titolari di diritti di proprietà industriale che abbiano fondato motivo di ritenere che i prodotti relativi a prodotti offerti *on line* da *merchant* o da una piattaforma non siano autentici e che un venditore offra prodotti non autorizzati al *merchant* e/o alla piattaforma, rispetto alla quale il *merchant* si impegna a ritirare sollecitamente dal proprio sito il prodotto, e la piattaforma ad informare prontamente il venditore, invitandolo all'immediato ritiro e ad adottare provvedimenti idonei, incluso il blocco dell'*account* del venditore, in caso di mancato ed ingiustificato ritiro della merce contraffatta; il potere di chiedere la rimozione del prodotto è previsto anche da parte delle associazioni dei consumatori e dalle associazioni dei titolari dei diritti.

8.5. La normativa di tutela del consumatore e in tema di comunicazioni elettroniche.

Un altro aspetto sul quale la Commissione ha avuto modo di soffermarsi è quello, nel settore delle controversie di consumo, e della tutela del consumatore, della procedura di risoluzione alternativa

delle controversie (ADR-*Alternative Dispute Resolution*). Si tratta di una procedura, non qualificata come arbitraggio, ma come gestione della negoziazione del reclamo, prevista dalla direttiva *On line Dispute Resolution* 2013/11/UE, recepita in Italia dal decreto legislativo 6 agosto 2015, n. 130, che è gestita da un organismo pubblico o privato riconosciuto dal MISE, che consiste nella veloce ed efficace soluzione dei conflitti di consumo senza ricorrere al giudice.

Per il ricorso a tale procedura è autorizzato in Italia il Consorzio NETCOMM, che ha concluso un accordo con 19 associazioni dei consumatori. Tale procedura riguarda i consumatori nel loro rapporto con i *merchant*s, ossia le aziende digitali che operano *on line*. Esiste un ADR anche a livello europeo [(82)].

Altra normativa da valutare sul tema è la direttiva 2011/83 sui diritti dei consumatori (*Consumer rights*), relativa ai contratti conclusi a distanza, tra cui quelli in rete, recepita in Italia dal decreto legislativo 6 settembre 2005, n. 206, Codice del Consumo. Tale normativa può costituire un *benchmark* di riferimento per la tutela del consumatore anche rispetto al contenuto della direttiva sull'*e-commerce*. In particolare la direttiva 2011/83 stabilisce una serie di principi per la protezione del consumatore nelle vendite *on line,* e costituisce la base degli interventi disposti in materia dall'Autorità Garante della Concorrenza e del Mercato.

Un ulteriore aspetto da approfondire è quello dell'esperibilità di azioni giudiziarie di gruppo (*class actions*), riferibili a tutti i prodotti contraffatti presenti sui siti illegali, anche per superare i problemi derivanti dal vincolo di territorialità delle azioni condotte su base nazionale e relative a singoli prodotti contraffatti.

Per quanto riguarda la normativa in tema di comunicazioni elettroniche, va ricordato che l'articolo 3 del decreto legislativo 1° agosto 2003, n. 259 « *Codice delle comunicazioni elettroniche* », indica, tra i principi generali di tale normativa, l'obiettivo di garantire i diritti inderogabili di libertà delle persone, comprese la libertà di comunicazione e la segretezza delle comunicazioni nell'uso dei mezzi di comunicazione elettronica, nonché il diritto di iniziativa economica ed il suo esercizio in regime di concorrenza. Tale disposizione potrebbe consentire lo sviluppo di misure che consentano una adeguata tutela dei diritti compromessi da fattispecie illecite, tra cui la contraffazione.

Il concetto di reti di comunicazione elettronica è esteso e riguarda tutti i sistemi di trasmissione via cavo, via radio, con fibre ottiche o altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, *internet*, le reti per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica se utilizzati per trasmettere i segnali. L'Autorità nazionale di regolamentazione è l'Autorità per le Garanzie nelle Comunicazioni.

8.6. Gli accordi in sede internazionale.

In sede internazionale va ricordata l'infelice vicenda dell'ACTA (*Anti-Counterfeiting Trade Agreement*), accordo commerciale plurila-

(82) V. audizione del 25 maggio 2016 del presidente del Consorzio del commercio elettronico italiano – NETCOMM, Roberto Liscia.

terale anticontraffazione, volto a dettare norme più efficaci per contrastare la contraffazione e la pirateria informatica, al fine di tutelare *copyright*, brevetti e altre forme di privativa su beni, servizi e attività legati alla rete, armonizzandole con le regole dell'Accordo TRIPs (*Trade-Related Aspects of Intellectual Property Rights*) in tema di diritto industriale, recepito nell'ordinamento italiano con la legge 29 dicembre 1994, n. 747. L'accordo, siglato a Tokyo il 26 gennaio 2012 tra 22 dei 28 Stati membri dell'Unione europea, tra cui l'Italia (non hanno firmato Cipro, Repubblica d'Estonia, Repubblica Slovacca, Germania e Paesi Bassi), Australia, Canada, Giappone, Corea, Messico, Marocco, Nuova Zelanda, Singapore, Svizzera e Stati Uniti d'America, è stato respinto per la ratifica dal Parlamento europeo il 4 luglio 2012.

