LUISS

Dipartimento di Giurisprudenza

Cattedra di Diritto Penale 2

Tutela penale della proprietà intellettuale e responsabilità delle piattaforme digitali secondo il Digital Service Act.

Chiar.mo Prof. Antonio Gullo

RELATORE

Chiar.ma Prof.ssa Maria Novella Masullo

CORRELATORE

Pietro Giordano
Matr. 157913

CANDIDATO

Anno accademico 2022/2023

Sommario

INTRODUZIONE.

La presente dissertazione si pone l'obiettivo di analizzare quali siano i casi in cui una piattaforma digitale può essere ritenuta penalmente responsabile in virtù di violazioni, commesse dai propri utenti, di fattispecie criminose aventi ad oggetto la tutela dei diritti di proprietà intellettuale. La questione è particolarmente spinosa: ipotizzare, infatti, in capo ai gestori di piattaforme digitali un dovere di controllo – sia esso *ex ante* ovvero *ex post* – del materiale generato e/o condiviso dagli utenti attraverso i rispettivi servizi, in assenza del quale potrebbe scaturire una responsabilità penale, potrebbe equivalere ad introdurre uno strumento di censura privata che mal si concilierebbe con alcune delle libertà fondamentali dettate dal nostro ordinamento – quale, ad esempio, la libertà di manifestazione del pensiero *ex* articolo 21 della nostra Costituzione.

Nel corso dell'ultimo ventennio, la digitalizzazione ha giocato un ruolo fondamentale nell'economia mondiale. Non è un caso che nel 2019, sette tra le dieci più grandi imprese del mondo erano presenti sul mercato digitale, il più delle volte come intermediari *online*.[1] Secondo un'indagine condotta dall'Eurostat[2] nel 2021, in quello stesso anno il 74% degli utenti di Internet ha fatto acquisti online nel territorio europeo e il 42% degli *e-buyer* ha effettuato acquisti per un importo compreso tra 100 e meno di 500 euro nei 3 mesi precedenti l'indagine.[3]

Ciò è dovuto al fatto che le attività quotidiane di imprese e consumatori si sono spostate sempre più nella dimensione *online*: dallo *shopping* allo sfruttamento di contenuti, dalla socializzazione alla stipula di un mutuo, arrivando fino all'organizzazione di un viaggio. Ogni tipo di attività, oggi, può essere effettuata in via digitale.

---

[1]Si fa riferimento ad Apple, Microsoft, Amazon.com, Alphabet, Facebook, Alibaba, and Tencent Holdings.

[2]Eurostat è l'ufficio statistico dell'Unione europea, responsabile della pubblicazione di statistiche e indicatori di alta qualità a livello europeo che consentono di effettuare confronti tra Paesi e regioni. Per un approfondimento si veda: *https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/eurostat-european-statistics_en*

[3]Si veda: *https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics_for_individuals#General_overview*

Tuttavia, se da un lato sono innumerevoli i vantaggi apportati da Internet, altrettanto numerose possono essere le minacce che vi si celano: se quasi ogni attività quotidiana può essere compiuta in rete, non bisogna dimenticare che lo stesso vale per le attività illecite. I comportamenti in violazione della legge tenuti dagli utenti in rete possono assumere diverse forme, tra queste particolare rilevanza ha la violazione dei diritti di proprietà intellettuale: si pensi alla vendita di prodotti contraffatti sui mercati digitali[4] o alla riproduzione o condivisione abusiva di opere dell'ingegno protette tramite programmi di condivisione dei documenti.[5]

I prodotti contraffatti e i contenuti «pirata», cioè prodotti e/o distribuiti in violazione delle norme sul diritto d'autore, sono presenti in quasi ogni settore di mercato. Di conseguenza, tutte le aziende che sfruttano la proprietà intellettuale («PI») e, i marchi in particolar modo, comprese le piccole e medie imprese («PMI»), sono esposte al rischio di commercio illecito di loro prodotti contraffatti con conseguente perdita di potenziale profitto. Allo stesso tempo, il 40% delle PMI dell'UE non monitora i propri mercati alla ricerca di contraffazioni e potenziali violazioni della propria PI, non avendo le risorse per farlo,[6] e ciò risulta ancor più grave se si pensa che le PMI svolgono un ruolo importante nella maggior parte delle economie: ad esempio, nei Paesi dell'OCSE[7] queste costituiscono la maggior parte delle imprese e rappresentano circa i due terzi dell'occupazione totale.[8]

---

[4]«Il termine mercato in economia indica un luogo tradizionalmente fisico in cui diversi soggetti (operatori economici) realizzano tra loro degli scambi commerciali di diversa natura. Con l'avvento di Internet, si è assistito alla creazione e successivamente allo sviluppo di un mercato digitale. Il web, infatti, si è trasformato in un enorme mercato globale che ha avvicinato domanda e offerta, anche se fisicamente lontane. Il mercato digitale ha affiancato in alcuni settori le vendite fisiche, permettendo di ampliare la clientela servita dall'aziende, in altri, invece, si è totalmente sostituito al mercato tradizionale». Per un approfondimento si veda: *https://www.digital-coach.com/it/blog/case-histories/mercato-digitale/*

[5]Con il termine *file*-sharing «si intende la condivisione di file all'interno di una rete di pc *client-server* o ancora *peer-to-peer*. La traduzione letterale del termine inglese file sharing è infatti condivisione di file. Nel 2020 solitamente ci si riferisce al termine file sharing con riferimento ad un apposito sistema che consente agli utenti di condividere file e documenti sul web o all'interno della medesima rete. Grazie ai programmi e siti di file sharing è infatti possibile trasferire dei documenti da un device all'altro». Così: *https://www.chcbs.ch/blog/188/cos%C3%A8-il-file-sharing-ecco-tutto-quello-che-dovete-sapere.html*

[6]OECD e EUIPO, *Risks of Illicit Trade in Counterfeits*, cit., 10.

[7]«Con 57 Stati partecipanti del Nord America, dell'Europa e dell'Asia, l'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE) è la più grande organizzazione di sicurezza regionale al mondo. L'OSCE si adopera per assicurare stabilità, pace e democrazia a oltre un miliardo di persone attraverso il dialogo politico su valori condivisi e attività pratiche che mirano ad avere effetti duraturi». Per un approfondimento: *https://www.osce.org/it/who-we-are*

[8]OECD e EUIPO, *Risks of Illicit Trade in Counterfeits to Small and Medium-Sized Firms*, 2023, 10.

Il presente elaborato, dunque, nell'ottica di perseguire lo scopo descritto nelle prime righe di questa introduzione, analizzerà la disciplina avente ad oggetto la tutela penale della proprietà intellettuale in Italia, con particolare riguardo alla sua potenziale applicazione ai gestori delle piattaforme digitali le quali, al verificarsi di determinate condizioni, possono essere ritenute penalmente responsabili, in quanto favoriscono gli utenti nella vendita e/o condivisione e/o distribuzione di materiale in violazione della normativa succitata. Si pensi al caso in cui un *marketplace online* consenta ai propri utenti di vendere prodotti contraffatti; data per certa la responsabilità penale diretta dell'utente, il dubbio è se in capo al gestore del *marketplace online* sia configurabile una responsabilità penale, e, in caso affermativo, che tipo di responsabilità. È a queste domande che la presente dissertazione si propone di trovare una risposta.

Nello specifico, il Capitolo I fornirà una descrizione generale del quadro normativo italiano con riferimento alla tutela penale della proprietà intellettuale: verranno, dunque, analizzate le norme a tutela di marchi, brevetti, disegni o modelli industriali, di segni distintivi registrati e non,[9] di indicazioni geografiche e denominazioni d'origine,[10] di segreti commerciali[11] e, infine, del diritto d'autore.[12] In particolare, tenendo conto dell'oggetto del presente lavoro, l'analisi tratterà in maniera più dettagliata tutte quelle fattispecie criminose in cui assumono rilevanza delle condotte che si prestano ad essere commesse anche dalle piattaforme digitali (oltre all'utente); saranno, dunque, oggetto di un'analisi più approfondita quei reati che puniscono le condotte di ««vendita», «distribuzione», «messa in circolazione», «diffusione» o «trasmissione» o «comunicazione al pubblico» di prodotti od opere dell'ingegno in violazione dei diritti di privativa spettanti ai rispettivi titolari.

Il Capitolo II darà, *in primis*, una definizione di piattaforma digitale, propedeutica alla disciplina che verrà analizzata nel corso dello stesso Capitolo e in quello successivo. Dopodiché si descriveranno dapprima gli interventi che il

[9]Cfr. art. 473 c.p. («Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni»); art. 474 c.p. («Introduzione nello Stato e commercio di prodotti con segni falsi»); art. 517 c.p. («Vendita di prodotti industriali con segni mendaci»); art. 517-*ter* c.p. («Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale»).
[10]Cfr. art. 517-*quater* c.p. («Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari»).
[11]Cfr. art. 623 c.p. («Rivelazione di segreti scientifici o industriali»).
[12]Cfr. artt. 171-171-*nonies* l. n. 633 del 1941.

legislatore comunitario, tramite fonti di *soft law* e Direttive, ha realizzato nell'ottica di adeguare la tutela della proprietà intellettuale alle minacce avanzate dall'Internet per poi passare in rassegna le normative di attuazione domestiche delle Direttive succitate. Ci si riferisce in particolare a due Memorandum – il Memorandum d'intesa sulla pubblicità online e i diritti di proprietà intellettuale e il Memorandum d'intesa sulla vendita di merci contraffatte su Internet – , e a due Direttive: la Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, recepita dal d.lgs. n. 68 del 2003, e la Direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale attuata dal d. lgs. n. 140 del 2006.

Infine, il Capitolo III analizzerà la disciplina, comunitaria e nazionale, avente ad oggetto la responsabilità non solo dei «prestatori di servizi della società dell'informazione» (c.d. "*Internet service providers*" o "ISP") ma di ogni piattaforma digitale, così come definita in premessa al Capitolo II. Nello specifico, verranno dapprima descritte le normative comunitarie – e, nello specifico, la Direttiva 2000/31/EC, la Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e il Regolamento EU 2022/2065 sui servizi digitali, che disciplinano le condizioni in presenza delle quali una piattaforma digitale può considerarsi responsabile –, per poi declinare la disciplina così introdotta in ambito nazionale, cercando di comprendere meglio che tipo di responsabilità penale e civile attribuire alla piattaforma *online*. In ambito penale, si analizzerà l'ipotesi di imputazione diretta della piattaforma per omesso impedimento dell'evento *ex* articolo 40, co. 2, c.p. o, in alternativa, una responsabilità per concorso omissivo nel reato commissivo dell'utente, secondo il combinato disposto degli articoli 110 e 40, co. 2 c.p.; in ambito civile, il dubbio ricadrà, invece, sull'ipotesi di attribuire alla piattaforma una responsabilità aquiliana *ex* articolo 2043 c.c., o alternativamente, una responsabilità contrattuale *ex* articolo 1218 c.c., con le relative conseguenze di disciplina che ne derivano. Si concluderà con dei cenni comparatistici, inerenti alla disciplina prevista dai principali ordinamenti di *common law*: Stati Uniti, Australia, Nuova Zelanda e Regno Unito.

CAPITOLO I

LA TUTELA PENALE DELLA PROPRIETÀ INTELLETTUALE: UN INQUADRAMENTO SISTEMATICO.

Premessa.

Il quadro regolatorio penalistico riferito alla materia degli *intangibles* può convenzionalmente distinguersi in ragione della classica bipartizione di cui si caratterizza la categoria della proprietà intellettuale: proprietà industriale e diritto d'autore.

Tale distinzione, in ambito, penalistico, ha avuto luogo solo recentemente: il legislatore del 2009, con la legge n. 99[1] ha infatti espunto dall'articolo 473 c.p. («Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni») qualsiasi riferimento alle opere protette dal diritto d'autore (le c.d. "opere dell'ingegno"), la cui protezione è oggi affidata agli articoli 171-174 *ter* della legge n. 633 del 1941,[2] nonostante qualche riferimento sia ancora presente all'articolo 517 c.p.

Al contempo, la proprietà industriale trova tutela nel codice penale, all'interno del «Titolo VII» riguardante i «Delitti contro la fede pubblica» - in particolare agli articoli 473, 474, i c.d. "delitti di falso", aventi ad oggetto marchi, segni distintivi registrati, brevetti, disegni e modelli industriali -, e al «Titolo VIII» in materia di «Delitti contro l'economia pubblica, l'industria e il commercio», dove gli articoli 517, 517-*ter*, 517-*quater* disciplinano rispettivamente «la vendita di prodotti industriali con segni mendaci», «la fabbricazione e il commercio di beni realizzati usurpando titoli di proprietà industriale» e «la contraffazione di indicazioni geografiche o denominazioni d'origine dei prodotti agroalimentari».

All'interno del «Titolo XII», sui «Delitti contro la persona», è contenuto poi l'articolo 623 il quale si occupa di disciplinare la fattispecie di rivelazione di segreti scientifici o commerciali, i c.d. "*trade secrets*".

La dissertazione, dunque, analizzerà dapprima la disciplina codicistica riferita quasi esclusivamente ai delitti contro la proprietà industriale (ad esempio

[1]L. n. 99 del 2009, «Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia», art. 15.
[2]L. n. 633 del 1941, «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio».

marchi, brevetti, segni distintivi diversi dal marchio registrato, modelli e disegni, denominazioni d'origine e *trade secrets*), per poi passare all'analisi della disciplina *extra-codicem* contenuta nella legge n. 633 del 1941 – già citata – riguardante la tutela penale della seconda ramificazione della categoria dei diritti di proprietà intellettuale: il diritto d'autore.

1. La tutela penale della proprietà industriale.

Come anticipato, all'interno della tutela penale della proprietà industriale, è possibile distinguere tra una tutela prevista per marchi, segni distintivi registrati, brevetti, disegni e modelli industriali *ex* articoli 473 e 474 c.p., e una tutela «mediata»[3] prevista dall'articolo 517 c.p. per i segni distintivi non registrati.

Poi, gli articoli 517-*ter* e 517-*quater* c.p. colpiscono rispettivamente i comportamenti c.d. "parassitari" ai danni dei titolari dei diritti di privativa industriale e di contraffazione o alterazione delle indicazioni geografiche o denominazioni d'origine dei prodotti agroalimentari. Infine, l'articolo 623 c.p. punisce la rivelazione di segreti scientifici o commerciali.

Per ragioni di ordine espositivo si procederà all'analisi, dapprima, delle tutele previste per i segni distintivi registrati nonché brevetti, disegni e modelli industriali e del loro corretto sfruttamento economico (articoli 473, 474, 517-*ter* c.p.), per poi procedere all'analisi della tutela dei segni distintivi non registrati (articolo 517 c.p.) e accennando alla questione dei c.d. "nomi a dominio". Infine, si approfondiranno le disposizioni aventi ad oggetto la tutela delle indicazioni geografiche o denominazioni d'origine dei prodotti agroalimentari (articolo 517-*quater*) e dei segreti commerciali (articolo 623 c.p.).

1.1. La tutela dei segni distintivi registrati e dei brevetti, disegni e modelli industriali: gli articoli 473, 474 e 517-*ter* c.p.

Come anticipato, tra le fattispecie criminose poste a tutela della proprietà industriale rilevano, innanzitutto, gli articoli 473 («Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni»)[4] e 474

[3]Cfr. RIVERDITI, *La tutela penalistica della proprietà intellettuale*, in *Dir. ed ec. dell'impresa*, 2016, 1, 73.

[4]Art. 473 c.p.: «Chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque,

(«Introduzione nello Stato e commercio di prodotti con segni falsi»)[5] c.p., collocati, per via della legge 99/2009, all'interno del titolo VII, Capo II, dedicato ai delitti di falso: tale scelta è stata fortemente criticata, in quanto dibattuto risulta essere il bene giuridico protetto.[6]

Il problema dell'individuazione del bene giuridico tutelato dalla norma in esame non è da sottovalutare, in quanto ha rilevanza sia da un punto di vista sostanziale che processuale: dal punto di vista sostanziale, infatti, non va dimenticato che la Corte costituzionale ha definito il bene giuridico come un fondamentale canone ermeneutico che impone al giudice di espellere dalla norma incriminatrice tutti quei fatti che, nonostante possano essere ricondotti entro la cornice dei possibili significati letterali, sono in concreto inoffensivi del bene giuridico tutelato.[7] Ulteriore conseguenza sostanziale di tale impostazione è la differente individuazione della persona offesa dal reato. Ciò avrebbe delle ricadute

---

senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.500 a euro 25.000. Soggiace alla pena della reclusione da uno a quattro anni e della multa da euro 3.500 a euro 35.000 chiunque contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati. I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale».

[5]Art. 474 c.p.: «Fuori dei casi di concorso [110] nei reati previsti dall'articolo 473, chiunque introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati è punito con la reclusione da uno a quattro anni e con la multa da euro 3.500 a euro 35.000. Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello Stato, chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti di cui al primo comma è punito con la reclusione fino a due anni e con la multa fin a euro 20.000. I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale».

[6]Cfr. RIVERDITI, *La tutela penalistica*, cit., 70; GATTA, *La disciplina della contraffazione del marchio d'impresa nel codice penale (artt. 473 e 474): tutela del consumatore e/o del produttore?*, in *Dir. pen. cont.*, 2012, 2 s.

[7]Corte cost., 7 luglio 2005, n. 265: «Questa Corte ha già avuto modo di precisare che il principio di offensività opera su due piani, rispettivamente della previsione normativa, sotto forma di precetto rivolto al legislatore di prevedere fattispecie che esprimano in astratto un contenuto lesivo, o comunque la messa in pericolo, di un bene o interesse oggetto della tutela penale («offensività in astratto»), e dell'applicazione giurisprudenziale («offensività in concreto»), quale criterio interpretativo-applicativo affidato al giudice, tenuto ad accertare che il fatto di reato abbia effettivamente leso o messo in pericolo il bene o l'interesse tutelato (v. sentenze numeri 360 del 1995, 263 e 519 del 2000, ove viene appunto definita la duplice sfera di operatività, in astratto e in concreto, del principio di necessaria offensività, quale criterio di conformazione legislativa delle fattispecie incriminatrici e quale canone interpretativo per il giudice)».

non di certo irrilevanti anche dal punto di vista processuale, considerati i diritti e prerogative riconosciute alla persona offesa del reato.[8]

Per tale motivo è opportuno descrivere brevemente gli orientamenti contrapposti in dottrina e giurisprudenza con riferimento al tema del bene giuridico tutelato dagli articoli 473 e 474 c.p. con le relative conseguenze sostanziali che ne derivano, con particolare riferimento alla persona offesa dal reato e al connesso caso del c.d. del falso grossolano.

In seguito, si procederà ad analizzare le condotte incriminate dagli articoli 473 e 474 c.p., per poi chiudere il paragrafo con l'analisi della fattispecie di cui all'articolo 517-*ter* c.p.

1.1.1. Il bene giuridico «fede pubblica».

Il primo degli orientamenti in analisi ravvisa nella «fede pubblica» il bene giuridico tutelato dalle norme a protezione della proprietà industriale.

Ciò in quanto, come anticipato, secondo l'impostazione codicistica, gli articoli 473 e 474 c.p. rientrano tra i delitti di falso, i quali, essendo inseriti all'interno del Titolo VII, ledono il bene giuridico «fede pubblica», intesa come interesse dei consociati alla certezza dei rapporti giuridici. Dunque, la tutela apprestata dal Capo II del Titolo VII del Codice penale potrebbe essere declinata nella fiducia che i consumatori ripongono nei mezzi simbolici di pubblico riconoscimento che contraddistinguono i prodotti o servizi industriali, come ad esempio il marchio.

Di conseguenza, il bene giuridico tutelato dalle norme succitate, poste a tutela della proprietà industriale, sembra potersi inquadrare nell'interesse collettivo

[8]Art. 408 c.p.p.: «1. Entro i termini previsti dagli articoli precedenti, il pubblico ministero, se la notizia di reato è infondata, presenta al giudice richiesta di archiviazione. Con la richiesta è trasmesso il fascicolo contenente la notizia di reato, la documentazione relativa alle indagini espletate e i verbali degli atti compiuti davanti al giudice per le indagini preliminari. 2. L'avviso della richiesta è notificato, a cura del pubblico ministero, alla persona offesa che, nella notizia di reato o successivamente alla sua presentazione, abbia dichiarato di volere essere informata circa l'eventuale archiviazione. 3. Nell'avviso è precisato che, nel termine di venti giorni, la persona offesa può prendere visione degli atti e presentare opposizione con richiesta motivata di prosecuzione delle indagini preliminari. 3-bis. Per i delitti commessi con violenza alla persona e per il reato di cui all'articolo 624-bis del codice penale, l'avviso della richiesta di archiviazione è in ogni caso notificato, a cura del pubblico ministero, alla persona offesa ed il termine di cui al comma 3 è elevato a trenta giorni».

dei consumatori alla conoscenza della fonte di provenienza dei prodotti e/o servizi venduti sul mercato.

Sulla base di questi presupposti la Suprema Corte ha affermato «il principio per il quale l'interesse giuridico tutelato dalla norma dell'art. 473 c.p., (in piena coincidenza con quello dell'art. 474 c.p.) è la 'pubblica fede' in senso oggettivo, intesa come affidamento dei cittadini nei marchi o segni distintivi che individuano le opere dell'ingegno o i prodotti industriali e ne garantiscono la circolazione, e non l'affidamento del singolo, sicché non è necessario per integrare il reato che sia realizzata una situazione tale da indurre il cliente in errore sulla genuinità del prodotto. Al contrario, il reato può sussistere - se la contraffazione sia oggettivamente realizzata - (come pacifico nella specie) anche se il compratore è stato messo a conoscenza dallo stesso venditore della non autenticità del marchio (Cassazione penale, sez. 5^, 05/11/2001, n. 1195)».[9]

Le conseguenze sostanziali che derivano da tale interpretazione sono diverse.

Dal punto di vista sostanziale se il bene giuridico tutelato è la «fede pubblica» ne consegue, innanzitutto che la persona offesa sarebbe da individuarsi nel pubblico dei consumatori – e relative associazioni di categoria – con esclusione dei titolari dei diritti di proprietà industriale contraffatti o alterati ad agire tanto in sede penalistica quanto in sede civilistica per ottenere, *inter alia*, un risarcimento del danno.[10] Tale conseguenza porta con sé un'ulteriore risultato: se la persona offesa dal reato s'individua nel pubblico dei consumatori, e non nei titolari dei diritti di privativa, la fattispecie di «falso grossolano» non è penalmente rilevante: tale fattispecie si verifica ogni qualvolta i segni mendaci, apposti sul prodotto, non siano idonei a trarre in inganno i consumatori,[11] con la conseguenza che la condotta dell'agente non sarebbe soggetta alla sanzione penale.

[9]Cfr. Cass. pen., Sez. II, 16 luglio 2012, n. 28423.
[10]Cfr. PISANI, *I reati contro la fede pubblica*. In: (a cura di): ANTONIO FIORELLA, *Questioni fondamentali della parte speciale del diritto penale* Torino, 2012, 510 ss.
[11]Cass. pen., Sez. unite, 18 dicembre 2007, n. 46982: «In estrema sintesi, può qualificarsi come falso grossolano il falso inoffensivo rispetto al bene 'fede pubblica', proprio per l'inidoneità dello stesso a trarre in inganno la collettività; inidoneità che, derivando dalle modalità della falsificazione - prevalentemente di natura materiale - comporta una valutazione giudiziale in punto di fatto.» Nello stesso senso anche Cass. pen., Sez. II, 5 febbraio 2014, n. 5687 e Cass. pen., Sez. VI, 29 aprile 2015, n. 18015.

1.1.2. I soli diritti di esclusiva del titolare dei diritti di privativa come bene giuridico tutelato.

Una soluzione diversa è proposta da dottrina minoritaria, la quale ipotizza che il bene giuridico tutelato dalle norme in esame siano i soli diritti di esclusiva in capo al titolare dei diritti di privativa.[12]

Tale tesi poggia essenzialmente su due argomenti. Da un lato, viene sostenuto che la riforma del 1992[13] svilisce la funzione identificativa del marchio, in quanto ne consente la libera cessione indipendentemente dalla cessione dell'azienda produttrice: se dunque l'orientamento tradizionale, che ravvisa nella «fede pubblica» il bene giuridico tutelato, si fonda sulla protezione della funzione identificativa del marchio («affidamento dei cittadini nei marchi o segni distintivi che individuano le opere dell'ingegno o i prodotti industriali e ne garantiscono la circolazione»),[14] allora viene da sé che, venuta meno la funzione identificativa del marchio, viene meno anche la base su cui l'orientamento anzidetto forma il suo convincimento; dall'altro lato, si osserva come la riforma degli articoli 473-474 c.p. sia stata introdotta con l'articolo 15 della legge n. 99 del 2009 rubricato «tutela penale dei diritti di proprietà industriale».

Tale interpretazione porterebbe a conseguenze diametralmente opposte a quelle viste nel sottoparagrafo precedente: nel caso in cui ad essere «persona offesa dal reato», non siano i consumatori, ma i soli titolari dei diritti di privativa, la condotta di contraffazione del *reo* assumerebbe rilevanza penale anche nel caso del falso grossolano. [15]

1.1.3. Le fattispecie di cui agli articoli 473 e 474 come reati plurioffensivi.

A cavallo tra queste due soluzioni interpretative, diametralmente opposte, vi è una terza posizione intermedia, avallata dalla giurisprudenza di legittimità più recente,[16] secondo la quale le fattispecie criminose in esame avrebbero un carattere

[12]Cfr. MANCA, *La tutela penale della proprietà industriale e della struttura produttiva italiana. Prospettive e ripercussioni della legge 23 luglio 2009, n. 99*, Padova, 2009.
[13]D. lgs. n. 480 del 1992, «Attuazione della direttiva n. 89/104/CEE del Consiglio del 21 dicembre 1988, recante ravvicinamento delle legislazioni degli Stati membri in materia di marchi di impresa.»
[14]Cfr. Cass. pen., cit., 28423/2012.
[15]*Contra* v. GATTA, *La disciplina della contraffazione*, cit., 5.
[16]Cass. Pen., Sez. II, 2 ottobre 2019, n. 40324: «Va ulteriormente specificato che 'il reato di cui all'art. 473 c.p., ha natura di reato plurioffensivo, destinato a tutelare non solo quel particolare bene

«plurioffensivo» tutelando, allo stesso tempo, sia il pubblico dei consumatori, sia i titolari dei diritti di privativa industriale.

Infatti, è certamente vero che la falsificazione di marchi o altri segni distintivi lede la fiducia del pubblico dei consumatori, allo stesso tempo, tuttavia, è innegabile che anche gli interessi dei titolari dei diritti di privativa risultano compromessi.

1.1.4. Le condotte penalmente rilevanti degli articoli 473 e 474 c.p.

Passando all'analisi delle condotte penalmente rilevanti, la fattispecie di cui all'articolo 473 c.p. non punisce ogni uso distorto dei segni distintivi (comma 1) – o dei brevetti, disegni o modelli industriali (comma 2) –, ma la sola «contraffazione» e «alterazione» degli stessi,[17] esulano, dunque, dall'ambito di rilevanza penale, tutte quelle fattispecie che non ricadono nelle condotte di «contraffazione» o «alterazione», pur comunque rientrando nella fattispecie civilistica della concorrenza sleale disciplinata dall'articolo 2598 c.c.

Risulta dunque rilevante capire in cosa consistano le condotte di «contraffazione» e «alterazione», in quanto, in assenza di queste, qualsiasi condotta, seppur illecita dal punto di vista civilistico, non assume rilevanza in ambito penale.

La contraffazione consiste «nel dare al prodotto quella forma e quei colori particolari che possono indurre il pubblico a identificarlo come proveniente da una certa impresa, anche contro le eventuali indicazioni dei marchi con i quali venga contrassegnato. Ciò che rileva ai fini della contraffazione, infatti, è la funzione rappresentativa del modello, non il diritto di esclusiva del titolare del brevetto. Ed è evidente che la funzione rappresentativa del modello, vale a dire la sua idoneità a individuare una certa provenienza del prodotto, può risultare attenuata, ma non esclusa, quando l'autore della contraffazione adoperi legittimamente anche un suo marchio di fabbrica».[18]

---

giuridico, di natura immateriale e collettiva, rappresentato dalla pubblica fede, ma anche altri beni meritevoli di protezione, quali le privative sui marchi registrati, l'interesse alla regolarità del commercio e dell'industria e, più in generale, l'economia nazionale, secondo una condivisibile tendenza volta ad assicurare effettività ai principi costituzionali in materia di iniziativa economica e di proprietà privata' (Sez. 5, Sentenza n. 18289 del 27/01/2016, Volponi, Rv. 267119; sulla portata plurioffensiva dei reati contro la fede pubblica in generale, cfr. Sezioni Unite, Sentenza n. 46982 del 25/10/2007, Pasquini, Rv. 237855).»

[17]Cfr. RIVERDITI, *La tutela penalistica*, cit., 72.

[18]Cfr. Cass. pen., Sez. V, 28 luglio 2017, n. 37957.

La giurisprudenza offre un contributo anche con riferimento alla «alterazione» di marchi, affermando «l'alterazione di marchi prevista dall'art. 473, comprende anche la riproduzione solo parziale del marchio, idonea a far sì che esso si confonda con l'originale e da verificarsi mediante un esame sintetico - e non analitico - dei marchi in comparazione, che tenga conto dell'impressione di insieme e della specifica categoria di utenti o consumatori cui il prodotto è destinato, soprattutto se si tratta di un marchio celebre (Fattispecie relativa al sequestro di magliette di note squadre di calcio recanti marchi contraffatti). (Sez. 5, n. 33900 del 08/05/2018 - dep. 19/07/2018, P.M. in proc. Cortese, Rv. 27389301)».[19]

Sembra dunque potersi concludere, che la giurisprudenza, con il termine «contraffazione», intenda un'imitazione anche solo parziale degli elementi del marchio in tutta la sua portata emblematica e denominativa, mentre per «alterazione» intenda un'imitazione fraudolenta o falsificazione parziale in modo che il prodotto alterato possa confondersi con quello originario.[20] Bisogna ancora sottolineare che, a ben leggere l'articolo 473 c.p., la «contraffazione» o «alterazione» degli *intagibles* è solo uno degli elementi della fattispecie: infatti la rilevanza penale della condotta è subordinata a due ulteriori presupposti, uno attinente alla conformità degli *intangibles* con le norme domestiche e internazionali e l'altra riferita all'elemento soggettivo del c.d. "falsificatore".

Sotto il primo profilo, infatti l'articolo 473 c.p., al comma 3, richiede «che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale». Dunque, qualora i segni distintivi o brevetti, disegni o modelli industriali non rispettino questo limite formale, la tutela in esame rimane preclusa ai loro titolari.[21]

[19]Cfr. Cass. Pen. Sez. II, 1 giugno 2020, n.16568.

[20]La contraffazione «presuppone la riproduzione integrale in tutta la sua configurazione emblematica e denominativa, di un marchio o di un segno distintivo».
Per alterazione «si intende la riproduzione solo parziale ma tale da potersi confondere col marchio originario o col segno distintivo», essendo «sufficiente la riproduzione del marchio 'nei suoi elementi essenziali' e tale valutazione deve essere condotta sulla base di un esame, non analitico, ma sintetico che tenga conto dell'impressione d'insieme e della specifica categoria cui il prodotto è destinato». Così, Cass. pen., Sez. V, 19 luglio 2018, n. 33900.

[21]È stato affermato come l'art. 473 c.p. tuteli il marchio o segno distintivo sol che esso sia stato depositato, registrato o brevettato nelle forme di legge e soltanto all'esito positivo della procedura amministrativa ritualmente avviata. Cfr. Cass. pen., Sez. V, 26 giugno 2012 n. 25273.

Ci si riferisce, in particolare, alle formalità previste dal c.p.i.[22] nonché dalle normative comunitarie e internazionali: (I) per ciò che riguarda la normativa comunitaria ci si riferisce, tra gli altri, alla Direttiva (UE) 2015/2436 sul ravvicinamento delle legislazioni degli Stati membri in materia di marchi d'impresa;[23] alla direttiva 2004/48/CE, conosciuta anche come IPRED («*Intellectual property rights enforcement directive*») sui meccanismi di implementazione dei diritti esclusivi e sugli strumenti giuridici azionabili dai loro titolari; [24] il Regolamento (UE) 2017/1001 sul marchio dell'Unione europea;[25] (II) per ciò che concerne le fonti extracomunitarie, tra i trattati internazionali promossi dall'Organizzazione Mondiale della Proprietà Intellettuale (OMPI-WIPO),[26] ci si riferisce al protocollo di Madrid, firmato nel 1891[27] che disciplina una procedura semplificata per il riconoscimento del marchio internazionale valevole come nel Paese d'origine in tutti gli Stati aderenti presso i quali il richiedente avanzi domanda; la Convenzione di Parigi per la protezione della proprietà industriale, firmata nel 1883,[28] che stabilisce misure di reciprocità tra gli Stati nell'uso dei diritti di proprietà industriale; ed infine, l'*Agreement on Trade Related Aspects of*

[22]Con riferimento ai marchi si vedano gli artt. 12, 13, 14 c.p.i; riguardo alle invenzioni si vedano gli artt. 46, 48, 49, 50, 51 c.p.i.

[23]Direttiva (UE) 2015/2436 del Parlamento Europeo e del Consiglio del 16 dicembre 2015 sul ravvicinamento delle legislazioni degli Stati membri in materia di marchi d'impresa.

[24]Direttiva 2004/48/CE del Parlamento Europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale.

[25]Regolamento (UE) 2017/1001 del Parlamento Europeo e del Consiglio del 14 giugno 2017 sul marchio dell'Unione europea.

[26]La *World Intellectual Property Organization* (in italiano Organizzazione Mondiale per la Proprietà Intellettuale [OMPI]) è una delle agenzie specializzate delle Nazioni Unite, creata nel 1967 con la finalità di incoraggiare l'attività creativa e promuovere la protezione della proprietà intellettuale nel mondo.

[27]Il protocollo di Madrid concernente la registrazione internazionale dei marchi è un trattato amministrato dall'Ufficio internazionale dell'Organizzazione mondiale della proprietà intellettuale (OMPI), con sede a Ginevra. In vigore dall'aprile 1996, il protocollo è stato sottoscritto da molti paesi di tutto il mondo, tra cui la maggior parte degli Stati europei, gli Stati Uniti, il Giappone, l'Australia, la Cina, la Russia, nonché, nell'ottobre 2004, l'Unione europea in quanto tale. Il protocollo di Madrid dà ai titolari di marchi la possibilità di estendere la protezione degli stessi in molti paesi grazie al semplice deposito di una domanda direttamente presso l'ufficio nazionale o regionale competente in materia di marchi. Per approfondimenti si veda *https://euipo.europa.eu/ohimportal/it/madrid-protocol#:~:text=Il%20protocollo%20di%20Madrid%20d%C3%A0,competente%20in%20materia%20di%20marchi*.

[28]Convenzione di Parigi per la protezione della proprietà industriale del 20 marzo 1883. Riveduta a Bruxelles il 14 dicembre 1900, a Washington il 2 giugno 1911, all'Aja il 6 novembre 1925, a Londra il 2 giugno 1934, a Lisbona il 31 ottobre 1958 e a Stoccolma il 14 luglio 1967 e modificata il 2 ottobre 1979.

Intellectual Property Rights («TRIPS»),[29] adottato a Marrakech il 15 aprile 1994 che disciplina gli standard minimi necessari per il rispetto della proprietà intellettuale a livello mondiale.

Sotto il profilo dell'elemento soggettivo, poi, si richiede che l'agente possa conoscere dell'esistenza del titolo di privativa industriale altrui («potendo conoscere dell'esistenza del titolo di proprietà industriale»). Si tratta di un elemento di difficile collocazione dogmatica: «da un lato, infatti, parrebbe operare sul terreno soggettivo, richiedendo che l'autore del reato, oltre ad essere in dolo rispetto alla falsificazione, sia anche quantomeno in colpa circa l'esistenza dei presupposti di tutela dell'oggetto materiale della condotta; d'altro canto, anche in considerazione dell'anomalia di un simile 'arricchimento' dell'elemento soggettivo (che oltretutto degrada a 'parzialmente colposo' un delitto comunque punito come doloso), si potrebbe ritenere che in tal modo il legislatore abbia (più o meno consapevolmente) inteso circoscrivere la rilevanza penale del falso alle sole ipotesi in cui il marchio e gli altri segni distintivi abbiano già ottenuto tutela sul terreno 'sostanziale-civilistico', escludendo la configurabilità del reato nel caso di mero deposito della domanda o della richiesta di registrazione».[30]

Questa seconda interpretazione, sembrerebbe essere coerente con il principio di *extrema-ratio* dell'azione penale: qualora il marchio e gli altri segni distintivi non abbiano già ottenuto una tutela sul piano civilistico, perché non ancora registrati, allora *a fortiori* non potrebbero ottenerla sul piano penalistico– salva ovviamente l'applicazione della tutela civilistica e penalistica attenuata per i segni distintivi non registrati, ai sensi, rispettivamente dell'articolo 2571 c.c. [31] e dell'articolo 517 c.p. (che verrà esaminato nel paragrafo 1.2).