8.7. La certificazione di qualità dei siti.

Altro intervento possibile è quello di un ruolo di garanzia svolto da una certificazione di qualità dei siti e delle piattaforme di vendita *on line*, effettuata da associazioni di categoria e da consorzi, che attesti la loro conformità al complesso di normative che regolano il commercio *on line* – oltre a quella per il commercio elettronico, quella in tema di lotta alla contraffazione, di tutela del consumatore e di smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE) – al fine di identificare le « offerte legali ».

Nel corso delle audizioni è stato illustrato il ruolo di garanzia che intende svolgere il Sigillo NETCOMM, concesso dal consorzio a chi rispetti 80 parametri legati al rispetto delle citate normative [(83)].

8.8. La tutela penale.

La tutela penale oggi applicabile ai reati di contraffazione via *web* è quella generale presente nell'ordinamento per la tutela del diritto d'autore e dei diritti di proprietà industriale. I reati di contraffazione non sono reati di natura strettamente informatica, ma sono fattispecie delittuose che anche nel *web* trovano un mezzo per la loro effettuazione. Le fattispecie incriminatrici esistenti in tema di contraffazione non prevedono nessuno strumento specifico per il contrasto di tali fenomeni sul *web* e va pertanto valutato se tale caratteristica delle norme identifichi oggi una vera e propria lacuna normativa.

L'individuazione degli autori di reato nel *web* è resa difficile dal fatto che le tecniche di indagine tradizionale a disposizione della magistratura non sono sempre applicabili ai « reati telematici ».

La principale tecnica di indagine investigativa è costituita dall'acquisizione dei *file di log,* ove sono memorizzati il nome di accesso dell'utente, la *password*, l'orario di connessione e le azioni compiute dall'utente in rete, che consentono di individuare il titolare del contratto di connessione alla rete, spesso coincidente con quello di telefonia. La Polizia Postale e il Nucleo speciale della Guardia di

(83) V. audizione del 25 maggio 2016 con il Presidente del Consorzio del commercio elettronico italiano – NETCOMM, Roberto Liscia.

Finanza operano al fine di estrapolare e tracciare gli indirizzi IP (*Internet Protocol address*) che hanno provocato il comportamento delittuoso, richiedendo gli intestatari e i *caller id* ai *provider* fornitori del servizio. Gli indirizzi IP sono etichette numeriche che identificano univocamente un dispositivo (PC, *tablet*, cellulare, ecc.), detto *host*, collegato a una rete informatica che utilizza l'*Internet Protocol* come protocollo di rete. Se gli assegnatari degli IP sono *provider* italiani, il reperimento delle informazioni avviene mediante decreto di acquisizione dei *files di log* notificato allo stesso *provider*. Se gli IP sono stati assegnati da fornitori di servizio *internet* situati all'estero, tale attività deve essere demandata all'Interpol.

Altre tecniche di indagine sono l'intercettazione di comunicazioni informatiche e telematiche, previste dall'articolo 266-*bis* c.p.p., introdotto dalla legge n. 547/1993, prevista per i reati commessi mediante l'impiego di tecnologie informatiche o telematiche e, specificatamente per i reati di contraffazione, e per il reato previsto dall'articolo 600-*ter* c.p. (pedopornografia). Il P.M., *ex* articolo 267 c.p.p., richiede al GIP l'autorizzazione a disporre le operazioni di intercettazioni telematiche, che viene concessa con decreto motivato quando vi siano gravi indizi di reato e l'intercettazione risulti indispensabile ai fini della prosecuzione delle indagini. È possibile altresì la duplicazione delle caselle di posta elettronica utilizzate dall'indagato, come forma particolare di intercettazione telematica.

Per quanto riguarda la perquisizione, il sequestro *ex* articolo 253 c.p.p. e la perizia del materiale sequestrato, il comma 2 dell'articolo 253 c.p.p. indica quale corpo del reato non solo le cose sulle quali o mediante le quali il reato è stato commesso, ma anche quelle che ne costituiscono il prodotto, il profitto o il prezzo. In sede giurisprudenziale è stata riconosciuta alternativamente la natura del *computer* o del *server* come corpo di reato o mezzo attraverso il quale si è perpetrato il reato, oppure di « cosa pertinente al reato »; l'esame di essi potrebbe dimostrare il fatto criminoso nel suo complesso, pure se il vincolo pertinenziale non sussiste in via sistematica tra il reato e l'intero supporto informatico, in quanto si avrebbe una arbitraria estensione del vincolo a tutti i dati e i programmi presenti sull'*hard disk* o sul *server*, anche quelli di contenuto lecito. In molti casi, pertanto, in luogo del sequestro, caducabile in sede di riesame dei provvedimenti, è stata disposta una masterizzazione delle tracce di reato tramite ispezione delegata *ex* articolo 246 c.p.p. in quanto atto irripetibile.