---

[29] AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS.

[30] Cfr. RIVERDITI, *La tutela penalistica*, cit., 72. Tale interpretazione sembra essere coerente con quanto affermato dalla Suprema Corte. Cfr. Cass. pen., cit., 25273/2012: «Tuttavia deve osservarsi, conformemente anche alla dottrina che ha commentato la innovazione apportata alla materia de qua con l. 23 luglio 2009 n. 99 (che con l'art. 15 comma 1 lett. a) ha 'riscritto' l'art. 473 c.p.), che l'inciso inserito nel nuovo testo dell'art. 473 comma 1 c.p. 'potendo conoscere dell'esistenza del titolo di proprietà industriale' lascia fondatamente pensare che, con la detta riforma, si è inteso ratificare la giurisprudenza che richiedeva per la tutela penale, la avvenuta registrazione del marchio o del segno, non bastando la semplice domanda: si può conoscere, infatti, solo un titolo già rilasciato mentre la semplice richiesta dello stesso non dà luogo, di per sé, alla garanzia dell'esito positivo della procedura amministrativa avviata».

[31] Art. 2571 c.c.: «Chi ha fatto uso di un marchio non registrato alla facoltà di continuare ad usarne, nonostante la registrazione da altri ottenuta, nei limiti in cui anteriormente se ne è avvalso».

Per concludere l'analisi dell'articolo 473 c.p. non si può fare a meno di evidenziare come, al fine di incrementare la tutela contro la persona offesa dal reato – la cui individuazione, come si è detto, varia a seconda di quale sia il bene giuridico tutelato considerato – la fattispecie punisca anche chiunque senza essere concorso nella contraffazione o alterazione, fa «uso» di tali «marchi o segni contraffatti o alterati» o «brevetti, disegni o modelli contraffatti o alterati».

Dunque, oltre al falsificatore, il legislatore, considera responsabile anche colui che «usa» gli *intangibles* contraffatti o alterati. La condotta di «uso» di marchi e segni distintivi, punita penalmente – in alternativa alla contraffazione o alterazione –, deve identificarsi con l'attività diretta a determinare un collegamento tra il marchio contraffatto e un certo prodotto, non con la semplice detenzione.[32]

Passando all'analisi dell'articolo 474 c.p., questo punisce, sia chiunque, non avendo concorso alla falsificazione, introduca nel territorio dello Stato prodotti con segni falsi (comma 1), sia chi li detenga per la vendita, li ponga in vendita o li metta altrimenti in circolazione (comma 2) al fine di trarne profitto - elemento soggettivo, quest'ultimo, il dolo specifico, richiesto per entrambe le fattispecie previste dai 2 commi.

Relativamente alle condotte previste dal comma 2, la detenzione per vendere si realizza ogni qualvolta l'agente possieda la merce contraffatta con l'intenzione di venderla; segnatamente, la messa in vendita si ritiene integrata con

[32]«Secondo la condivisibile giurisprudenza di questa Corte, infatti, l'uso di marchi e segni distintivi punito da detta disposizione (condotta prevista dalla norma in discorso in alternativa alla contraffazione o alterazione) deve identificarsi con l'attività diretta a determinare un collegamento tra il marchio contraffatto e un certo prodotto (Sez. 5, n. 26398 del 05/04/2019, De Gregorio; Rv. 276893; Sez. 2, n. 26263 del 22/06/2010, Portarapillo, Rv. 247684; Sez. 5, n. 4305 del 02/04/1996, Vollero, Rv. 204837, sentenze intervenute sul tema del distinguo tra i reati di cui agli artt. 473 e 474 c.p.); tale uso si sostanzia nell'attività squisitamente ma unicamente funzionale a determinare detto collegamento, tale non potendo ritenersi il mero trasporto di uno zaino contenente i marchi incorporati negli accessori, attività obiettivamente neutra rispetto alla strumentalizzazione dei medesimi per contrassegnare falsamente dei prodotti non autentici». Così, Cass. pen., Sez. V, 3 settembre 2020, n. 25036. Inoltre, «ai fini della distinzione tra le fattispecie di cui agli art. 473 e 474 c.p., l'uso di marchi e segni distintivi punito dalla prima norma, essendo inteso a determinare un collegamento tra il marchio contraffatto e un certo prodotto, precede l'immissione in circolazione dell'oggetto falsamente contrassegnato e, comunque, se ne distingue. L'uso punito dall'art. 474 c.p., invece, è direttamente connesso con l'immissione in circolazione del prodotto falsamente contrassegnato, in quanto presuppone già realizzato il collegamento tra contrassegno e prodotto o, più specificamente, già apposto il contrassegno su un determinato oggetto. Nel primo reato, la condotta ha per oggetto materiale il contrassegno, nel secondo il prodotto contrassegnato. (Fattispecie nella quale è stato ritenuto correttamente applicato l'art. 473 c.p., essendo stato contraffatto il marchio 'Panasonic', applicato a simulacri lignei di videocamere e videoregistratori, confezionati per l'offerta in vendita)». Così, massima a Cass. pen., Sez. V, 24 aprile 1996, n. 4305.

la mera giacenza della merce nei luoghi usualmente destinati al commercio, senza necessità che vi sia alcuna offerta o esposizione al pubblico; infine, la condotta di mettere altrimenti in circolazione consiste nella possibilità di ricavare qualsiasi utilità dalla diffusione – intesa quale azione che possa conferire rilevanza penale agli atti diversi dalla vendita – dei prodotti con segni mendaci.[33]

Anche in questo caso è richiesto lo stesso requisito riguardante la conformità dei segni distintivi con le norme domestiche e internazionali (comma 3).[34]

Per concludere l'analisi delle due fattispecie, si evidenzia che l'orientamento maggioritario di giurisprudenza e dottrina è nel senso di annoverare i delitti di cui agli articoli 473-474 c.p. all'interno della categoria dei delitti c.d. "di pericolo", contrapposti ai reati c.d. "di danno o lesione":[35] cioè reati « per la cui integrazione è sufficiente anche la sola attitudine della falsificazione ad ingenerare confusione, con riferimento non solo al momento dell'acquisto, ma anche a quello della successiva utilizzazione del prodotto contraddistinto dal marchio contraffatto (Cass. 1.7.2009, n. 40170)».[36]

1.1.5. Le condotte «parassitarie» penalmente rilevanti: l'articolo 517-*ter*.

Salvi i casi appena esaminati, definiti «delitti di falso», attinenti alla «contraffazione» e «alterazione» dei marchi, segni distintivi registrati, brevetti, disegni e modelli industriali (ex artt. 473-474 c.p.), l'articolo 517-*ter*,[37] come

[33]Per un approfondimento v. CINGARI, *Misure punitive per il rilancio della competitività: tra repressione dell'incauto acquisto di prodotti «taroccati» e tutela del made in Italy*, in *Dir. Pen. e proc*., 2005, 11, 1342 s.

[34]Art. 474 co. 3 c.p.: «I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale».

[35]In diritto penale vengono infatti configurati i reati di danno (o di lesione), con cui il legislatore reprime fatti che compromettono l'integrità dei beni; e reati di pericolo, con cui il legislatore anticipa la tutela: reprime fatti che minacciano l'esistenza o il godimento del bene. Cfr. MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale: parte generale*, 9ª ed., Milano, 2020, 261 s.

[36]Cfr. Trib. Napoli, Sez. Proprietà Industriale e Intellettuale, 14 gennaio 2013, n. 539.

[37]Art. 517-*ter* c.p.: «Salva l'applicazione degli articoli 473 e 474 chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso è punito, a querela della persona offesa, con la reclusione fino a due anni e con la multa fino a euro 20.000. Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al primo comma. Si applicano le disposizioni di cui agli articoli 474 bis, 474 ter, secondo comma, e 517 bis, secondo comma. I delitti previsti dai commi primo e secondo sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale».

anticipato, anziché punire i «falsificatori», punisce i c.d. "parassiti", cioè sia coloro che «potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica[no] o adopera[no] industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso», sia coloro che «al fine di trarne profitto, introduc[ono] nel territorio dello Stato, det[engono] per la vendita, pon[gono] in vendita con offerta diretta ai consumatori o mett[ono] comunque in circolazione i beni» realizzati usurpando o violando i diritti di privativa industriale.

La portata di tale fattispecie sembra essere molto più ampia di quella prevista dagli articoli 473 e 474 c.p., in quanto la condotta parassitaria *ex* articolo 517-*ter* c.p. riguarda l'intera categoria dei titoli di proprietà industriale, che, *ex* articolo 1 del Codice della Proprietà Industriale (c.p.i.), comprende non solo marchi, segni distintivi registrati, brevetti, disegni e modelli industriali, ma anche «indicazioni geografiche, denominazioni di origine, modelli di utilità, topografie dei prodotti a semiconduttori, informazioni aziendali riservate e nuove varietà vegetali».[38]

L'articolo 517-*ter* punisce due condotte: l'usurpazione e la violazione del diritto industriale altrui.

«Usurpa» chi, pur non avendone titolo, realizza il bene oggetto del diritto di privativa; «viola» il diritto industriale altrui chi non rispetta le norme relative all'esistenza, all'ambito e all'esercizio dei diritti di proprietà industriale di cui al capo II del c.p.i.[39]

Anche con riferimento a tale fattispecie criminosa è richiesto lo stesso requisito riguardante la conformità dei segni distintivi con le norme domestiche e internazionali (comma 3).

[38]Art. 1 c.p.i.: «Ai fini del presente codice, l'espressione proprietà industriale comprende marchi ed altri segni distintivi, indicazioni geografiche, denominazioni di origine, disegni e modelli, invenzioni, modelli di utilità, topografie dei prodotti a semiconduttori, segreti commerciali e nuove varietà vegetali».
[39]Cfr. RIVERDITI, *La tutela penalistica*, cit., 75.

1.2. La tutela penale «attenuata» dei segni distintivi non registrati: l'articolo 517 c.p.

A differenza delle fattispecie appena analizzate, che puniscono condotte aventi ad oggetto diritti di privativa registrati – come si evince dal comma 3 di tutte e tre le norme su esaminate –, l'articolo 517 c.p.[40] punisce, con sanzioni assai più tenui, condotte aventi ad oggetto i diritti di proprietà intellettuale, compreso il diritto d'autore, non registrati, e in particolare chi «pone in vendita o mette altrimenti in circolazione» prodotti industriali con segni mendaci, cioè «opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto».

Dunque, affinché le condotte di mendacio siano rilevanti dal punto di vista penalistico è necessario che (I) i segni falsificati siano utilizzati per contraddistinguere prodotti industriali oppure opere dell'ingegno (essendo la mera falsificazione del segno penalmente irrilevante, a differenza dell'articolo 473 c.p.);[41] (II) tali beni siano messi in vendita o «altrimenti in circolazione»; (III) la falsificazione sia idonea ad indurre in inganno[42] il compratore su origine, provenienza o qualità dell'opera o prodotto.

Da questa premessa è possibile notare come il legislatore penale, al pari di quello civile,[43] come conseguenza del mancato rispetto degli oneri di registrazione previsti dalla legge, disponga una tutela attenuata, in cui la fattispecie di «falsificazione»[44] assume rilevanza solo con la compresenza degli altri requisiti

---

[40]Art. 517 c.p.: «Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri [2563-2574], atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a due anni e con la multa fino a euro 20.000».

[41]Cfr. RIVERDITI, *La tutela penalistica*, cit., 73.

[42]«Il prodotto deve quindi essere idoneo a generare equivocità a riguardo dell'origine, provenienza o qualità. Si ricordi che la norma non richiede il compimento di atti fraudolenti o dissimulatori, ma solamente quindi un'attitudine ingannatoria, risultando sufficiente anche un'imitazione generica del prodotto, la quale deve essere valutata in riferimento al cosiddetto consumatore medio, che tendenzialmente, effettuando acquisiti con celerità, non presta troppa attenzione alle caratteristiche dei prodotti». Così: *https://www.brocardi.it/codice-penale/libro-secondo/titolo-viii/capo-ii/art517.html?q=517+cp&area=codici*

[43]Per le differenze di tutela, sul piano civilistico, tra segni distintivi registrati e non, si veda CAMPOBASSO, *Diritto commerciale 1: diritto dell'impresa*, 7ª ed, Milano, 2017, 188 s.

[44]La falsificazione può essere sia materiale, realizzandosi in forma di contraffazione o alterazione, sia ideologica, se si mente riguardo a specifiche caratteristiche del prodotto. Così, RIVERDITI, *La tutela penalistica*, cit., 73.

succitati: in particolare, essa rileva solo qualora la presentazione complessiva del prodotto sia dotato della summenzionata idoneità ingannatoria. Da tale struttura dell'articolo 517 c.p. deriva la sua qualificabilità come reato di pericolo, in quanto la punibilità non è connessa né all'errore del compratore circa l'origine, provenienza o qualità dell'opera o del prodotto né tantomeno al danno che questi possa subire, ma alla sola idoneità– da accertarsi in concreto– del prodotto con segni mendaci a determinare l'inganno, e dunque l'errore, sull'origine, provenienza o qualità dell'opera o del prodotto.[45]

Inoltre, è bene sottolineare come, coerentemente con l'intento di offrire una tutela meno ampia al detentore dei diritti di privativa che non si sia curato di adempiere agli oneri legislativi, ad essere prese in considerazione sono solo le condotte di falsificazione realizzate sui beni «posti in vendita o altrimenti messe in circolazione»[46], con esclusione, sembrerebbe, di qualsiasi ipotesi di detenzione.[47]

La giurisprudenza ha ampliato la portata della norma in esame, estendendo la tutela anche agli oggetti di design industriale[48] nonostante le resistenze avanzate dalla dottrina.[49] La Suprema Corte ha precisato che sono «oggetti di *design*» quei

[45]Cfr. RIVERDITI, *La tutela penalistica*, cit., 73.

[46]«Vengono alternativamente considerate le condotte di messa in vendita, ovvero di offerta di un bene a titolo oneroso, e di messa in commercio, la quale può essere anche a titolo gratuito. Vi rientrano dunque l'esposizione della merce, l'offerta nei listini, la detenzione in magazzino ai fini della vendita». Si veda: *https://www.brocardi.it/codice-penale/libro-secondo/titolo-viii/capo-ii/art517.html?q=517+cp&area=codici*

[47]Ciò sembrerebbe confermato dal fatto che la norma fa espresso richiamo alla figura del «compratore» ai fini della rilevanza penale della fattispecie.

[48]Cass. pen., Sez. III, 21 febbraio 2011, n. 6254: «deve osservarsi che la decisione impugnata appare immune da censure anche per quanto riguarda l'applicabilità, nella fattispecie, dell'art. 517 c.p., contestata da entrambi i ricorrenti. Va preliminarmente osservato, a tale proposito, che la giurisprudenza di questa Corte ha da tempo definito l'ambito di operatività della disposizione penale richiamata. In particolare, si è avuto modo di precisare che, per la configurabilità del reato, non sono richiesti la registrazione o il riconoscimento di un marchio né, tantomeno, la sua effettiva contraffazione o la concreta induzione in errore dell'acquirente sul prodotto acquistato, essendo sufficiente la mera attitudine a trarre in inganno il consumatore sulle caratteristiche essenziali del prodotto (Sez. 3^, n. 23819, 9 giugno 2009 ed altre prec. conf.) e che il bene giuridico oggetto di tutela non è l'interesse dei consumatori o quello degli altri produttori, ma quello generale attinente all'ordine economico, tanto che la messa in vendita o in circolazione di prodotti con segni mendaci determina, di per sé, una lesione effettiva e non meramente potenziale della lealtà degli scambi commerciali (Sez. 3^, n. 2003 15 gennaio 2008). Tali principi trovano peraltro riscontro nella collocazione del reato nel Codice penale tra i delitti contro l'industria e commercio, diversamente da quelli di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti modelli e disegni (art. 473 c.p.) e di introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.) inseriti tra i delitti contro la fede pubblica. Ciò posto, deve rilevarsi che certamente il reato in questione può configurarsi anche con riferimento ai prodotti individuabili, come nella fattispecie, in 'oggetti di design'».

[49]Cfr. RIVERDITI, *La tutela penalistica*, cit., 74.

«manufatti, prodotti anche in serie, il cui elemento caratterizzante si può dire individuato, principalmente, nel particolare profilo estetico, nelle singole caratteristiche funzionali o di progettazione ovvero dalle particolari metodologie di lavorazione o produzione applicate».[50] Dunque, (I) il profilo estetico, (II) le caratteristiche funzionali o di progettazione e (III) le particolari metodologie di lavorazione o produzione adottate costituiscono il «segno distintivo che ne consente l'esatta individuazione e, conseguentemente, garantisce la loro originalità e la provenienza da un determinato produttore».[51]

Tuttavia, tale scelta ermeneutica di far ricadere i prodotti di *industrial design* all'interno della fattispecie criminosa di cui all'articolo 517 c.p., in cui viene punito l'uso fraudolento di «nomi, marchi o segni distintivi nazionali o esteri» e non anche la mera forma del prodotto o particolare profilo estetico», sembra contrastare con i principi generali di riserva di legge, il cui corollario è costituito dal divieto di analogia in *malam partem* nei confronti dell'autore della condotta.[52]A tale critica si potrebbe, d'altro canto, rispondere che la *species «industrial design»* rientra all'interno del più ampio *genus* «marchio» o «segno distintivo» e che, pertanto, l'interpretazione della Cassazione è, al più, estensiva.

1.3. I *domain names*: una disciplina ancora da scrivere.

Ad oggi, con riferimento alla tutela penale dei nomi di dominio– c.d. "*domain names"* –, minimo è stato il contributo offerto dalla dottrina e dalla giurisprudenza. Tuttavia, l'argomento risulta di grande interesse, per tali motivi si procederà a fornire comunque delle considerazioni sulla materia anche in ottica di una futura riforma della disciplina penalistica.

Risulta opportuno premettere in cosa consista il nome di dominio: esso è l'indirizzo in formato alfabetico di un sito *web*. Senza l'esistenza dei nomi a dominio, i siti web sarebbero rintracciabili soltanto tramite gli indirizzi *Internet*

[50]Cass. pen., cit., 6254/2011.
[51] Cass. pen., cit., 6254/2011: «In conclusione, deve quindi affermarsi il principio secondo il quale gli oggetti cosiddetti di 'designi, la cui produzione si contraddistingue per la stretta correlazione tra aspetti prettamente industriali e sensibilità artistica dell'autore che ne determinano la originalità e la riconoscibilità da parte dei consumatori, ancorché interessati ad uno specifico ambito commerciale, traggono da tale peculiarità il loro segno distintivo che ne consente l'esatta individuazione e, conseguentemente, garantisce la loro originalità e la provenienza da un determinato produttore».
[52]Cfr. RIVERDITI, *La tutela penalistica*, cit.,74.

Protocol (indirizzi IP), cioè sequenze irriconoscibili di numeri. Grazie alle regole del *Domain Name System* ("DNS"),[53] a ciascun indirizzo IP riconducibile ad un sito web viene invece assegnato un nome di dominio. In altre parole, il nome di dominio «è un sistema tecnico di conversione degli indirizzi IP in sequenze di lettere separate da punti».[54]

In questo modo, i siti possono essere più facilmente trovati, riconosciuti e ricordati dagli utenti.

Ogni nome di dominio è organizzato in una sequenza di caratteri separati da un punto: nell'esempio «www.abcde.com» dunque, il prefisso (I) «www» (*World Wide Web*), indica un sito Internet ed è un suffisso convenzionale creato in automatico dal fornitore del servizio di *hosting*, (II) «abcde» è il c.d. *Second-level domain,* cioè la parola che sceglie colui che registra il nome di dominio e infine (III) «*com*» è il *Top Level Domain* («*TLD*») posizionato alla fine del nome di dominio, che identifica il tipo di attività svolto sul sito (es.: *.com*- sito web commerciale; *.org* -organizzazioni non a scopo di lucro; .net - privati o aziende quando il .com non è più disponibile; *.info* - siti web di informazione e news, ecc.); ovvero identifica un determinato ambito territoriale (es.: .it - aziende europee che vogliono marcare l'identità italiana o il collegamento con l'Italia; .eu – utilizzato da individui, aziende o organizzazioni che devono risiedere o avere sede nell'UE; ecc.).[55]

Tra i tre livelli previsti per i nomi a dominio, quello che assume maggiore rilevanza, ai nostri fini, è il secondo: il "*second level domain*". Questo è posizionato nella parte centrale del nome di dominio, e identifica il titolare del sito (nell'esempio «abcde»), svolgendo una funzione tipicamente distintiva per chi vuole proporre e promuovere sul mercato i propri prodotti o servizi e che può

[53]«Il Domain Name System (DNS) è la 'guida telefonica' di Internet. Le persone accedono alle informazioni online tramite dei nomi di dominio, come ad esempio nytimes.com o espn.com. I browser Web interagiscono tramite indirizzi Internet Protocol (IP). Il DNS traduce i nomi di dominio in indirizzi IP, in modo che i browser possano caricare le risorse Internet.» Così, https://www.cloudflare.com/it-it/learning/dns/what-is-dns/

[54]CASABURI, *Nomi a dominio Internet e tutela della proprietà industriale*, in *Giur. di merito*, 2008, 5, 1495.

[55]Cfr. PARODI, *Profili di tutela penale dei domini su internet*, in *Dir. pen. e proc*., 2001, 4, 505.

diventare elemento di valorizzazione per l'affidabilità, la serietà e la rinomanza di un'impresa (al pari del marchio).[56]

Il nome di dominio, quindi, può identificare un'impresa che offre *on-line* i propri prodotti o servizi, ovvero qualsiasi altra persona fisica o organizzazione, anche non economica, che si serve della rete Internet per le proprie comunicazioni agli utenti finali.

La richiesta di registrazione di un nome di dominio– con la quale ci si riserva un nome a dominio su Internet per un determinato periodo di tempo, di solito un anno, rinnovabile alla scadenza– deve essere inviata al Registro competente (nazionale per il top level «.it», regionale per il top level «.eu» o generico per il top level «.com») tramite appositi soggetti accreditati chiamati *Registrar*, le società alle quali ci si rivolge per l'acquisto del dominio e dei servizi annessi, come ad esempio il servizio di hosting.[57]

L'intero procedimento si basa sul principio «*first come, first served*», secondo cui, come intuibile, il *second level domain* scelto dal richiedente viene assegnato solo se nessuno prima di lui ha registrato lo stesso nome. Tale principio ha portato alla diffusione di una pratica scorretta, il c.d. "*cybersquatting"* o "*domainsquatting"* con la quale gli utenti registrano parole di uso comune o nomi di imprese notorie nel mercato fisico a prezzi modesti per poi venderli ad un prezzo di gran lunga più elevato a chi voglia registrare, in un momento successivo, lo stesso

[56]Cfr. PARODI, *Profili di tutela penale*, cit. 505.
[57]Per un approfondimento si veda: *https://www.maggipinto.eu/nomi-a-dominio-tutela-e-procedura-di-riassegnazione/*

nome. Nei celebri casi «Interflora»[58] e «Google France»[59] decisi dalla Corte di Giustizia dell'Unione Europea, i giudici di Lussemburgo hanno ritenuto lesivi i

[58]CGUE, 22 settembre 2011, Interflora, C-323/09, para. 83-87: « 83 Laddove, per contro, il giudice del rinvio dovesse concludere che l'annuncio pubblicitario lanciato da detto uso del segno identico al marchio INTERFLORA non abbia consentito all'utente di Internet normalmente informato e ragionevolmente attento di capire che il servizio pubblicizzato dalla M & S è indipendente rispetto a quello della Interflora, e quest'ultima dovesse insistere affinché il giudice del rinvio, oltre a ritenere che sia stato arrecato pregiudizio alla funzione di indicazione d'origine di detto marchio, constati che la M & S ha del pari arrecato pregiudizio al carattere distintivo del marchio in questione contribuendo a trasformarne la natura in termine generico, sarebbe compito di tale giudice valutare, in base a tutti gli elementi che gli sono stati forniti, se la scelta, quali parole chiave su Internet, di segni corrispondenti al marchio INTERFLORA abbia avuto un impatto tale sul mercato dei servizi di consegna di fiori che il termine «Interflora» sia passato a designare, nella mente del consumatore, qualsiasi servizio di consegna di fiori. Il vantaggio indebitamente tratto dal carattere distintivo o dalla notorietà del marchio (parassitismo). 84 Come la Corte ha già considerato, un inserzionista che abbia scelto, nell'ambito di un servizio di posizionamento su Internet, una parola chiave corrispondente ad un marchio altrui mira a far sì che gli utenti di Internet, inserendo tale parola quale termine di ricerca, selezionino non solo i link mostrati sullo schermo che provengono dal titolare di detto marchio, ma anche il link promozionale di detto inserzionista (sentenza Google France e Google, cit., punto 67). 85 Risulta del pari che la circostanza che un marchio goda di notorietà rende probabile che gli utenti di Internet, in gran numero, utilizzino il nome di tale marchio come parola chiave per effettuare le loro ricerche su Internet al fine di reperire informazioni o offerte sui prodotti o i servizi di tale marchio. 86 In tali circostanze, come ha osservato l'avvocato generale al paragrafo 96 delle sue conclusioni, è incontestabile che, allorché il concorrente del titolare di un marchio che gode di notorietà sceglie quest'ultimo come parola chiave nell'ambito di un servizio di posizionamento su Internet, tale uso ha lo scopo di trarre vantaggio dal carattere distintivo e dalla notorietà del marchio in questione. In effetti siffatta scelta è idonea a generare una situazione in cui i consumatori, probabilmente numerosi, che effettuano una ricerca su Internet di prodotti o servizi del marchio che gode di notorietà mediante tale parola chiave vedranno apparire sui loro schermi l'annuncio del concorrente considerato. 87 È peraltro incontestabile che, laddove gli utenti di Internet acquistino, dopo aver preso conoscenza dell'annuncio di detto concorrente, i prodotti o i servizi offerti da quest'ultimo invece di quelli del titolare del marchio sui quali verteva inizialmente la loro ricerca, detto concorrente trae un vantaggio concreto dal carattere distintivo e dalla notorietà del marchio in questione».

[59]CGUE, 23 marzo 2010, Google France SARL c. Louis Vuitton Malletier SA e altri, cause riunite C-236, 237 e 238/08, para. 82-85: «82 La funzione essenziale del marchio consiste nel garantire al consumatore o all'utilizzatore finale l'identità di origine del prodotto o del servizio contrassegnato, consentendogli di distinguere tale prodotto o tale servizio da quelli di diversa provenienza (v., in tal senso, sentenze 29 settembre 1998, causa C-39/97, Canon, Racc. pag. I-5507, punto 28, e 6 ottobre 2005, causa C-120/04, Medion, Racc. pag. I-8551, punto 23). 83 La questione se sussista una violazione di tale funzione allorché, a partire da una parola chiave identica a un marchio, è mostrato agli utenti di Internet un annuncio di un terzo, quale un concorrente del titolare di tale marchio, dipende in particolare dal modo in cui tale annuncio è presentato. 84 Sussiste violazione della funzione di indicazione di origine del marchio quando l'annuncio non consente o consente soltanto difficilmente all'utente di Internet normalmente informato e ragionevolmente attento di sapere se i prodotti o i servizi a cui l'annuncio si riferisce provengano dal titolare del marchio o da un'impresa economicamente connessa a quest'ultimo o, al contrario, da un terzo (v., in tal senso, sentenza Céline, cit., punto 27 e giurisprudenza ivi citata). 85 Infatti, in una situazione del genere – caratterizzata del resto dal fatto che l'annuncio in questione appare subito dopo che l'utente di Internet interessato abbia inserito il marchio come parola da ricercare ed è visualizzato in un momento in cui il marchio, in qualità di parola da ricercare, è parimenti indicato sullo schermo – l'utente di Internet può confondersi sull'origine dei prodotti o dei servizi in questione. In tali circostanze, l'uso del segno identico al marchio da parte del terzo, come parola chiave che lancia la visualizzazione di detto annuncio, è idoneo ad avvalorare l'esistenza di un collegamento materiale nel commercio tra i prodotti o servizi interessati e il titolare del marchio (v.,

comportamenti suddetti laddove pregiudichino le seguenti funzioni del marchio: garanzia di provenienza, investimenti, pubblicità.

Ciò detto, è opportuno interrogarsi in merito alla natura del *domain name*: dottrina e giurisprudenza gli assegnano, allo stesso tempo, una funzione tecnico-informatica grazie alla quale l'utente ha accesso ad un determinato sito *web*, e una funzione distintiva, capace di attrarre l'attenzione dei consumatori verso quel determinato sito *web*.[60]

Dunque, se da un punto di vista civilistico è pacifico rinvenire, per analogia, la disciplina del nome di dominio negli articoli 6, 7, 8 e 9 c.c. (che tutelano il diritto al nome),[61] negli artt. 2569 e ss. c.c.[62] e artt. 12 comma 1 lett. b) e 22 c.p.i (che tutelano i marchi e i segni distintivi)[63] e infine negli artt. 2598-2601 c.c. (regolanti

---

per analogia, sentenze Arsenal Football Club, cit., punto 56, e 16 novembre 2004, causa C-245/02, Anheuser-Busch, Racc. pag. I-10989, punto 60)».

[60]GALLI, *I domain name nella giurisprudenza. L'analisi dei problemi. Il testo di 78 provvedimenti italiani dal 1996 al 2001. Il repertorio sistematico delle massime*, Milano, 2001.

[61]Art. 6 c.c.: «Ogni persona ha diritto al nome che le è per legge attribuito. Nel nome si comprendono il prenome e il cognome. Non sono ammessi cambiamenti, aggiunte o rettifiche al nome, se non nei casi e con le formalità dalla legge indicati». Art. 7 c.c.: «La persona, alla quale si contesti il diritto all'uso del proprio nome o che possa risentire pregiudizio dall'uso che altri indebitamente ne faccia, può chiedere giudizialmente la cessazione del fatto lesivo, salvo il risarcimento dei danni. L'autorità giudiziaria può ordinare che la sentenza sia pubblicata in uno o più giornali (120 c.p.c.)». Art. 8 c.c.: «Nel caso previsto dall'articolo precedente, l'azione può essere promossa anche da chi, pur non portando il nome contestato o indebitamente usato, abbia alla tutela del nome un interesse [101 c.p.c.] fondato su ragioni familiari degne d'essere protette». Art. 9 c.c.: «Lo pseudonimo, usato da una persona in modo che abbia acquistato l'importanza del nome, può essere tutelato ai sensi dell'articolo 7».

[62]Art. 2569 c.c.: «Chi ha registrato nelle forme stabilite dalla legge un nuovo marchio idoneo a distinguere prodotti o servizi ha diritto di valersene in modo esclusivo per i prodotti o servizi per i quali è stato registrato.

In mancanza di registrazione, il marchio è tutelato a norma dell'articolo 2571».

Art. 2570 c.c.: «I soggetti che svolgono la funzione di garantire l'origine, la natura o la qualità di determinati prodotti o servizi possono ottenere la registrazione di marchi collettivi per concederne l'uso, secondo le norme dei rispettivi regolamenti, a produttori o commercianti».

[63]Art. 12 co. 1 lett. b) c.p.i.: « 1. Non possono costituire oggetto di registrazione come marchio d'impresa i segni che alla data del deposito della domanda: […] b) siano identici o simili a un segno già noto come ditta, denominazione o ragione sociale, insegna e nome a dominio usato nell'attività economica, o altro segno distintivo adottato da altri, se a causa della identità o somiglianza fra i segni e dell'identità o affinità fra l'attività d'impresa da questi esercitata ed i prodotti o servizi per i quali il marchio è registrato possa determinarsi un rischio di confusione per il pubblico, che può consistere anche in un rischio di associazione fra i due segni. L'uso precedente del segno, quando non importi notorietà di esso, o importi notorietà puramente locale, non toglie la novità. L'uso precedente del segno da parte del richiedente o del suo dante causa non è di ostacolo alla registrazione». Art. 22 c.p.i.: «1. È vietato adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio di un sito usato nell'attività economica o altro segno distintivo un segno uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività di impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni. 2. Il divieto di cui al comma 1 si estende all'adozione come ditta, denominazione o ragione

la concorrenza sleale),[64] dal punto di vista penalistico, secondo alcuni,[65] maggiori dubbi sorgono con riferimento ad una applicazione analogica dell'articolo 473 c.p., essendo questa vietata se *in malam partem*. Sul punto, in particolare, parte della dottrina sostiene che i nomi di dominio non rientrerebbero nel *genus* dei segni distintivi per due ordini di motivi: in primo luogo, i *domain names* non sarebbero di «proprietà» del titolare, dato che vengono concessi solo in «uso»; in secondo luogo, i nomi di dominio non vengono concessi a seguito di un procedimento amministrativo con valore costitutivo come accade, ad esempio, nel caso dei marchi: invero, in questo ambito, non esiste nessuna normativa positiva al riguardo ma solo una disciplina avente carattere meramente pattizio.[66]

La giurisprudenza ha, tuttavia, ritenuto che i *domain names* potessero rientrare sotto la nozione di segni distintivi, registrati, in modo da tenere aperta la porta per future applicazioni delle fattispecie succitate.[67]

---

sociale, insegna e nome a dominio di un sito usato nell'attività economica o altro segno distintivo di un segno uguale o simile ad un marchio registrato per prodotti o servizi anche non affini, che goda nello Stato di rinomanza se l'uso del segno senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi».

[64]Art. 2598 c.c: «Ferme le disposizioni che concernono la tutela dei segni distintivi [2563, 2568, 2569] e dei diritti di brevetto [2584, 2592, 2593], compie atti di concorrenza sleale chiunque: 1) usa nomi o segni distintivi idonei a produrre confusione [2564] con i nomi o i segni distintivi legittimamente usati da altri, o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti e con l'attività di un concorrente; 2) diffonde notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o si appropria di pregi dei prodotti o dell'impresa di un concorrente; 3) si vale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda [1175, 2599, 2600]». Art. 2599 c.c: «La sentenza che accerta atti di concorrenza sleale ne inibisce la continuazione e dà gli opportuni provvedimenti affinché ne vengano eliminati gli effetti [2598, n. 3]». Art. 2600 c.c: «Se gli atti di concorrenza sleale sono compiuti con dolo o con colpa, l'autore è tenuto al risarcimento dei danni [2043, 2598, n. 3]. In tale ipotesi può essere ordinata la pubblicazione della sentenza [120 c.p.c.]. Accertati gli atti di concorrenza, la colpa si presume [2727]». Art. 2601 c.c: «Quando gli atti di concorrenza sleale [2598] pregiudicano gli interessi di una categoria professionale, l'azione per la repressione della concorrenza sleale può essere promossa anche [dalle associazioni professionali e] dagli enti che rappresentano la categoria».

[65]CASABURI, *Nomi a* dominio, cit., 1495.

[66]CASABURI, *Nomi a* dominio, cit., 1495.

[67]Cass. pen., Sez. V, 15 giugno 2022, n. 23364 , la quale nell'escludere che il c.d. "modello ornamentale" sia un segno distintivo in senso tecnico, ha espressamente affermato che all'interno di tale categoria rientrino i nomi a dominio: «[n]el rinnovato giudizio di merito, dunque, i Giudici del rinvio dovranno chiarire il substrato fattuale dal quale traggono il convincimento relativo alla qualificazione giuridica del fatto, secondo le indicate coordinate ermeneutiche, tenendo, altresì, a mente che il modello cd. ornamentale (per cui si intende "quello idoneo a conferire a determinati prodotti industriali uno speciale ornamento, sia per la forma, sia per una particolare combinazione di linee o di altri qualificanti elementi" (R.D. 25 agosto 1940, n. 1411, art. 5, in materia di brevetti per invenzioni industriali), non è né marchio, né segno distintivo in senso tecnico, nozione che comprende il marchio, la ditta, l'insegna e i nomi a dominio […]».