Altro problema esistente è quello della conservazione dei dati da parte delle società di telecomunicazione. L'articolo 123 del T.U. n. 196/2003 sul trattamento dei dati personali prevede la cancellazione o l'anonimizzazione, da parte del fornitore della rete pubblica di comunicazione, dei dati personali relativi al traffico quando non sono più necessari per la trasmissione della comunicazione elettronica e, comunque, per un periodo non superiore a sei mesi. In sede interpretativa si è ritenuto ricomprendere all'interno della categoria dei dati personali relativi al traffico anche quelli del traffico *web* raccolti e memorizzati dai fornitori di accesso alla rete e dei relativi servizi nella gestione dei *files di log* e dei correlati *data base* contenenti i codici identificativi e i dati anagrafici dei clienti. L'articolo 132 dello

stesso T.U. prevede che i dati relativi al traffico telefonico siano conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

9. CONCLUSIONI E PROPOSTE

L'analisi approfondita condotta dalla Commissione conduce ad una serie di considerazioni conclusive e ad un ventaglio di proposte operative.

Due prime considerazioni riguardano l'adeguatezza della normativa internazionale, comunitaria e nazionale in materia e la necessità di tutelare dalle frodi nel commercio elettronico i diritti di proprietà industriale e il diritto d'autore in maniera comparabile.

Inevitabilmente, si osserva che l'analisi della normativa mostra come in materia di lotta alla contraffazione nel commercio elettronico vi sia una sostanziale assenza di accordi internazionali, rispetto ai quali svolgono un ruolo di « supplenza » la normativa e le prassi giurisprudenziali degli Stati Uniti, cui spesso le grandi aziende dell'economia digitale si conformano.

La disciplina del commercio elettronico in sede comunitaria, con la più volte esaminata limitazione della responsabilità contenuta nella direttiva sull'*e-commerce*, è molto datata nel tempo ed è divenuta obsoleta, in un settore ove l'evoluzione tecnologica e le dinamiche del mercato si sono sviluppate a ritmi vertiginosi. La realtà del mercato digitale cui si rivolgeva è mutata profondamente negli ultimi anni, perché oggi esiste una pluralità di ISP, molto più ampia di quella individuata dalla direttiva, che sono divenuti erogatori di servizi diversificati, con il conseguente aumento esponenziale dei profitti, cose che non possono non determinare un conseguente ed equo aumento delle responsabilità per queste aziende digitali.

Il contenuto delle legislazioni nazionali, d'altronde, non può derogare al dettato comunitario e quindi non sono ipotizzabili, dal punto di vista normativo, iniziative nazionali autonome di tipo sostanziale circa i profili più rilevanti richiamati.

Costituisce parte del problema anche l'assenza di un organismo internazionale di regolazione per taluni aspetti delle attività su *internet*, quali la tutela dei diritti dei terzi rispetto agli illeciti.

La Commissione ritiene perciò che vada sostenuta ed implementata ogni iniziativa dell'UE in tema di revisione della normativa sull'*e-commerce*, già avviata con una consultazione pubblica, nel senso di garantire una maggiore tutela, per quanto riguarda la lotta alla contraffazione e alla pirateria digitale, ai titolari di diritti.

Il tema di prevedere forme di maggiore responsabilizzazione degli ISP rispetto alle attività illecite veicolate su *internet* non deve essere in alcun modo lesivo della libertà di espressione o costituire un limite per lo sviluppo del commercio *on line*, che costituisce un valore primario nell'economia digitale di questi anni. Si può però tradurre nell'adozione di forme equilibrate di contemperamento di tutti gli

interessi in gioco che prevedano obblighi proattivi e preventivi di vigilanza, con il superamento della procedura di *Notice and Take Down* e l'approdo verso l'approccio del *Notice and Stay Down*.

D'altronde, i dati reali del mercato dell'*e-commerce* di cui occorre tenere conto mostrano che le aziende titolari dei diritti di proprietà industriale non trovano un'adeguata tutela nel solo potere di segnalazione, violazione per violazione, nel quale si sostanzia il *Notice and Take Down*, troppo frammentato rispetto all'enorme numero delle contraffazioni *on line* ed oneroso, sia in termini organizzativi che finanziari, per le aziende danneggiate, particolarmente per le PMI.

Le recenti proposte di modifica alle direttive UE in tema di diritto d'autore, nel settore degli audiovisivi, mostrano una linea di tendenza che introduce, anche se parzialmente, forme di estensione della responsabilità in casi di gravi comportamenti illeciti.