La dottrina è divisa sul punto: una parte condivide l'approccio della giurisprudenza, ritenendo che la normativa in tema di marchi e segni distintivi possa estendersi a tutti i settori ove possa sorgere un pericolo di «confusione» per il consumatore, possibilità non rara laddove il dominio presenti caratteri simili a determinati marchi o altri segni distintivi (si pensi al caso Interflora succitato);[68] altri autori[69] hanno invece fatto leva sulle condotte fraudolente di registrazione di nomi simili a marchi notori al fine di trarre profitto al fine di applicare l'articolo 513 c.p.,[70] il quale punisce condotte vicine, ma non equipollenti, alla concorrenza sleale.

1.4. La tutela penale delle indicazioni geografiche e denominazioni d'origine: l'articolo 517-*quater*.

Il sistema delle fonti che disciplinano l'origine dei prodotti, da un punto di vista storico, sorge nel 1891 con l'Accordo di Madrid,[71] che all'articolo 1 menziona per la prima volta l'indicazione di provenienza;[72] a tale trattato si accompagnano poi l'Accordo di Lisbona del 1958-[73] che all'articolo 2 definiva le nozioni di

[68]Cfr. C. PARODI, *Profili di tutela penale*, cit. 505 ss.
[69]GIUNTA, *Lineamenti di diritto penale dell'economia*, 2ª ed., Giappichelli, Torino, 2004.
[70]Art. 513 c.p.: «Chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio è punito, a querela della persona offesa, se il fatto non costituisce un più grave reato, con la reclusione fino a due anni e con la multa da euro 103 a euro 1.032».
[71]Accordo di Madrid sulla repressione delle false o fallaci indicazioni di provenienza del 14 aprile 1891. I. Atto riveduto a Washington il 2 giugno 1911, all' Aja il 6 novembre 1925, a Londra il 2 giugno 1934 e a Lisbona il 31 ottobre 1958. II. Atto aggiuntivo di Stoccolma del 14 luglio 1967. Disponibile al seguente link: https://www.wipo.int/edocs/pubdocs/it/wipo_pub_261.pdf.
[72]Art. 1 Accordo di Madrid: «1. Qualsiasi prodotto recante una falsa o ingannevole indicazione di provenienza, nella quale uno dei paesi, cui si applica il presente Accordo, o un luogo situato in uno di essi, fosse direttamente o indirettamente indicato come paese o come luogo d'origine, sarà sequestrato alla importazione in ciascuno dei detti paesi. 2. Il sequestro sarà eseguito anche nel paese in cui la falsa o ingannevole indicazione di provenienza sarà stata apposta, o in quello in cui sarà stato importato il prodotto recante tale falsa o ingannevole indicazione. 3. Se la legislazione di un paese non ammette il sequestro all'importazione, questo sarà sostituito dal divieto d'importazione. 4. Se la legislazione di un paese non ammette né il sequestro all'importazione, né il divieto d'importazione, né il sequestro nell'interno, dette misure, nell'attesa che detta legislazione sia adeguatamente modificata, saranno sostituite dalle azioni e dai mezzi che la legge di quel paese assicura in simili casi ai propri cittadini. 5. In mancanza di sanzioni speciali che assicurino la repressione delle false o ingannevoli indicazioni di provenienza, saranno applicabili le sanzioni previste dalle corrispondenti disposizioni delle leggi sui marchi o sui nomi commerciali».
[73]Accordo di Lisbona per la protezione e la registrazione Internazionale delle denominazioni di origine e relativo regolamento di esecuzione. L'Accordo di Lisbona ha introdotto anche la possibilità per i titolari dei diritti d'effettuare una registrazione internazionale della denominazione d'origine valida in tutti i Paesi aderenti. Per ulteriori approfondimenti: https://www.wipo.int/treaties/en/registration/lisbon/.

«denominazione d'origine» e «paese di origine» intendendo la prima come «denominazione geografica di un Paese, di una regione o di una località, che serve a designare un prodotto ivi originario, la cui qualità o le cui caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico, compresi i fattori naturali e umani» e la seconda come «il paese il cui nome, o il paese in cui è situata la regione o la località il cui nome, costituisce la denominazione d'origine che ha conferito al prodotto la sua reputazione»- e l'articolo 22 del TRIPs che definisce le indicazioni geografiche come «indicazioni che identificano un bene come originario del territorio di un Membro, o di una regione o località di tale territorio, quando una determinata qualità, la reputazione o altre caratteristiche del bene sono essenzialmente attribuibili alla sua origine geografica».

Sempre lo stesso articolo 22 del TRIPs stabilisce come, con riferimento alle indicazioni geografiche, «le parti interessate devono disporre di mezzi legali per impedire l'uso di indicazioni che inducano in errore il pubblico sull'origine geografica del prodotto e l'uso che costituisca un atto di concorrenza sleale ai sensi dell'articolo 10-*bis* della Convenzione di Parigi (articolo 22.2).

La registrazione di un marchio che utilizza un'indicazione geografica in modo da indurre il pubblico in errore sul vero luogo di origine deve essere rifiutata o invalidata d'ufficio se la legislazione lo consente o su richiesta di una parte interessata (articolo 22.3)».

Il legislatore comunitario, infine, regola la materia in maniera più approfondita con il Regolamento (UE) n. 1151/2012 sui regimi di qualità dei prodotti agricoli e alimentari,[74] il quale detta, all'articolo 5, le nozioni di «denominazione d'origine» e «indicazione geografica».[75]

[74]Regolamento (UE) n. 1151/2012 del Parlamento Europeo e del Consiglio del 21 novembre 2012 sui regimi di qualità dei prodotti agricoli e alimentari.

[75]Art .5 Reg. (UE) n. 1151/2012: «1. Ai fini del presente regolamento, 'denominazione di origine' è un nome che identifica un prodotto: a) originario di un luogo, regione o, in casi eccezionali, di un paese determinati; b) la cui qualità o le cui caratteristiche sono dovute essenzialmente o esclusivamente ad un particolare ambiente geografico ed ai suoi intrinseci fattori naturali e umani; e c) le cui fasi di produzione si svolgono nella zona geografica delimitata. 2. Ai fini del presente regolamento, «indicazione geografica» è un nome che identifica un prodotto: a) originario di un determinato luogo, regione o paese; b) alla cui origine geografica sono essenzialmente attribuibili una data qualità; la reputazione o altre caratteristiche; e c) la cui produzione si svolge per almeno una delle sue fasi nella zona geografica delimitata. 3. In deroga al paragrafo 1, taluni nomi sono equiparati a denominazioni di origine anche se le materie prime dei relativi prodotti provengono da una zona geografica più ampia della zona geografica delimitata, o diversa da essa, purché siano soddisfatte le seguenti condizioni: a) la zona di produzione delle materie prime è delimitata; b)

In coerenza con tali fonti internazionali e comunitarie, il legislatore italiano, all'articolo 29 c.p.i afferma che «[s]ono protette le indicazioni geografiche e le denominazioni di origine che identificano un paese, una regione o una località, quando siano adottate per designare un prodotto che ne è originario e le cui qualità, reputazione o caratteristiche sono dovute esclusivamente o essenzialmente all'ambiente geografico d'origine, comprensivo dei fattori naturali, umani e di tradizione».

Dal punto di vista penalistico, il legislatore appresta una tutela non solo all'interno del Codice penale ma anche in svariate disposizioni *extra-codicem*;[76] tuttavia, la presente dissertazione, si concentrerà sulla tutela apprestata dal codice penale all'articolo 517-quater[77] introdotto dalla legge n. 99 del 2009 citata, data la sua potenziale più frequente applicazione anche nei confronti delle piattaforme digitali.

Tale fattispecie criminosa contrasta i fenomeni contraffattivi delle indicazioni geografiche e delle denominazioni d'origine dei soli prodotti agroalimentari. La norma si compone di due fattispecie disciplinanti condotte diverse (come avviene per l'articolo 474 c.p., seppur le condotte siano diverse): il primo comma sanziona la condotta di contraffazione, mentre il comma due punisce l'«introduzione», la «detenzione per la vendita», la «vendita diretta ai consumatori»[78] e in ogni caso «la messa in circolazione degli stessi prodotti con indicazioni o denominazioni contraffatte». Solo in questo secondo caso è richiesto

---

sussistono condizioni particolari per la produzione delle materie prime; c) esiste un regime di controllo atto a garantire l'osservanza delle condizioni di cui alla lettera b); e d) le suddette denominazioni di origine sono state riconosciute come denominazioni di origine nel paese di origine anteriormente al 10 maggio 2004».

[76]Si vedano, ad esempio, l'articolo 16 del d.l. 135/2009 che tutela il c.d. "*full made in Italy*"; l'art. 3 della legge n. 55 del 2010 in materia di prodotti tessili e calzaturieri.

[77]Art. 517-*quater* c.p.: «Chiunque contraffà o comunque altera indicazioni geografiche o denominazioni di origine di prodotti agroalimentari è punito con la reclusione fino a due anni e con la multa fino a euro 20.000. Alla stessa pena soggiace chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte. Si applicano le disposizioni di cui agli articoli 474 bis, 474 ter, secondo comma, e 517 bis, secondo comma. I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali in materia di tutela delle indicazioni geografiche e delle denominazioni di origine dei prodotti agroalimentari».

[78] Il fatto che la vendita debba essere diretta «ai consumatori» per assumere rilevanza penale, esclude la rilevanza della condotta posta in essere tra intermediari commerciali (operazioni B2B), una conseguenza a cui il legislatore dovrebbe porre rimedio.

l'elemento soggettivo del dolo specifico («al fine di trarne profitto»); mentre con riferimento al primo comma, e quindi per la condotta di contraffazione, è sufficiente il dolo generico.

L'art. 517-*quater* c.p. dunque, riprendendo le condotte rintracciabili negli artt. 473 e 474 c.p., colma la lacuna di questi ultimi laddove essi non includono tra i titoli di proprietà industriale protetti, le indicazioni geografiche tutelate *ex* art. 30 c.p.i. Se è vero che il legislatore, per la costruzione delle condotte della fattispecie in esame si è ispirato all'articolo 474 c.p., è altrettanto vero che lo stesso non è accaduto per ciò che riguarda il trattamento sanzionatorio: la mancata graduazione della pena in ragione del diverso disvalore offensivo tra i due commi, *rectius*, le due categorie di condotte (di «contraffazione» e di «introduzione», «detenzione per la vendita», «vendita diretta ai consumatori» e la «messa in circolazione»), appare irragionevole.

Sempre prendendo a modello l'articolo 474 c.p., l'ultimo comma dell'articolo 517-*quater* richiede come presupposto della condotta il fatto che «che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali in materia di tutela delle indicazioni geografiche e delle denominazioni di origine dei prodotti agroalimentari».

Infine l'articolo 517-*quinquies* prevede un'attenuante speciale ad effetto speciale laddove prevede una diminuzione della pena dalla metà ai due terzi qualora il «colpevole che si adopera per aiutare concretamente l'autorità di polizia o l'autorità giudiziaria nell'azione di contrasto […], nonché nella raccolta di elementi decisivi per la ricostruzione dei fatti e per l'individuazione o la cattura dei concorrenti negli stessi, ovvero per la individuazione degli strumenti occorrenti per la commissione dei delitti medesimi o dei profitti da essi derivanti».

1.5. La tutela dei c.d. *trade secrets*: l'articolo 623 c.p.

Il presente paragrafo, a seguito di una breve premessa circa la rilevanza dei segreti commerciali e la loro mutabilità nel corso degli anni, si concentrerà sulla definizione e disciplina dei segreti commerciali, così come riformata a seguito

dell'emanazione della Direttiva (UE) 2016/943[79] e, in seguito, analizzerà la problematica sovrapposizione delle due discipline, civilistica e penalistica, tentando di strutturare in modo differente l'oggetto del segreto commerciale tutelabile dalle due diverse branche del diritto.

La rilevanza dei segreti commerciali affonda le sue radici in un periodo addirittura antecedente la rivoluzione industriale; è, però, con il progredire dell'industria e del commercio che le particolari tecniche e processi di produzione industriali diventano oggetto di desiderio di imprese concorrenti, disposte a tutto pur di ridurre il *gap* competitivo, anche a realizzare condotte illecite, talvolta, a rilevanza anche penale.

Se la rilevanza del segreto industriale è una costante storica, lo stesso non può dirsi con riferimento al contenuto del segreto stesso: questo è andato mutando nel corso degli anni, riflettendo il cambiamento vissuto dal tessuto economico-sociale. Particolarmente rilevante a questi fini è stato l'avvento delle tecnologie digitali e di Internet: le quali hanno, da un lato, mutato il bene giuridico oggetto di tutela e, dall'altro, variato le modalità di attacco a tale bene giuridico.

In questo scenario è intervenuta l'Unione Europea con l'emanazione della già citata Direttiva (UE) 2016/943 che mira a proteggere il c.d. "*know-how"*[80] stabilendo «le norme relative alla tutela contro l'acquisizione, l'utilizzo e la divulgazione illeciti dei segreti commerciali».[81] Con la ricezione di tale Direttiva– avvenuta per via del d.lgs. 11 maggio 2018, n. 63–,[82] il legislatore italiano ha colto l'occasione di riformare l'ormai secolare articolo 623 c.p., tentando di rendere l'ordinamento giuridico domestico adatto a fronteggiare la *data-driven economy*.[83]

[79]Direttiva (UE) 2016/943 del Parlamento Europeo del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti.

[80]Per *know-how* s'intende quel patrimonio cognitivo ed organizzativo necessario per la costruzione, l'esercizio, la manutenzione di un apparato industriale.

[81]Art. 1 Dir. (UE) 2016/943.

[82]D.lgs. n. 63 del 2018, «Attuazione della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti».

[83]La *data-driven economy* è un'economia in cui l'uso dei dati è centrale nelle strategie e nella gestione del business, nello sviluppo di nuovi prodotti e servizi, nei processi decisionali, nel rinnovamento dei modelli di business, nella creazione di innovazione e nella diffusione della conoscenza. Non sarebbe sbagliato affermare che i dati possono assurgere, e quasi sempre lo fanno, a segreti commerciali.

La Direttiva, all'articolo 2, riprendendo la definizione dell'articolo 39 dei TRIPs, definisce «segreto commerciale» quelle informazioni segrete «nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; hanno valore commerciale in quanto segrete; sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete».

Tale definizione non era, d'altro canto, lontana da quella confluita nel 2005 nell'articolo 98 c.p.i, [84] anch'esso oggetto di riforma per via della ricezione della Direttiva, per mezzo del d.lgs. n. 63 del 2018. Dall'entrata in vigore dei TRIPs e sino al maggio 2018, quindi, l'ordinamento italiano, in materia di tutela del segreto nel campo economico-tecnologico, aveva una duplice anima: se il sistema penale rimaneva ancorato ad una fattispecie di stampo prettamente napoleonico,[85] incentrata sul segreto di fabbrica e sull'idea dell'applicazione industriale, l'ordinamento civile si apriva ad una visione moderna ed anglosassone del sapere tecnologico, che poneva al centro della propria azione di tutela l'informazione commerciale in quanto tale.[86]

Lo scenario regolatorio cambia dopo il recepimento della Direttiva, con il quale il legislatore domestico abbandona il summenzionato doppio binario in favore

[84]Testo originario art. 98 c.p.i.: «Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni: a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore; b) abbiano valore economico in quanto segrete; c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete». Il testo vigente, frutto delle modifiche del d.lgs. n. 63/2018, statuisce che «Costituiscono oggetto di tutela i segreti commerciali. Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni: a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore; b) abbiano valore economico in quanto segrete; c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete».

[85]Infatti, l'articolo 623 del codice penale del 1930, prima della riforma del 2018, riprendeva l'articolo 298 del codice penale del 1889 il quale era frutto delle disposizioni napoleoniche a tutela del *secret de fabrication*. Così OMODEI, *La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione*, in *Dir. pen. cont*., 2019, 116.

[86]OMODEI, *La tutela penale del segreto commerciale in Italia*. cit., 115.

di un modello unico: la disciplina penalistica, riformata dal decreto in questione, si allinea con quella civilistica. La novella, in particolare, è intervenuta sia con riguardo al bene giuridico tutelato sia con riferimento alle modalità di aggressione con cui il reo può minacciare il segreto commerciale: la disciplina di cui all'articolo 623 c.p., prima della riforma,[87] optava per una relazione funzionale tra agente e segreto, punendo sia i lavoratori dipendenti sia soggetti esterni all'ente che, a vario titolo, partecipassero alle attività produttive dell'impresa («venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte») e tutelava il bene giuridico «notizie destinate a rimanere segrete» o «applicazioni industriali».

Il progredire tecnologico ha reso, però, nel giro di poco tempo tale norma scarsamente efficace: essa mostrava le proprie pecche soprattutto in merito al bene tutelato, in quanto, seppur la nozione di «applicazioni industriali» fosse interpretata, dalla più recente giurisprudenza, in senso ampio,[88] il tenore letterale della disposizione non permetteva all'interprete di sanzionare con lo strumento penale le condotte di violazione dei c.d. "segreti commerciali" (essendo tale termine più ampio rispetto a «notizie destinate a rimanere segrete» o «applicazioni industriali»), ed in generale di tutte quelle informazioni e dati assolutamente centrali nell'odierna *data-driven economy*– senza sfociare in un'operazione analogica, vietata.

Con la novella in disamina, si è assistito, da una parte, alla sostituzione della formula «applicazioni industriali» con l'espressione «segreti commerciali»; dall'altra è stato inserito un nuovo comma all'articolo 623 che commina la stessa pena di cui al comma 1 (reclusione sino a due anni) anche a «chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o

[87]Art. 623 c.p. prima dell'11 maggio 2018: «1. Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni. 2. Il delitto è punibile a querela della persona offesa».

[88]Cass. pen., Sez. V, 30 ottobre 2002, n. 36309: «In tema di segreti scientifici o industriali, il concetto di notizia destinata al segreto va elaborata, sotto l'aspetto soggettivo, con riferimento all'avente diritto al mantenimento del segreto stesso (il titolare dell'azienda) e, sotto quello oggettivo, all'interesse a che non vengano divulgate notizie attinenti ai metodi (di progettazione, produzione e messa a punto dei beni prodotti) che caratterizzano la struttura industriale) e, pertanto, il c. d. know-how, ossia quel patrimonio cognitivo e organizzativo necessario per la costruzione, l'esercizio e la manutenzione di un apparato industriale. Ne consegue che oggetto della tutela penale del reato in questione deve ritenersi il segreto industriale in senso lato, vale a dire quell'insieme di conoscenze riservate e di particolar 'modus operandi' in grado di garantire la riduzione al minimo degli errori di progettazione e realizzazione e dunque la compressione dei tempi di produzione (sez. V, 19.5.01, n. 25008, P.)».

altrui profitto». [89] Tale comma richiama la struttura dell'illecito civile di cui al primo comma dell'articolo 99 c.p.i[90], i cui elementi essenziali sono quasi tutti presenti nella disposizione penalistica, facendo sorgere quindi all'interprete dubbi circa la corretta definizione dei ruoli dei vari strumenti di tutela in materia di segreto commerciale.

A seguito della riforma del 2018, infatti, la sovrapposizione dei piani di tutela appare assai evidente. Entrambe le disposizioni si rivolgono ad una platea potenzialmente indiscriminata di autori, entrambe richiamano l'«abusività» della condotta del soggetto agente e tutti e due gli ambiti sembrano guardare allo stesso bene, ossia il segreto commerciale. Tuttavia, mentre nell'illecito civile l'abusività si riferisce a tutte e tre le condotte rilevanti - «acquisizione», «rilevazione» e «utilizzo» - nella fattispecie criminosa, al contrario, il termine «abusivo» si riferisce alla sola condotta acquisitiva; ulteriori differenze tra gli articoli articolo 623 c.p. e 99 c.p.i., sembrano poi potersi rinvenire nell'elemento psicologico– solo dolo, e non anche colpa, per la fattispecie penalistica–, e nell'impiego, del segreto, per proprio o altrui profitto– condizione, questa, richiesta solo dalla norma penale. L'elemento soggettivo richiesto dalla fattispecie criminosa è, dunque, quello del dolo specifico.

A ciò si aggiunga che il legislatore penale non dà una definizione di «segreto commerciale»: ciò porterebbe l'interprete ad applicare la definizione civilistica, con conseguente sovrapponibilità delle due fattispecie – quella civilistica ex art. 99 c.p.i e quella penalistica ex art. 623 c.p. – se non per le minime differenze attinenti alla condotta e all'elemento soggettivo succitate. In altre parole, ciò che porta a violare la norma civile sovente integra la violazione della norma penale, la quale, in

[89]Il nuovo articolo 623 c.p. recita: «1. Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di segreti commerciali o di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, li rivela o li impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni. 2. La stessa pena si applica a chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o altrui profitto. 3. Se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata. 4. Il colpevole è punito a querela della persona offesa.»

[90]Art. 99 co. 1 c.p.i.: «Ferma la disciplina della concorrenza sleale, il legittimo detentore dei segreti commerciali di cui all'articolo 98, ha il diritto di vietare ai terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali segreti, salvo il caso in cui essi siano stati conseguiti in modo indipendente dal terzo».

astratto, per il principio di *extrema ratio* del diritto penale, dovrebbe chiedere un *quid pluris* più sostanzioso.[91]

Dunque, se da un lato è vero che la riforma operata col d.lgs. n. 63 del 2018 ha il pregio di conformare la normativa domestica alle nuove e moderne istanze tecnologiche e socio-economiche, dall'altro lato pone al giurista dei dubbi riguardo una ragionevole gradazione della responsabilità del singolo.

All'inizio del paragrafo si è accennato al fatto che, oltre a mutare i beni giuridici che oggi costituiscono segreti commerciali, sono mutate, per via degli sviluppi tecnologici anche le modalità di aggressione contro tali beni: ebbene, il legislatore del 2018 non è stato indifferente a tale tematica, inserendo un ulteriore comma, il terzo, il quale prevede un'aggravante ad efficacia comune nel caso in cui «il fatto relativo ai segreti commerciali [sia] commesso tramite qualsiasi strumento informatica».

2. La tutela penale del diritto d'autore: gli articoli 171-171-ter della legge n. 633 del 1941.

Il quadro regolatorio riguardante la tutela penale del diritto d'autore è stato oggetto, a partire dalla fine degli anni 60, di rilevanti riforme, dovute alle numerose sollecitazioni sovranazionali, soprattutto di matrice euro unitaria,[92] volte ad adeguare il contesto legislativo all'evoluzione tecnologica (si pensi alla nascita di *software* e banche dati) e alla diffusione di Internet (basti pensare alla tutela delle opere protette dal diritto d'autore, primi tra tutti film e musica, diffuse abusivamente su siti *web*).

Una delle conseguenze delle trasformazioni causate da Internet in materia di diritto d'autore è stato il ripensamento della concezione stessa di opera dell'ingegno: il prodotto creativo oggi si può manifestare in forma digitale, a prescindere della sua incorporazione in un supporto materiale.[93] Tale modificazione nella concezione dell'oggetto di tutela rendeva inidonee tutte quelle fattispecie

[91]Per un approfondimento cfr. OMODEI, *La tutela penale*, cit., 119 ss.
[92]Si vedano, tra le altre, la Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (attuata dal d.lgs. n.68 del 2003; la Direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale (attuata dal d.lgs. n. 140 del 2006); la Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale- e che modifica le direttive 96/9/CE e 2001/29/CE (attuata dal d.lgs. n.177 del 2021).
[93]Cfr. FLOR, voce *AUTORE (DIRITTO DI) (diritto penale)*, in *Enc. del dir.*, vol. X, 2017, 113.

incriminatrici costruite sullo sfruttamento abusivo del supporto materiale, piuttosto che dell'opera creativa, espressione di un'idea, dell'originalità e creatività dell'autore.

La Sezione II del Capo III («Difese e sanzioni penali») della legge n. 633 del 1941 ingloba diciassette norme, a dimostrazione di quanto fitto e complesso sia l'attuale sistema; tuttavia, ai fini del presente elaborato verranno analizzati solo gli articoli 171, 171-*bis* e 171-*ter* data la loro più frequente violazione nonché potenziale applicazione anche nei confronti delle piattaforme digitali.[94]

Questo microsistema penale tutela, non solo i diritti degli autori dell'opera creativa, ma anche i diritti connessi, disciplinati dai Titoli II e II-*bis* della stessa legge, e la *ratio* di una tutela penale del diritto d'autore- soprattutto incentrata sullo sfruttamento economico dell'opera, come si vedrà-, è da rinvenirsi nell'incoraggiamento all'innovazione e alla produzione di altre opere nell'interesse generale alla cultura.[95]

Prima di analizzare nello specifico le tre norme succitate, si procederà ad effettuare una breve panoramica generale: il quadro cui ci si riferisce contiene

[94]In particolare, verranno analizzate le lettere a-*bis*) del comma 1 dell'articolo 171 e del comma 2 dell'articolo 171-*ter*, data il necessario coinvolgimento della piattaforma digitale: infatti tali fattispecie richiedono che l'agente abbia comunicato al pubblico l'opera protetta «immettendola in un sistema di reti telematiche». L'artico 171-*bis* tutela, poi, i programmi per elaboratore e le banche dati la cui circolazione abusiva avviene sovente per mezzo di prestatori di servizi della società dell'informazione.

[95]Corte cost., 6 aprile 1995, n. 108, n. 29: «La protezione dei diritti patrimoniali e non patrimoniali derivanti da ogni produzione scientifica, letteraria e artistica viene giustificata, per tradizione ormai secolare, dal doveroso riconoscimento del risultato della capacità creativa della personalità umana, cui si collega l'ulteriore effetto dell'incoraggiamento alla produzione di altre opere, nell'interesse generale della cultura».

fattispecie criminose a tutela sia di qualsiasi opera dell'ingegno, [96] che di specifiche opere,[97] nonché di specifiche destinazioni dell'opera.[98]

Ancora, si distinguono illeciti in cui la condotta si esplica esclusivamente mediante il mezzo-tipico della tecnologia informatica o telematica,[99] e condotte che possono essere commesse anche mediante internet– ma per le quali la rete non è mezzo esclusivo di realizzazione della condotta–,[100] oppure ancora illeciti in cui il bene giuridico protetto è di "carattere tecnologico-informatico".[101]

---

[96]Le opere protette dal diritto d'autore sono elencate all'interno dell'art. 2 della l. n. 633 del 1941: «In particolare sono comprese nella protezione: 1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale; 2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale; 3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti; 4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia; 5) i disegni e le opere dell'architettura; 6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del Capo V del Titolo II; 7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del Capo V del Titolo II; 8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. 9) le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto. 10) Le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico.

[97]Si pensi ad esempio all'art. 171 co. 1 lett. a) che fa riferimento a «un'opera altrui» in contrasto con la lett. b) dello stesso articolo che invece parla di «un'opera altrui adatta a pubblico spettacolo od una composizione musicale».

[98]Si pensi all'art. 171-*ter* comma 1 lett. a): «È punito, […] chiunque a fini di lucro: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento».

[99]Si pensi all'art. 171 co. 1 lett. a-*bis*): «Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito […] chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: […] a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa […]»

[100]Si veda l'art. 171-*ter* comma 1 lett. b): «È punito […] chiunque a fini di lucro: […] b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati […]».

[101]Ad esempio l'articolo 171-ter lett. f-*bis*) punisce chiunque, ai fini di lucro e per uso non personale «fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime

Chiarito ciò, iniziamo l'analisi delle tre fattispecie succitate, per semplicità espositiva, si procederà dapprima all'analisi dell'articolo 171-*bis*, il quale tutela programmi per elaboratore (c.d. "*software"*) e banche dati, per poi analizzare contestualmente gli articoli 171 e 171-*ter*.

2.1. La tutela di programmi per elaboratore e banche dati: l'articolo 171-*bis* della legge n. 633 del 1941.

Il legislatore nazionale si è mostrato particolarmente all'avanguardia con riferimento alla tutela penale di nuove opere dell'ingegno che alla fine degli anni 90' si sono sviluppate dapprima negli Stati Uniti, e in seguito in territorio comunitario. Infatti, già con l'articolo 13 della legge 18 agosto 2000, n. 248[102] il previgente articolo 171-*bis* era stato sostituito con la seguente disposizione: «1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità. 2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-*quinquies* e 64-*sexies*, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità».

---

conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale».

[102]L. n. 248 del 2000, «Nuove norme di tutela del diritto di autore».

Rinviando a brevissimo la disamina del comma 1, la formulazione del secondo comma, con riferimento alle banche dati, non desta alcuna perplessità con riferimento all'elemento soggettivo del dolo specifico («al fine di trarne profitto») e alle condotte («riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico» ovvero «distribuisce, vende o concede in locazione»). Tuttavia, altri elementi della fattispecie risultano maggiormente criticabili: *in primis*, l'espressione «banca dati» non viene definita dalla norma, con la conseguenza che l'oggetto materiale del reato risulta generico e indeterminato, contrastando con il principio di precisione di diritto penale generale;[103] in secondo luogo ci si chiede perché il legislatore abbia fatto rinvio alle norme 64-*quinquies*[104] e 64-*sexies*[105] dato che non vi è coincidenza fra le condotte illecite. Il rinvio al primo

[103]Per la definizione di banca dati si rinvia dunque all'art. 2 n.9 l. n. 633 del 1941, secondo cui le banche dati sono «intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto». Ai sensi della giurisprudenza comunitaria, una banca dati è meritevole di tutela «purché la scelta o la disposizione dei dati […] sia espressione originale dello spirito creativo dell'autore della banca di dati». Cfr. CGUE, 1 marzo 2012, Football Dataco Ltd e altri c. Yahoo! UK Ltd e altri, C-604/10.

[104]Art. 64-*quinquies* l. n. 633 del 1941: «1. L'autore di una banca di dati ha il diritto esclusivo di eseguire o autorizzare: a) la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma; b) la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica; c) qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati; la prima vendita di una copia nel territorio dell'Unione europea da parte del titolare del diritto o con il suo consenso esaurisce il diritto di controllare, all'interno dell'Unione stessa, le vendite successive della copia; d) qualsiasi presentazione, dimostrazione o comunicazione in pubblico, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma; e) qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di cui alla lettera b)».

[105]Art. 64-*sexies* l. n. 633 del 1941: «1. Non sono soggetti all'autorizzazione di cui all'articolo 64-*quinquies* da parte del titolare del diritto: a) l'accesso o la consultazione della banca di dati quando abbiano esclusivamente finalità didattiche o di ricerca scientifica, non svolta nell'ambito di un'impresa, purché si indichi la fonte e nei limiti di quanto giustificato dallo scopo non commerciale perseguito. Nell'ambito di tali attività di accesso e consultazione, le eventuali operazioni di riproduzione permanente della totalità o di parte sostanziale del contenuto su altro supporto sono comunque soggette all'autorizzazione del titolare del diritto; b) l'impiego di una banca di dati per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale. 2. Non sono soggette all'autorizzazione dell'autore le attività indicate nell'articolo 64-quinquies poste in essere da parte dell'utente legittimo della banca di dati o di una sua copia, se tali attività sono necessarie per l'accesso al contenuto della stessa banca di dati e per il suo normale impiego; se l'utente legittimo è autorizzato ad utilizzare solo una parte della banca di dati, il presente comma si applica unicamente a tale parte. 3. Le clausole contrattuali pattuite in violazione del comma 2 sono nulle ai sensi dell'articolo 1418 del codice civile. 4. Conformemente alla Convenzione di Berna per la protezione delle opere letterarie e artistiche, ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, le disposizioni di cui ai commi 1 e 2 non possono essere interpretate in modo da consentire che la loro applicazione arrechi indebitamente pregiudizio al titolare del diritto o entri in conflitto con il normale impiego della banca di dati».

sembra riferirsi al fatto che le condotte sanzionate dal comma 2 dell'articolo 171-*bis* devono essere tenute da chi «non ha diritto», mentre il rinvio al secondo si riferisce al fatto che le condotte assumono rilevanza penale se non hanno ad oggetto opere soggette al regime delle «utilizzazioni libere».[106] In altre parole, se esiste l'autorizzazione del titolare dei diritti sulla banca dati o se si tratta di attività autorizzata per legge, le condotte previste dal comma 2 dell'articolo 171-*bis* non hanno rilevanza penale.[107]

Infine, la norma punisce anche le condotte di «estrazione»[108] o «reimpiego»[109] della banca di dati, tenute in violazione delle disposizioni di cui agli

[106]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 120.
[107]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 120.
[108]Per «estrazione» s'intende «il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di estrazione». Così, l'articolo 102-*bis*, comma 1 lett. b).
[109]Per «reimpiego» s'intende «qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di reimpiego». 102-*bis*, comma 1 lett. c).

articoli 102-*bis*[110] e 102-*ter*.[111] Tramite il combinato disposto dei due articoli sembrerebbe che le condotte di «estrazione» o «reimpiego» assumano rilevanza penale quando compiute in modo «ripetuto» e «sistematico», quando «presuppongano operazioni contrarie alla normale gestione della banca di dati o

[110]Art. 102-*bis* della l. n. 633 del 1941: «1. Ai fini del presente titolo si intende per: a) costitutore di una banca di dati: chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro; b) estrazione: il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di estrazione; c) reimpiego: qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma. L'attività di prestito dei soggetti di cui all'articolo 69, comma 1, non costituisce atto di reimpiego. 2. La prima vendita di una copia della banca di dati effettuata o consentita dal titolare in uno Stato membro dell'Unione europea esaurisce il diritto di controllare la rivendita della copia nel territorio dell'Unione europea. 3. Indipendentemente dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti e senza pregiudizio dei diritti sul contenuto o parti di esso, il costitutore di una banca di dati ha il diritto, per la durata e alle condizioni stabilite dal presente Capo, di vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale della stessa. 4. Il diritto di cui al comma 3 si applica alle banche di dati i cui costitutori o titolari di diritti sono cittadini di uno Stato membro dell'Unione europea o residenti abituali nel territorio dell'Unione europea. 5. La disposizione di cui al comma 3 si applica altresì alle imprese e società costituite secondo la normativa di uno Stato membro dell'Unione europea ed aventi la sede sociale, l'amministrazione centrale o il centro d'attività principale all'interno della Unione europea; tuttavia, qualora la società o l'impresa abbia all'interno della Unione europea soltanto la propria sede sociale, deve sussistere un legame effettivo e continuo tra l'attività della medesima e l'economia di uno degli Stati membri dell'Unione europea. 6. Il diritto esclusivo del costitutore sorge al momento del completamento della banca di dati e si estingue trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data del completamento stesso. 7. Per le banche di dati in qualunque modo messe a disposizione del pubblico prima dello scadere del periodo di cui al comma 6, il diritto di cui allo stesso comma 6 si estingue trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data della prima messa a disposizione del pubblico. 8. Se vengono apportate al contenuto della banca di dati modifiche o integrazioni sostanziali comportanti nuovi investimenti rilevanti ai sensi del comma 1, lettera a), dal momento del completamento o della prima messa a disposizione del pubblico della banca di dati così modificata o integrata, e come tale espressamente identificata, decorre un autonomo termine di durata della protezione, pari a quello di cui ai commi 6 e 7. 9. Non sono consentiti l'estrazione o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca di dati, qualora presuppongano operazioni contrarie alla normale gestione della banca di dati o arrechino un pregiudizio ingiustificato al costitutore della banca di dati. 10. Il diritto di cui al comma 3 può essere acquistato o trasmesso in tutti i modi e forme consentiti dalla legge».

[111]Art. 102-*ter* della l. n. 633 del 1941: «1. L'utente legittimo della banca di dati messa a disposizione del pubblico non può arrecare pregiudizio al titolare del diritto d'autore o di un altro diritto connesso relativo ad opere o prestazioni contenute in tale banca. 2. L'utente legittimo di una banca di dati messa in qualsiasi modo a disposizione del pubblico non può eseguire operazioni che siano in contrasto con la normale gestione della banca di dati o che arrechino un ingiustificato pregiudizio al costitutore della banca di dati. 3. Non sono soggette all'autorizzazione del costitutore della banca di dati messa per qualsiasi motivo a disposizione del pubblico le attività di estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo. Se l'utente legittimo è autorizzato ad effettuare l'estrazione o il reimpiego solo di una parte della banca di dati, il presente comma si applica unicamente a tale parte. 4. Le clausole contrattuali pattuite in violazione dei commi 1, 2 e 3 sono nulle».

arrechino un pregiudizio ingiustificato al costitutore della banca di dati», ed abbiano ad oggetto «parti non sostanziali del contenuto della banca di dati»,[112] per il cui utilizzo non è richiesta l'autorizzazione del costitutore della banca di dati, che sia stata «messa per qualsiasi motivo a disposizione del pubblico».[113]

Passando adesso ad analizzare il primo comma, che tutela il *software*, è sin da subito da notare, come esso si componga di due parti: la prima parte dell'articolo 171-*bis* sanziona con la stessa pena condotte tra loro eterogenee («duplica», «importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori»), mentre la seconda punisce condotte meramente prodromiche o strumentali alla violazione dei diritti, condotte che hanno ad oggetto le misure tecnologiche di protezione.