Un tema sul quale occorre riflettere è quello della necessità di garantire forme di tutela equiparata tra i diritti di proprietà industriale e il *copyright*.

La constatazione che in sede comunitaria non sono ipotizzabili modifiche a breve termine sulla direttiva sull'*e-commerce*, a differenza di quanto accade per il diritto d'autore sui media audiovisivi, accentua il problema.

La tutela degli IPR, come più volte richiamato, appare più difficoltosa rispetto a quella del diritto d'autore, per due ordini di motivi: per la sussistenza di soluzioni tecnologiche, già operanti in rete, in grado di riconoscere immediatamente le opere coperte da *copyright*, che sono ormai spesso originariamente in formato digitale. Per le merci, invece, l'identificazione del falso è già di per sé difficile rispetto a prodotti imitati con perizia, quando il controllo deve essere effettuato sui prodotti fisici; ma è ancora più difficile su merci vendute in rete, perché spesso queste non sono nella disponibilità degli ISP e perché quindi è necessario svolgere complesse indagini solo su annunci di vendita e si tratta di esaminare parametri quali la sussistenza di licenze di vendita, l'identità degli operatori, ecc.

Inoltre la realtà economica mostra come le opere coperte dal diritto d'autore, segnatamente gli audio video, sono nella disponibilità di grandi aziende multinazionali, le cui dimensioni economiche consentono lo sviluppo di strategie di tutela maggiori ed una possibilità di interlocuzione e negoziazione più efficace con gli ISP, mentre le merci coperte da marchi contraffatti sono spesso prodotte da aziende non solo di grandi dimensioni, ma anche da PMI, che, ad esempio nel settore agroalimentare, sono espressione di filiere produttive territoriali, che non hanno né la capacità organizzativa né il peso economico per attivare una difesa efficace.

Il tema, dunque, è molto rilevante e richiede iniziative positive.

La strada da perseguire è quindi l'introduzione di un dovere di diligenza (*Duty of Care*) che sia alla base dell'attività di ingaggio degli ISP nella tutela degli IPR sulla rete. Di questo concetto fanno parte l'introduzione di regole di gestione chiare ed efficaci nonché uniformi per le segnalazioni effettuate dai titolari di diritti, nonché attuare ogni misura, anche tecnologica, al fine di impedire il ripetersi di attività illecite attraverso le loro piattaforme. Al pari è da considerarsi parte di un concetto di « *Duty of Care* » anche l'impegno degli ISP, e in

generale degli intermediari, a introdurre misure volte a impedire l'*upload* di contenuti lesivi dei diritti, potendo quindi applicare misure tecnologiche certamente alla portata e fatta salva l'assenza di impatto sulle libertà fondamentali, andando a concentrarsi sui soli contenuti lesivi dei diritti IPR.

Un altro risultato concreto che emerge dall'inchiesta svolta è la consapevolezza che non esiste una sola soluzione per combattere i fenomeni contraffattivi, ma serve invece una pluralità di tecniche di contrasto, atteso che le forme del commercio elettronico sono diversificate, a seconda che si tratti di piattaforme di vendita in modalità *retail* o di *marketplace*, di piattaforme di mero *hosting*, di *social network*, di motori di ricerca. Un'unica soluzione per il contrasto della contraffazione non può esistere, sia per la virulenza del fenomeno criminale, legato a organizzazioni illecite di dimensioni internazionali, sia per la diversità merceologica dei beni oggetto di contraffazione, ognuno dei quali settori ha le proprie caratteristiche e le forme più efficaci di contrasto.

In base a tale considerazioni la Commissione formula le seguenti proposte per un contrasto efficace alla contraffazione nel commercio elettronico:

a) Una corretta informazione ed adeguata sensibilizzazione del cittadino consumatore, con particolare riguardo agli acquisti o alla fruizione di servizi sul *web*, resta ineludibile. Permane, infatti, una scarsa percezione e considerazione circa la natura non solo illegale, ma socialmente ed economicamente devastante del commercio di merci contraffatte e della pirateria digitale. Se in audizione si è avuto conferma da parte degli auditi di tale fatto, giova riaffermare la necessità di un impegno determinato e di una strategia integrata tra istituzioni, forze dell'ordine, associazioni di categoria, ecc. per una più efficace alfabetizzazione degli utenti del *web* in materia. In particolare, oltre ai rischi connessi ad incauti acquisti – si pensi in particolare ai farmaci o a prodotti con materiali tossici – è necessario rendere maggiormente noto il potenziale distruttivo che la contraffazione ha sull'economia legale, la vita delle imprese sane, il lavoro regolare e i suoi diritti, ecc. Se non aumenterà la consapevolezza del disvalore sociale associato alla contraffazione difficilmente sarà possibile compiere soddisfacenti passi avanti in termini di prevenzione e contrasto;

b) un primo *step* da colmare, come detto, è quello rappresentato dall'adozione di procedure di contrasto non solo di tipo reattivo, secondo le modalità attuali del *Notice and Take Down*, ma anche di anche di tipo proattivo e preventivo, secondo la procedura del *Notice and Stay Down*.