Si procederà dapprima all'analisi della prima parte del comma 1, per poi procedere alla seconda parte.

Per ciò che riguarda la prima parte del comma 1 dell'articolo 171-*bis*, le condotte penalmente rilevanti, succitate, sono, da un lato, condotte dirette alla violazione dei diritti d'autore e aventi quale oggetto materiale l'opera dell'ingegno, dall'altro, condotte di "possesso" aventi come oggetto l'opera dell'ingegno (il *software*), entrambe rilevanti se commesse con dolo specifico («per trarne profitto»).

Per ciò che riguarda le condotte di «importazione», «distribuzione», «vendita» e «concessione in locazione» non sorgono particolari problemi interpretativi nonostante, la punibilità sia, forse irragionevolmente, limitata ai *software* fissati su supporti non contrassegnati dalla SIAE.

Maggiormente complessa, al contrario, sembra essere l'attività ermeneutica da svolgere con riferimento alle condotte di «detenzione a scopo commerciale o imprenditoriale» a causa delle modifiche intervenute sulla condotta stessa (da «detenzione a scopo commerciale» a «detenzione a scopo commerciale o imprenditoriale») e sull'elemento soggettivo del reato (da «scopo di lucro» a «profitto»).[114] Tali modifiche, infatti, hanno ampliato la portata applicativa della

[112]Art. 102-*bis* co. 9 della l. n. 633 del 1941.
[113]Art. 102-*ter* co. 3 della l. n. 633 del 1941.
[114]Modifiche intervenute con la l. cit. n. 248 del 2000.

fattispecie criminosa in esame: oggi risultano punibili condotte poste in essere per «risparmiare» (che antecedentemente non rientravano nella nozione di «lucro», ma che rientrano nella nozione di «profitto»), rischiando di attrarre nell'alveo della sanzione penale anche condotte realizzate non a scopo commerciale ma bensì in ambito privato e personale.

Si pensi al caso in cui il titolare di un esercizio commerciale detenga copie non autorizzate di software che utilizza al fine gestire in maniera più efficiente il proprio sistema informatico, senza venderlo. Il dubbio è se tale condotta sia penalmente rilevante *ex* articolo 171-*bis* comma 1.[115] La giurisprudenza è divisa sul punto.

Una corrente ritiene che la detenzione e l'uso di copie non autorizzate di software integrino gli elementi oggettivi e soggettivi del reato:[116] lo scopo di «profitto», come anticipato, rende penalmente rilevante il perseguimento di ogni vantaggio anche non patrimoniale;[117] mentre per ciò che riguarda la «detenzione per scopo commerciale o imprenditoriale», secondo questa parte di giurisprudenza, il legislatore non avrebbe inteso ampliare l'ambito di applicazione della fattispecie quanto piuttosto avrebbe inserito tale specificazione («o imprenditoriale») recependo correttamente la direttiva europea.

Altra parte di giurisprudenza, al contrario, ha ritenuto errata l'interpretazione secondo cui «la detenzione per fini imprenditoriali» sarebbe integrata ogni qualvolta un software venga utilizzato in modo abusivo da un professionista o una ditta: lo scopo imprenditoriale non dovrebbe essere costituito dall'uso del software da parte di un imprenditore *per sé*, ma viene integrato dalla

[115]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 124.

[116]Cfr. Cass. Pen., Sez. III, 8 maggio 2008, n. 25104: «Per la configurabilità del reato del reato di cui all' art.171 bis non è richiesto, infatti, che la riproduzione dei software sia finalizzata al commercio, essendo sufficiente il fine di profitto, come contestato, né il dolo specifico del fine di lucro. Ha più volte affermato questa Corte che, a seguito della modifica del primo comma dell'art.171 bis L. 27 aprile 1941 n.633 (apportata dall'art.13 L.18 agosto 2000 n.248), non è più previsto il dolo specifico del "fine di lucro" ma quello del "fine di trarne profitto"; si è, quindi, determinata un'accezione più vasta che non richiede necessariamente una finalità direttamente patrimoniale ed amplia quindi i confini della responsabilità dell'autore (cfr. ex multis Cass. pen. sez.3, del 6.9.2001 n.33303; Cass.pen.sez.3, 9.1.2007 n.149)».

[117]Una parte di dottrina, al contrario, ritiene che dato che tali norme incriminatrici sono poste a tutela di interessi patrimoniali, il dolo specifico, seppur di profitto e non di lucro, dovrebbe comunque intendersi come legato a vantaggi solo economici. Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 124.

condotta di chi commette il fatto «esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione".[118]

La Suprema Corte sembra avallare quest'ultimo indirizzo in merito al significato da attribuire alla detenzione a scopo commerciale o imprenditoriale a fine di profitto: quest'ultima non sarebbe riferita al mero possesso di *software* abusivamente utilizzati per ottenere un risparmio nella sfera privata, ma riguarderebbe piuttosto la detenzione del programma al fine di una sua commercializzazione o destinazione imprenditoriale.[119]

Ovviamente, con riferimento allo scopo di profitto, la responsabilità dell'imputato è da escludersi ogni qualvolta non venga provato che i *software* detenuti abusivamente in un computer siano utilizzati in relazione all'attività commerciale o imprenditoriale; in questo caso è applicabile la sanzione amministrativa dell'articolo 174-*ter*.[120]

---

[118]Trib. Bolzano, Sez. ufficio indagini preliminari, 31 marzo 2005: «In realtà ciò che è stato accertato non prova affatto che l'imputato abbia detenuto programmi duplicati o programmi duplicati illegalmente o che abbia agito con il dolo richiesto né che abbia agito a scopo imprenditoriale.
Preliminarmente si rileva che non appare corretta l'interpretazione secondo cui basta che un programma sia in uso presso un professionista o una ditta per realizzare il richiesto 'scopo imprenditoriale'. Questa interpretazione è senza dubbio superficiale perché lo scopo imprenditoriale non è costituto dall'uso del programma da parte di un imprenditore (interpretazione assurda che non consentirebbe di ritenere illegittimo lo stesso comportamento posto in essere da una associazione ONLUS!), ma, […], si riferisce alla condotta di chi commette il fatto 'esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore».

[119]Cass. Pen., Sez. III, 26 gennaio 2016, n. 23365: «La sentenza impugnata, infatti, ha congruamente ritenuto che la detenzione per scopi commerciali dei programmi per elaboratore fosse integrata dalla installazione dei software privi di licenza d'uso sul computer detenuto nell'eliografia dell'imputato, che esercita imprenditorialmente l'attività di fotocopisteria, commercio di cancelleria, materiale informatico e di stampa. Tali elementi sono stati ritenuti univocamente indizianti la destinazione dei programmi a scopo commerciale, in assenza di prova di un soltanto asserito (e francamente inverosimile) uso personale».

[120]Art. 174-*ter* l. n. 633 del 1941: «1. Chiunque abusivamente utilizza, anche via etere o via cavo, duplica, riproduce, in tutto o in parte, con qualsiasi procedimento, anche avvalendosi di strumenti atti ad eludere le misure tecnologiche di protezione, opere o materiali protetti, oppure acquista o noleggia supporti audiovisivi, fonografici, informatici o multimediali non conformi alle prescrizioni della presente legge, ovvero attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche è punito, purché il fatto non concorra con i reati di cui agli articoli 171, 171-bis, 171-ter, 171-quater, 171-quinquies, 171-septies e 171-octies, con la sanzione amministrativa pecuniaria di euro 154 e con le sanzioni accessorie della confisca del materiale e della pubblicazione del provvedimento su un giornale quotidiano a diffusione nazionale. 2. In caso di recidiva o di fatto grave per la quantità delle violazioni o delle copie acquistate o noleggiate, la sanzione amministrativa è aumentata sino ad euro 1032,00 ed il fatto è punito con la confisca degli strumenti e del materiale, con la pubblicazione del provvedimento su due o più giornali quotidiani a diffusione nazionale o su uno o più periodici specializzati nel settore dello spettacolo e, se si tratta di attività imprenditoriale, con la revoca della concessione o dell'autorizzazione di diffusione radiotelevisiva o dell'autorizzazione per l'esercizio dell'attività produttiva o commerciale».

Problematiche interpretative sono sorte circa la condotta di «duplicazione»: in particolare, ci si è chiesti, da un lato, se le condotte di «duplicazione» e «riproduzione» fossero da considerare come equivalenti, e, dall'altro, se la «duplicazione» solo parziale del codice sorgente potesse assumere rilevanza penale.[121]

Sotto il primo profilo, è stato notato come i termini succitati non siano da considerarsi sinonimi per due ordini di motivi: *in primis*, il legislatore fa riferimento agli articoli 64-*bis*, 64-*ter*, 64-*quater* alla condotta di «riproduzione» con la conseguenza che, se norme diverse prevedono altrettante condotte diverse, queste sono da ritenersi separabili e distinguibili,[122] in secondo luogo, e *a fortiori*, esistono norme all'interno delle quali sono tipizzate entrambe le condotte.[123]

Sotto il secondo profilo, la giurisprudenza di legittimità, in accordo con parte della dottrina, afferma che il codice sorgente ha natura creativa, anche qualora lo sforzo creativo addizionale sia minimo, se ha una propria autonomia funzionale e, comunque costituisce il cuore dell'opera. La conseguenza è che l'abusiva duplicazione, anche solo parziale del codice sorgente è rilevante penalmente se la parte di codice abusivamente duplicato è dotato di autonomia funzionale.[124]

Lo stesso meccanismo sanzionatorio - ma non lo stesso elemento soggettivo del dolo specifico di cui sopra - è previsto poi, destando qualche dubbio circa il principio di proporzionalità, per le condotte disciplinate dalla seconda parte del comma 1 dell'articolo 171-*bis*, meramente prodromiche o strumentali alla violazione dei diritti, le quali hanno ad oggetto le misure tecnologiche di protezione: «[l]a stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a

[121]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 120.
[122]Nello specifico la nozione di «riproduzione» può considerarsi più ampia di quella di «duplicazione», con la conseguenza che «riproduzione» e «duplicazione» stanno in un rapporto di *genus* a *species*. Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 122. Nello stesso senso Cass. Pen., Sez. III, 27 febbraio 2002, n. 15509.
[123]Si vedano gli articoli 171-*bis*, 171-*ter*, 171-*sexies*, 174-*ter* della l. n. 633 del 1941.
[124]Cass. Pen., cit., 15509/2002: «Pertanto occorre graduare i vari contenuti dell'atto di elaborazione creativa di dati reali, istruzioni tecniche o idee, seguendo in ordine all'individuazione di un contenuto minimo di originalità i criteri elaborati dalla dottrina e dalla giurisprudenza con riguardo alle opere di natura tecnico - scientifica in modo tale da apprestare la tutela penale più al programma - sorgente ed al code line invece che al programma - oggetto, qualora lo sforzo creativo addizionale sia minimo».

consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori».[125]

Conclusa così l'analisi dell'articolo 171-bis, come premesso si procederà d'ora innanzi all'analisi contestuale delle fattispecie di cui agli articoli 171[126] e 171-*ter*[127] della legge n. 633 del 1941, le quali presentano una potenziale applicazione maggiore contro le piattaforme digitali.

---

[125]Per un approfondimento sulle misure tecnologiche di protezione si rinvia al Capitolo III.

[126]Art. 171 l. n. 633 del 1941: «Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana; a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa; b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico; c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge; d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare; e) (soppresso) f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati. 1-bis. Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato. La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore. La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164».

[127]Art. 171-*ter* l. n. 633 del 1941: «1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b); d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o

2.2. La immissione abusiva di un'opera dell'ingegno protetta dal diritto d'autore in un sistema di reti telematiche: gli articoli 171 e 171-*ter* della legge n. 633 del 1941.

La risposta, all'avvento di Internet, del legislatore nazionale, è avvenuta con il recepimento della già citata Direttiva 2001/29/CE per via del d.lgs. n. 68 del 2003 che introduce le lettere a-*bis* negli articoli 171, comma 1, e 171-*ter,* comma 2, le quali recitano rispettivamente: «[s]alvo quanto disposto dall'art. 171-bis e dall'articolo 171-*ter* è punito […] chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma […] mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa», e «[è] punito […] chiunque […] in violazione

sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato; f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto. f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale; h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102- quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse. 2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque: a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1; c) promuove o organizza le attività illecite di cui al comma 1. 3. La pena è diminuita se il fatto è di particolare tenuità. 4. La condanna per uno dei reati previsti nel comma 1 comporta: a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale; b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale; c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale. 5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici».

dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa».

Le difficoltà interpretative sorte in origine – ora superate– delle due fattispecie riguardavano il soggetto autore della condotta illecita: ci si chiedeva, in particolare, se a rispondere dei reati dovessero essere i singoli *user* che condividevano materiale protetto online tramite sistemi *peer-to-peer*[128], o se invece la responsabilità fosse imputabile ai gestori dei siti web che fornivano servizi di indicizzazione e ricerca.

Rinviando al Capitolo III un approfondimento sulla responsabilità dell'*Internet Service Provider* («ISP»),[129] basti qui ricordare che i giudici di legittimità, nel famoso caso *The Pirate Bay*–[130] che ricorrerà anche nel Capitolo successivo–, hanno ritenuto colpevoli sia i gestori di un sito web– considerati sussistenti gli elementi costitutivi della fattispecie criminosa *ex* articolo 171-*ter* comma 2 lett. a-*bis* e ordinato il sequestro preventivo del sito web perché i gestori avevano concorso nell'attività, penalmente rilevante, di diffusione in Internet di opere protette dal diritto d'autore tramite attività di indicizzazione e trasferimento necessaria per il trasferimento dell'opera– sia i singoli *user* cui era direttamente imputabile l'immissione delle opere nelle reti telematiche.[131]

Procedendo con l'analisi delle due ipotesi di reato, diversi sono gli elementi comuni riscontrabili in entrambe le fattispecie: innanzitutto, è comune la condotta dei fatti tipici, ovverosia l'«immissione in un sistema di reti telematiche», c.d. "*upload*".[132]

---

[128]In una rete *peer-to-peer* («p2p»), le risorse sono condivise tra peer senza alcun coordinamento centrale da parte di un server. I pari agiscono sia come fornitori che come consumatori di risorse. I sistemi peer-to-peer implementano una rete overlay astratta a livello di applicazione sulla topologia di rete fisica. L'idea alla base delle reti peer-to-peer è quella di condividere le risorse in modo economico. Non esiste uno schema di sicurezza centralizzato e gli utenti finali stessi possono controllare l'accesso alle risorse, riducendo la sicurezza nelle reti peer-to-peer. Gli utenti possono creare qualsiasi punto di condivisione che desiderano nel proprio computer e la sicurezza può essere fornita solo assegnando una password quando creano il punto di condivisione.

[129]Per una definizione v. nota 204.

[130]Cfr. Cass. pen., Sez. III, 23 dicembre 2009, n. 49437.

[131]Cfr. Cass. pen., cit., n. 49437/2009.

[132]Operazione consistente nel trasferire un file dal proprio computer a un computer remoto attraverso un modem o una rete.

Un altro elemento comune è costituito dal risultato della condotta «messa a disposizione del pubblico» (articolo 171 comma 1 lett. a-*bis*) e «comunicazione al pubblico» (articolo 171-*ter* comma 2 lett. a-*bis*) dell'opera protetta, seppur tuttavia l'articolo 171-*ter* comma 2 lett. a-*bis* limita l'ambito di rilevanza penale richiedendo che venga contemporaneamente violato l'articolo 16.

Nonostante tale violazione non sia richiamata anche dall'articolo 171 comma 1 lett. a-*bis*), l'interprete nel verificare la sussistenza della «messa a disposizione del pubblico» deve comunque attingere all'articolo 16, essendo questa – la messa a disposizione del pubblico – una *species* del *genus* «comunicazione al pubblico».[133] La conseguenza è che, anche con riferimento a questo elemento, le due norme sono sostanzialmente equivalenti.

Un'eccezione ai fatti tipici appena citati è costituita da comma 1-*bis* dell'articolo 70, introdotto con l'articolo 2 della legge 9 gennaio 2008, n. 2, secondo cui «[è] consentita la libera pubblicazione attraverso la rete internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro».[134]

Concluso l'approfondimento sugli elementi comuni alle due norme, possiamo ora passare all'analisi delle differenze tra queste intercorrenti: l'articolo 171 comma 1 lett. a-*bis* richiede che le condotte vengano realizzate «senza averne diritto, a qualsiasi scopo e in qualsiasi forma»; trattasi dunque di reato a dolo generico.

Al contrario, l'articolo 171-*ter* comma 2 lett. a-*bis* prevede un reato a dolo specifico, punendo chiunque realizzi la condotta al fine di trarne profitto. Inoltre, lo stesso articolo esclude la punibilità se il fatto è commesso per uso personale, rinviando così agli articoli 71-*sexies*, 71-*septies*, 71-*octies*, 71-*nonies*: ne risulta di gran lunga più ampio l'ambito applicativo dell'articolo 171 comma 1 lett. a-*bis*.

Ultima differenza, la più irragionevole,[135] si rinviene nel trattamento sanzionatorio: l'articolo 171 punisce chi commette la condotta di cui al comma 1 lett. a-bis con una sanzione sia qualitativamente che quantitativamente irrisoria

[133]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 127.
[134]Critiche sono state avanzate ragionevolmente con riferimento a cosa debba intendersi per «bassa risoluzione o degradate». Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 127.
[135]Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 127. Cfr. FLOR, voce *AUTORE (DIRITTO DI)*, cit., 128.

(«multa da euro 51 a euro 2.065»), mentre l'articolo 171-*ter* comma 2– pur prevedendo, come visto sopra, condotte pressoché simili, incentrandosi il disvalore sociale nella «immissione in un sistema di reti telematiche» di opere protette–, prevede un trattamento sanzionatorio nettamente più dissuasivo («reclusione da uno a quattro anni e multa da euro 2.582 a euro 15.493»).