La soluzione può essere trovata, in sede preventiva, con sistemi di filtraggio automatici che operino rispetto a procedure di segnalazione non solo individuali, per singoli illeciti o da parte di singole aziende titolari di IPR, ma aventi portata complessiva, per interi settori merceologici e tipologie di illeciti. Questo ruolo, oltre che dalle singole aziende, può essere svolto efficacemente anche dalle associazioni rappresentative delle singole categorie merceologiche e dei

consumatori, da consorzi, che interloquiscano con gli ISP, con il supporto delle forze dell'ordine, in un quadro organico e continuativo di intervento. Serve, in altri termini, l'assunzione di una responsabilità più forte da parte degli ISP, utilizzando i sistemi di filtraggio che le più avanzate tecnologie mettono a disposizione; è auspicabile la predisposizione di *black list*, definite congiuntamente, quale risultante dinamica di segnalazioni di tipo seriale inviate dai titolari dei diritti lesi, tra ISP, rappresentanti delle aziende private ed Istituzioni (i Ministeri competenti, a tutela del Made in Italy e le forze dell'ordine), per identificare gli operatori, gli *account*, gli IP e i siti responsabili di transazioni illegali ripetute nel campo della contraffazione, portando alla loro impossibilità di continuare ad operare, anche se assumano altre forme o identità.

È importante sottolineare che la cooperazione tra aziende titolari di diritti e ISP è necessaria, in quanto non sarebbe ragionevole né sostenibile prevedere forme di attivazione generale ed indistinta a carattere preventivo degli ISP, da condurre su una base di dati illimitata quale quella dell'intero « universo *internet* »; viceversa, l'uso di segnalazioni di tipo seriale, effettuate da associazioni rappresentative, potrebbe delimitare il campo del controllo preventivo attraverso i sistemi automatizzati, e renderlo in tal modo efficiente, perfettibile nel tempo ed economicamente sostenibile.

c) Dal punto di vista tecnologico sistemi di filtraggio sono già operativi per determinate categorie di reati gravi (terrorismo, incitamento all'odio etnico e religioso, pedopornografia), ovvero per condizionare l'accesso ad *internet* nelle ricerche svolte in determinati contesti geografici; l'evoluzione tecnica degli algoritmi di ricerca consente ricerche sempre più accurate, essendo passati dalla ricerca lessicale delle parole ad una selezione basata su una pluralità di elementi, tra cui il *page ranking* e sistemi di « *machine learning* », ossia programmi in grado di migliorare le ricerche estraendo « regolarità » significative tra i dati tratti dall'enorme mole di informazioni in proprio possesso, permettendo « l'apprendimento » progressivo dell'intero sistema nell'individuazione delle risposte corrette da fornire agli utenti.

Possono essere trovate dunque soluzioni equilibrate, innanzitutto in sede di accordi consensuali con gli ISP, e poi anche in sede normativa di sostegno, per l'adozione di procedure che includano anche la contraffazione nell'insieme delle fattispecie di reato di elevata pericolosità, in considerazione della gravità sociale ed economica del fenomeno, dei danni causati alle aziende, al lavoro regolare, ai consumatori e all'erario statale, e della necessità di combattere le organizzazioni criminali che sono ormai sistematicamente dedite a questo traffico illecito.

d) Tra le misure utilizzabili per limitare il traffico commerciale contraffattivo, dando seguito alla definizione delle *black list*, sempre nel quadro di una tutela preventiva svincolata da singole e specifiche fattispecie di illecito, devono essere citati, sulla base di esperienze già avviate da alcuni ISP, il rifiuto a creare nuovi profili e la disattivazione degli IP per gli utenti il cui *account* sia stato disattivato, attraverso

strumenti automatici in grado di rilevare se tali soggetti, utilizzando lo stesso *device* o indirizzo IP, cerchino di ricreare un profilo per svolgere lo stesso tipo di attività; ovvero l'associazione ai contenuti audio-video, e multimediali più in generale, di un'impronta digitale (c.d. *Fingerprint*), che in caso di caricamenti dello stesso contenuto da parte di utenti non legittimati ne consenta l'immediata identificazione;

e) Per l'individuazione delle merci legali, una strada praticabile può essere anche quella della certificazione di qualità dei siti e delle piattaforme di vendita *on line*, attraverso l'apposizione di sigilli digitali, come quelli elaborati dal Consorzio *Netcomm* e da *Ecommerce Europe*, sulla base di modelli di certificazione elaborati da enti terzi certificatori, che attestino la trasparenza e il pieno rispetto di tutte le normative (e magari delle migliori prassi negoziate) di settore del *trading on line*;

f) Nell'affrontare il problema dell'assunzione dei costi di gestione dei sistemi preventivi di monitoraggio occorre valutare le risorse disponibili, tenendo conto del *value gap* che le transazioni commerciali *on line* determinano per gli ISP e che esiste tra profitti degli intermediari digitali ed aziende produttrici, anche per l'indotto pubblicitario ospitato sulle piattaforme. Tale fattore economico, su un piano di equità, deve essere considerato, come d'altronde già avvenuto nel caso di attribuzione di profitti derivanti dall'utilizzazione fuori licenza sulle piattaforme digitali a favore dei titolari di *copyright*;

g) Nell'adozione di misure proattive o reattive va considerata con grande attenzione la tipologia di piattaforma di commercio elettronico.

La realtà operativa mostra che, mentre per le piattaforme di *hosting* pubblicitarie e per quelle di *hosting* non pubblicitarie se ne registra la progressiva adozione, a seguito di accordi tra ISP e titolari di diritti, maggiori difficoltà si evidenziano per i motori di ricerca e per i *social network* e, in generale per la tutela degli IPR rispetto ai DPI.

Nei primi due casi si tratta di ambienti digitali controllati nell'accesso, per il quale vi sono termini e condizioni di entrata che prevedono esplicitamente il divieto di pubblicazione di contenuti che non rispettino i diritti di proprietà intellettuale altrui su *copyright* e marchi commerciali e l'impegno delle piattaforme a fornire gli strumenti necessari per la protezione di questi diritti; in particolare, sono state attivate misure proattive per la tutela degli DPI, che operano in automatico all'atto del caricamento di contenuti multimediali, attraverso sistemi di *machine learning*, consentendone la rimozione o prevedendo la possibilità ai titolari dei diritti DPI di chiedere la monetizzazione dell'uso non autorizzato degli audio video, in una concezione allargata del diritto d'autore. Per la tutela degli IPR, invece, il problema è molto più complesso, perché non vi sono opere in formato digitale che possano essere automaticamente esaminate all'atto del caricamento in rete, ma solo annunci di merce.

I problemi maggiori, come sottolineato, si pongono nel caso di piattaforme che ospitano motori di ricerca sul *web*. La tesi sostenuta

dagli ISP auditi è che il ruolo degli operatori sia meramente passivo, con conseguente esenzione della responsabilità, e che i motori di ricerca non abbiano il compito e la possibilità di controllare il contenuto dei siti che già si trovano sulla rete, ma solo quello di individuare tutti i siti che rispondano ai parametri degli algoritmi di ricerca. Anche in questo caso, tuttavia, occorre valutare se l'evoluzione dei sistemi di filtraggio e di ricerca, possa portare all'esclusione tra i risultati della ricerca, di siti illegali.

h) Per quanto riguarda gli interventi repressivi da parte delle Istituzioni competenti, in sede sia giurisdizionale che amministrativa, segnatamente con l'oscuramento dei siti illegali, va valutata l'opportunità di regolare, anche dal punto di vista normativo, la prassi di contrasto elaborata dalla Procura di Milano, in materia di siti *web* dediti a forme di contraffazione, che consente decreti di sequestro ed oscuramento dei siti « in bianco », con estensione agli altri siti aperti successivamente, a seguito delle operazioni di reindirizzamento, senza necessità di ulteriori provvedimenti giudiziari. Altro profilo da valutare è quello di rafforzare la tutela attraverso il blocco congiunto dell'indirizzo IP con il DNS (*Domain Name System*), funzione di *internet* che trasforma un nome dell'URL in un indirizzo IP, attraverso la quale la rete arriva al *server* cercato. Ulteriore profilo da valutare, infine, è quello di sanzionare per legge il potere delle autorità amministrative indipendenti (AGCOM e AGCM) di disporre i blocchi, attualmente previsti da un Regolamento o in via di prassi;

i) Fondamentale è poi lo sviluppo anche in Italia dell'approccio *Follow The Money*, soprattutto per la vendita di merci contraffatte, sulla scorta delle *best practices* statunitensi illustrate in precedenza, promosse dall'*International Anticounterfeiting Coalition* e contenute nel piano d'azione del luglio 2014, elaborato dalla Commissione europea.

Per la tutela degli IPR costituiscono un efficace strumento di lotta alla contraffazione nel commercio elettronico le intese tra titolari di marchi e segni distintivi, ISP e aziende di gestione dei mezzi di pagamento elettronici (carte di credito, *internet banking*), che consentono di bloccare, in presenza di transazioni relative a merce contraffatta sul *web*, l'effettuazione di pagamenti *on line* per l'acquisto di tale merce, rendendo non attivabili i circuiti finanziari digitali riguardo ai siti interessati.

Viceversa nel settore del diritto d'autore relativo al *file sharing* o all'*upload-download* illegale di audiovisivi, ove il profitto per gli operatori non deriva in massima parte dallo scarico di film o musica, che anzi talvolta è gratuito, ma dalla pubblicità ospitata dai siti, in rapporto al numero di contatti e il *page rank* degli stessi, l'approccio *Follow the Money* si traduce nella definizione di accordi tra ISP, titolari dei DPI e agenzie pubblicitarie, per impedire la presenza di *banner* pubblicitari sui siti illeciti.

j) Anche le agenzie di pubblicità debbono e possono essere chiamate ad un maggior grado di responsabilità: se, come indicato al punto precedente, è proprio la pubblicità a sostenere economicamente

una parte consistente della pirateria audio video e se, come illustrato, spesso i produttori inserzionisti non sono a diretta conoscenza delle scelte effettuate dalle agenzie, è allora indispensabile portare a esigibilità una filiera di responsabilità che impegni inserzionisti e agenzie nella messa al bando dei siti che commercializzano merce contraffatta o contenuti digitali piratati;

k) in via generale, sulla base delle esperienze maturate nella realtà operative di cui la Commissione ha preso atto nel ciclo di audizioni, lo sviluppo degli accordi consensuali tra ISP e aziende per prevenire i fenomeni illeciti, come nel caso delle già citate *black list* di siti illegali, è molto importante. Gli accordi sono necessari per bloccare la vendita di prodotti non autentici, in quanto possono coinvolgere, oltre ai *provider* e alle aziende, anche i fornitori di « *side services* », quali i trasportatori fisici dei prodotti (c.d. *shipping)*, il sistema pubblicitario (c.d. *advertising*), il circuito finanziario dei mezzi di pagamento (c.d. *payment processing*). La forza intrinseca di questi accordi è rappresentata dall'interesse degli operatori della società dell'informazione a mantenere una corretta reputazione sul mercato digitale, perché questo elemento ha una ricaduta commerciale evidente, sia in termini di fidelizzazione dell'utenza che di prevenzione di eventuali richieste risarcitorie, che particolarmente negli Stati Uniti sono state riconosciute come attivabili.

La Commissione valuta positivamente l'iniziativa « Carta Italia », sottoscritta il 14 luglio 2015 dal MISE, dal Consorzio del commercio elettronico italiano (NETCOMM), cui aderiscono aziende, ISP, servizi bancari e da INDICAM, che prevede lo sviluppo di *best practices* per contrastare la contraffazione *on line* ed impegni da parte degli aderenti per eliminare le merci contraffatte dai siti e dalle piattaforme di *e-commerce*. Va valutata, peraltro, la necessità di valutare il contesto giuridico ove gli accordi su base volontaria operano. L'ordinamento statunitense è caratterizzato da due elementi: il forte ruolo esercitato dagli accordi su base privatistica e consensuale, come quelli sviluppati efficacemente dall'IACC con il *Rogue Block Program*; la presenza di un sistema giudiziario improntato ai principi della *common law*, che dà valore giuridico di precedente alle decisioni assunte in sede giurisdizionale. In Europa, viceversa, per la tutela dei diritti il sistema è improntato alla supremazia della normativa, sulla base di norme cogenti ed imperative che per la tutela di interessi generali prevalgono sull'autonomia dei privati e sulle decisioni in sede giurisdizionale. Di qui la necessità che le istituzioni rappresentative riflettano approfonditamente, anche in sede comunitaria, sulla necessità di accompagnare le iniziative del mercato da percorsi di adeguamento e di revisione delle norme.

l) In sede normativa va sviluppata appieno la previsione contenuta nell'articolo 18 del decreto legislativo n. 70/2003, che già prevede l'adozione di codici di condotta in tema di commercio elettronico da parte delle associazioni imprenditoriali, professionali o di consumatori, da trasmettere al Ministero delle attività produttive ed alla Commissione Europea.

L'efficacia di tali intese va tuttavia valutata attentamente perché è emerso in audizione che la loro attuazione può essere inficiata dalla presenza di molte imprese operanti sul mercato che non aderiscono alle associazioni di categoria e che, quindi, non si adeguano ai comportamenti individuati. Di qui la necessità di riflettere sulla previsione di obblighi di comportamento che siano applicabili a tutti gli operatori del settore, per i quali servirebbe un'adeguata cornice normativa, innanzitutto in sede comunitaria, diversa e più evoluta di quella dell'esenzione della responsabilità per gli operatori ISP. Di questa istanza la Commissione si è fatta portatrice, sia presso il Governo italiano, da sempre più sensibile al problema e che ha assunto anche in recenti consultazioni posizioni avanzate rispetto agli altri paesi Ue, sia presso la stessa Commissione europea.

m) Per quanto riguarda la tutela degli IPR, segnatamente nel settore dell'audio video, va ricordata e riaffermata la positiva direzione di sviluppo che mette al centro l'offerta legale e gratuita di contenuti sostenuta dagli introiti pubblicitari. Non compete certo alla Commissione definire le strategie commerciali delle aziende, né esprimere valutazioni di carattere generale, ma appare di ogni evidenza, rispetto ai profili di interesse di questa indagine, come soluzioni efficaci e competitive di offerta legale riducano lo spazio al mercato illegale, alle sue filiere e alle organizzazione criminali, con costi di sistema infinitamente più contenuti. Per questa ragione pare opportuno non solo evidenziare questa consolidata esperienza, ma valutare sotto tutti i profili quale sostegno possa venirne dalle istituzioni, anche in termini di promozione di una più equilibrata distribuzione dei profitti;

n) se il *web* si è rivelato un ambiente straordinario per la crescita del mercato, la cattiva distribuzione della ricchezza (il c.d. *value gap*) è invece un ostacolo per la crescita dei ricavi di artisti, produttori e aventi diritto. Perché l'offerta legale possa davvero essere una strada condivisa di crescita e sviluppo del mercato digitale dell'audiovideo è quindi auspicabile un equilibrio più soddisfacente tra il valore che ritorna verso l'industria della produzione nel suo complesso e il valore accumulato da alcuni servizi digitali che consentono l'accesso. Le associazioni più rappresentative, oltre alla richiamata maggiore responsabilizzazione dei giganti del *web*, da tempo chiedono che questi siano obbligati a pagare *fee* di mercato ai titolari dei diritti. Non si tratta naturalmente di una strada che possa essere intrapresa da un solo Paese, ma di una proposta concreta per affrontare un problema ineludibile;

o) per quanto riguarda il contrasto alla contraffazione e la tutela del diritto d'autore, appare sempre più anacronistico l'obbligo del contrassegno Siae, così come previsto dalla legge 22 aprile 1941, n. 633. Come rilevato nel corso delle audizioni, tale obbligo persiste ormai in una strettissima minoranza di paesi europei (oltre all'Italia vi sono solo Portogallo e Romania). Per un mercato che ha assistito al sorpasso del digitale sul prodotto fisico – e che ha visto di conseguenza la stessa attività illegale della contraffazione muoversi ormai completamente nella dimensione digitale – l'apposizione del

bollino Siae appare agli occhi dei produttori sempre più come un incomprensibile e anacronistico balzello sui *cd, dvd* e gli altri prodotti fisici. Peraltro, proprio le principali associazioni di categoria rilevano la penalizzazione oggettiva, in termini di costi e quindi di prezzo finale, che il bollino determina rispetto ai prodotti del mercato estero, al mercato digitale e agli stessi prodotti acquistati *on line*, tutti esentati da tale obbligo di apposizione;

p) infine, altri strumenti praticabili nel settore dell'*e-commerce* riguardano la tutela del consumatore nelle transazioni elettroniche, quali, nel settore delle controversie di consumo, le procedure di risoluzione alternativa delle controversie (ADR-*Alternative Dispute Resolution*), per la gestione della negoziazione del reclamo. La stessa direttiva 2011/83 sui diritti dei consumatori relativa ai contratti conclusi a distanza, tra cui quelli in rete, recepita in Italia dal D.Lgs. 6 settembre 2005, n. 206, « Codice del Consumo » e l'articolo 3 del decreto legislativo 1º agosto 2003, n. 259, « *Codice delle comunicazioni elettroniche* », che garantisce il diritto di iniziativa economica ed il suo esercizio in regime di concorrenza, offrono spunti interessanti in materia.

Conclusivamente, occorre sottolineare come il settore del commercio elettronico, per le potenzialità che offre e le prospettive di sempre maggiore sviluppo nei prossimi anni, richieda, e al tempo stesso possa trarre beneficio, da un adeguato sistema di lotta alle forme di contraffazione che lo inquinano.

Dinanzi a tale realtà, estremamente pericolosa per le molte implicazioni che si sono descritte, ma che non destano un adeguato allarme sociale, è opportuno assumere un atteggiamento attento rispetto ai bisogni di tutela che i titolari di diritti manifestano e garantire un'adeguata protezione dei consumatori, che sempre più debbono essere informati e tutelati.

L'approccio corretto è quello di perseguire un equo contemperamento di interessi, assicurando la tutela necessaria a tutti i diritti coinvolti, aprendo ad un'impostazione innovativa che superi atteggiamenti conservativi o difensivi dello *status quo* e che non favorisca la contrapposizione tra settori produttivi, che debbono invece essere pienamente coinvolti in termini cooperativi nel quadro delle dinamiche odierne delle attività economiche. Per questa ragione, pertanto, le proposte indicate contemplano, congiuntamente, tanto la necessità di un'evoluzione e di un adeguamento del quadro normativo comunitario e nazionale, quanto la promozione e lo sviluppo delle migliori pratiche pattizie già sperimentate in sede nazionale ed internazionale.

170222018690