3. La disciplina statunitense: cenni comparatistici.

Con la liberalizzazione dei commerci internazionali e la progressiva riduzione delle barriere tariffarie raggiunte nell'ambito della Organizzazione Mondiale del Commercio («OMC»), [136] il commercio di prodotti contraffatti ha raggiunto dimensioni globali; basti pensare che, nel solo 2019, il volume del commercio internazionale di tali prodotti è ammontato a 464 miliardi di USD, pari al 2,5 % del commercio mondiale.[137]

La presente dissertazione, dunque, concluderà questo primo capitolo analizzando la disciplina penalistica statunitense in materia di contraffazione di marchi, furto di *trade secrets* e infine *copyright*, data l'assenza di qualsiasi tutela penale nei confronti degli altri diritti tutelati dalla normativa penale italiana su analizzata. Ciò in quanto gli Stati Uniti sono l'unico paese occidentale che rientra all'interno delle principali economie da cui provengono merci contraffatte e pirata in termini di sequestri doganali. [138]

Si anticipa già da adesso che nell'ordinamento statunitense le piattaforme digitali non possono, per espressa previsione normativa,[139] essere ritenute responsabili in nessun caso, salve due eccezioni: (I) quando la piattaforma concorre alla creazione

[136]L'Organizzazione Mondiale del Commercio (OMC) è l'unica organizzazione internazionale globale che si occupa delle regole del commercio tra le nazioni. L'obiettivo dell'organizzazione è garantire che il commercio fluisca nel modo più fluido, prevedibile e libero possibile.
[137]EUIPO, *Global Trade in Fakes. A Worrying Threat*, 2021.
[138]EUIPO, *Global Trade in Fakes*, cit., 19 ss.
[139]Communication Decency Act, 47 U.S.C., § 230, 1996.

o diffusione del contenuto illecito,[140] e nel caso di opere protette dal *copyright*.[141] Per un approfondimento sul tema della responsabilità delle piattaforme digitali negli Stati Uniti, si rinvia al Capitolo III.

3.1. Il *Trademark Counterfeiting Act* del 1984.

Fino all'avvento del *Trademark Counterfeiting Act* del 1984, l'ordinamento federale statunitense non prevedeva alcuna fattispecie criminosa a tutela dei marchi, i quali venivano tutelati solo attraverso i rimedi civilistici disciplinati dal *Lanham Act* del 1946.

Tuttavia, i deterrenti previsti da tale ultima normativa divennero insufficienti a fronte della internazionalizzazione delle imprese a cui conseguì la nascita di un forte fenomeno contraffattivo durante i primi anni 70',[142] giungendo, nel periodo 1977 – 1984, a causare danni per circa 100 miliardi di dollari alle aziende statunitensi.[143]

Per tale motivo il Congresso americano, avendo compreso l'eccessiva debolezza e la rara applicazione delle sanzioni civili, per contrastare il fenomeno di falso, emanò nel 1984 il *Trademark Counterfeiting Act* che introduce il 18 U.S.C. § 2320.[144]

Tale sezione punisce chiunque intenzionalmente «(1) *traffics in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services*» o «(2) *traffics in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to*

[140]In Huon v.Denton, 841 F.3d 733 (7th Cir. 2016), la corte ha ritenuto che Gawker stesso fosse un «fornitore di contenuti informativi, nella misura in cui Gawker: (1) incoraggiava e invitava gli utenti a diffamare Huon, selezionando ed esortando i commentatori più inclini alla diffamazione a «postare più commenti e continuare a intensificare il dialogo»; (2) modificava, modellava e coreografava il contenuto dei commenti che riceveva; (3) selezionava per la pubblicazione ogni commento che appariva sotto l'articolo di Jezebel; e (4) assumeva individui che erano autori di almeno alcuni dei commenti stessi». Nello stesso senso Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).
[141]Cfr. Digital Millennium Copyright Act , 17 U.S.C. (n. 47).
[142]Cfr. AMENDOLARA, *Knocking Out Knock-Offs: Effectuating the Criminalization of Trafficking in Counterfeit Goods*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 15, 2005, 3, 795.
[143]Cfr. AMENDOLARA, *Knocking Out Knock-Offs.*, cit., 796.
[144]18 U.S.C. § 2320.

deceive» oppure ancora «(3) *traffics in goods or services knowing that such good or service is a counterfeit military good or service the use, malfunction, or failure of which is likely to cause serious bodily injury or death, the disclosure of classified information, impairment of combat operations, or other significant harm to a combat operation, a member of the Armed Forces, or to national security*» ed infine «(4) *traffics in a drug and knowingly uses a counterfeit mark on or in connection with such drug*» con delle pene assai severe: ai sensi della subsezione b), infatti, è prevista una multa fino a 2.000.000 dollari e fino a dieci anni di reclusione, anche congiuntamente; se si tratta di recidiva, le sanzioni salgono fino a 5.000.000 dollari e venti anni di reclusione.[145]

Tale disciplina ha un punto di contatto con quella italiana succitata *ex* articolo 473 c.p.: la subsezione (f) del 18 U.S.C. § 2320, infatti, definendo cosa debba intendersi per «marchio contraffatto», richiede come presupposto della condotta il fatto che il marchio sia già registrato presso lo *United States Patent and Trademark Office* («USPTO») nonché la sua validità nel momento in cui si esercita l'azione penale.[146]

---

[145]18 U.S.C. § 2320, (b): «(b)Penalties. (1) In general: Whoever commits an offense under subsection (a): (A)if an individual, shall be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, shall be fined not more than $5,000,000; and (B)for a second or subsequent offense under subsection (a), if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000». Pene maggiori sono previste poi in casi specifici: si veda 18 U.S.C. § 2320 (b)(2)(A)(B) e 18 U.S.C. § 2320 (b) (3)(A)(B).

[146]18 U.S.C. § 2320, (f): «Definitions.—For the purposes of this section— (1)the term 'counterfeit mark' means— (A)a spurious mark— (i)that is used in connection with trafficking in any goods, services, labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature; (ii)that is identical with, or substantially indistinguishable from, a mark registered on the principal register in the United States Patent and Trademark Office and in use, whether or not the defendant knew such mark was so registered; (iii)that is applied to or used in connection with the goods or services for which the mark is registered with the United States Patent and Trademark Office, or is applied to or consists of a label, patch, sticker, wrapper, badge, emblem, medallion, charm, box, container, can, case, hangtag, documentation, or packaging of any type or nature that is designed, marketed, or otherwise intended to be used on or in connection with the goods or services for which the mark is registered in the United States Patent and Trademark Office; and (iv)the use of which is likely to cause confusion, to cause mistake, or to deceive; or (B) a spurious designation that is identical with, or substantially indistinguishable from, a designation as to which the remedies of the Lanham Act are made available by reason of section 220506 of title 36; but such term does not include any mark or designation used in connection with goods or services, or a mark or designation applied to labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature used in connection with such goods or services, of which the manufacturer or producer was, at the time of the manufacture or production in question, authorized to use the mark or designation for the type of goods or services so manufactured or produced, by the holder of the right to use such mark or designation.»

Diversamente da quanto avviene in Italia, invece, il legislatore federale statunitense sembra punire solo il «traffico» di beni o servizi contraffatti, non anche il processo di contraffazione in sé: ciò farebbe pensare che forse, la disciplina in disamina, appaia più simile– *mutatis mutandis*– a quella contenuta nell'articolo 517 c.p. («Vendita di prodotti industriali con segni mendaci») piuttosto che nell'articolo 473 c.p. dato che la condotta assume rilevanza nel momento in cui l'autore «*traffics*» (assimilabile a «pone in vendita o mette altrimenti in circolazione», *ex* articolo 517 c.p.) oggetti contraffatti e dato che si richiede che l'uso del segno sul bene venduto sia «*likely to cause confusion, to cause mistake, or to deceive*» (assimilabile a «atti a indurre in inganno», *ex* articolo 517 c.p.).

Tuttavia, tra le due discpline un'importante differenza va sottolineata: mentre la subsezione (f) del 18 U.S.C. § 2320 ritiene rilevante, ai fini penalistici, la condotta di «*traffic*» solo se il marchio in questione è «*identical, or substantially indistinguishable*» (solo così, infatti, il marchio può dirsi «contraffatto»), l'articolo 517 c.p. sembra avere maglie più larghe in quanto la decettività non è riferita solo al marchio ma al prodotto nel suo complesso.

3.2. L'*Economic Espionage Act*: 18 U.S.C. § 1831 e § 1832.

Quasi un decennio dopo aver penalizzato le condotte aventi l'obiettivo di commercializzare bene e servizi contraffatti, il legislatore federale statunitense decise di intervenire anche in materia di segreti commerciali: i rapporti dell'intelligence degli Stati Uniti, nella prima metà degli anni 90', stabilivano che esisteva una minaccia continua di spionaggio economico (c.d. *economic espionage*)– soprattutto con riferimento alle aziende dell'industria della difesa– che proveniva soprattutto da alleati come Francia, Giappone e Israele.[147]

L'entità del problema divenne sempre più rilevante col passare degli anni. La *White House Office of Science and Technology*, nel 1994, stimava che lo spionaggio industriale causava perdite alle aziende statunitensi per 100 miliardi di dollari all'anno in termini di vendite.[148] I bersagli più colpiti erano aziende operanti in specifici settori tecnologici indicati nella *National Critical Technologies List*

[147]Cfr. STUART, *The Criminalization of Trade Secret Theft: The Economic Espionage Act of 1996*, in *ILSA Journal of International & Comparative Law*, Vol. 4, 1998, 375 s.
[148]Cfr. STUART, *The Criminalization of Trade Secret Theft*, cit., 375 s.

("NCTL"), che include, tra le altre, sofisticate tecnologie di produzione, materiali, informazioni e telecomunicazioni.[149]

Spinto da tali motivazioni, il Congresso decise, nel 1996, di emanare l'*Economic Espionage Act* ("EEA"), che introdusse il titolo 18 U.S.C. § 1831[150] e § 1832.[151] Entrambe le disposizioni vanno lette in combinato disposto con il 18 U.S.C. § 1839[152] che detta le definizioni.

Dunque, l'*EEA* disciplina due reati separati: da un lato incrimina il furto di un segreto commerciale a beneficio di un'entità straniera (18 U.S.C. § 1831); dall'altro punisce il furto di un segreto commerciale volto a conferire un beneficio economico ad un terzo (18 U.S.C. § 1832).

Per avviare un'azione penale ai sensi di una delle due disposizioni dell'EEA, le informazioni devono essere qualificate come «segreti commerciali». L'EEA definisce in modo estensivo un «segreto commerciale»: ai sensi del 18

---

[149]Cfr. STUART, *The Criminalization of Trade Secret Theft*, cit., 375 s.

[150]18 U.S.C. § 1831: «(a) In General: Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly— (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both. (b) Organizations: Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided».

[151]18 U.S.C. § 1832: «(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly— (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both. (b) Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided».

[152]18 U.S.C. § 1839.

U.S.C. § 1839 (3)[153] per segreto commerciale, infatti, s'intendono «tutte le forme e i tipi di informazioni finanziarie, commerciali, scientifiche, tecniche, economiche o ingegneristiche, compresi schemi, piani, compilazioni, dispositivi di programma, formule, disegni, prototipi, metodi, tecniche, processi, procedure, programmi o codici, sia tangibili che intangibili, e se o come immagazzinati, compilati o memorizzati fisicamente, elettronicamente, graficamente, fotograficamente o per iscritto se: (A) il proprietario ha adottato misure ragionevoli per mantenere segrete tali informazioni; e (B) le informazioni traggono un valore economico indipendente, effettivo o potenziale, dal fatto di non essere generalmente conosciute e di non essere facilmente reperibili con mezzi adeguati da un'altra persona che possa ottenere un valore economico dalla divulgazione o dall'uso delle informazioni stesse».

La disposizione dell'*EEA* sullo «spionaggio economico», 18 U.S.C. § 1831, punisce coloro che si appropriano, o tentano, o cospirano per appropriarsi di segreti commerciali con l'intento o la consapevolezza che il reato andrà a beneficio di un governo, una *foreign insturmentality* o un agente straniero.

Il Congresso con *foreign instrumentality* intende «qualsiasi agenzia, ufficio, ministero, componente, istituzione, associazione o qualsiasi organizzazione legale, commerciale o aziendale, società, impresa o entità che sia sostanzialmente posseduta, controllata, sponsorizzata, comandata, gestita o dominata da un governo straniero».[154] Pertanto, una società straniera che si impegna nello spionaggio senza alcuna prova di sponsorizzazione o controllo da parte di un governo straniero non può essere soggetta a un procedimento penale ai sensi della § 1831. Tuttavia, un individuo o un'organizzazione che si dedica al furto di segreti commerciali, anche

[153]18 U.S.C. § 1839 (3): «*(*3) The term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A)the owner thereof has taken reasonable measures to keep such information secret; and (B)the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information».

[154]18 U.S.C. § 1839 (1): «The term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government».

se non al fine precipuo di avvantaggiare un'entità straniera, potrebbe essere responsabile della violazione della disposizione penale più generale sui segreti commerciali contenuta nella §1832 che si vedrà a brevissimo.

Tale appropriazione indebita deve essere stata commessa «consapevolmente» («*knowingly*»), in altre parole, l'individuo deve sapere che le informazioni sottratte hanno valore economico per il suo proprietario e che quest'ultimo ha preso misure ragionevoli per mantenerle riservate.

Secondo i lavori preparatori dell'EEA,[155] il «*benefit*» derivante da uno sforzo di spionaggio straniero include non solo un beneficio economico, ma anche un «beneficio reputazionale, strategico o tattico».[156]

Tuttavia, ottenere la prova che il furto del segreto commerciale abbia beneficiato un governo straniero risulta quasi impossibile: ciò spiega la quasi totale mancanza di applicazione della norma e le preoccupazioni avanzate dall'FBI.[157]

Passando all'analisi della § 1832, questa ha, come anticipato, un'applicazione più ampia e generale. Le condizioni ai fini dell'integrazione della fattispecie criminosa di furto di segreti commerciali sono (1) il furto, l'appropriazione, la distruzione, l'alterazione o la duplicazione intenzionale e/o consapevole di (2) un segreto commerciale relativo a un prodotto o servizio utilizzato o destinato a essere utilizzato nel commercio interstatale o estero (3) con l'intento di convertire il segreto commerciale («*with the intent to convert*») e (4) l'intento o la consapevolezza che tale azione danneggerà il proprietario.

Sono dunque chiare le differenze tra le § 1832 e § 1831. In primo luogo, la § 1832 non richiede che il reato vada a beneficio o intenda andare a beneficio di un'entità straniera; come anticipato, ha una portata molto più generale. Questa

[155]104th Congress, Report 104-788, To accompany H.R. 3723.
[156]104th Congress, Report 104-788, To accompany H.R. 3723: «This section requires that the government prove that the person charged with the crime acted with the intent to accomplish one of two goals. One, a person will be guilty under this section if they wrongfully copied or otherwise controlled a trade secret with the intent to benefit any foreign government, foreign instrumentality or foreign agent. In this instance, 'benefit'' is intended to be interpreted broadly. The defendant did not have to intend to confer an economic benefit to the foreign government, instrumentality, or agent, to himself, or to any third person. Rather, the government need only prove that the actor intended that his actions in copying or otherwise controlling the trade secret would benefit the foreign government, instrumentality, or agent in any way. Therefore, in this circumstance, benefit means not only an economic benefit but also reputational, strategic, or tactical benefit».
[157]Cfr. YEH, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Congressional research service, 2014, 8.

richiede poi che il furto sia economicamente vantaggioso per qualcuno che non sia il titolare del segreto commerciale, mentre la § 1831 comprende più ampiamente l'appropriazione indebita per qualsiasi scopo, compresi i vantaggi non economici, come «vantaggi reputazionali, strategici o tattici».

Stabilire che l'autore del reato intendeva arrecare un danno al titolare del segreto commerciale "non richiede che il governo dimostri il dolo o l'intenzione malvagia, ma semplicemente che l'attore sapeva o era consapevole con una certezza pratica che la sua condotta avrebbe causato un qualche svantaggio al legittimo titolare".[158]

Un'ultima differenza risiede infine nel trattamento sanzionatorio: la § 1832 prevede una pena che non può essere superiore nel massimo a 10 anni, mentre la § 1831, data la maggiore gravità della condotta, prevede una multa fino ad un massimo di 5.000.000 di dollari e 15 anni di carcere (sia alternativamente che cumulativamente). In entrambi i casi, ai sensi dei paragrafi (b) di entrambe le disposizioni, le pene sono aumentate se il fatto è commesso da un'organizzazione.[159]

3.3. Il *Criminal Copyright Infringement*: 17 U.S.C. § 506.

Gli Stati Uniti sono da sempre interessati a sostenere le industrie coinvolte nel settore dell'intrattenimento (musica, film, editoria) in ragione della loro rilevanza commerciale e politica;[160] non è un caso che già nel 1897 il Congresso decise di sanzionare la dolosa riproduzione o rappresentazione di una composizione musicale o drammatica a scopo di profitto con multe fino a 100 dollari e un anno di reclusione.[161]

---

[158]Cfr. YEH, *Protection of Trade Secrets*, cit., 9.

[159]18 U.S.C. § 1831 (b): «Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided».18 U.S.C. § 1832 (b): «Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided».

[160]Cfr. JENSEN, *The More Things Change, the More They Stay the Same: Copyright, Digital Technology, and Social Norms*, in *Stanford Law Review,* vol. 56, 2003, 2, 533,.

[161]Musical Public Performance Right Act of Jan. 6, 1897, ch. 4, 29 Stat. 481 (1897).

Oggi la disciplina è contenuta nella sezione 506 del Copyright Act (17 U.S.C. § 506)[162]: questa punisce chiunque violi intenzionalmente il copyright se la violazione è stata commessa (A) a scopo di vantaggio commerciale o di guadagno economico privato («*private financial gain*»); (B) mediante la riproduzione o la distribuzione, anche per via elettronica, durante un periodo di 180 giorni, di una o più copie o registrazioni fonografiche di una o più opere protette dal diritto d'autore, il cui valore totale al dettaglio sia superiore a 1.000 dollari; o (C) mediante la distribuzione di un'opera preparata per la distribuzione commerciale, rendendola disponibile su una rete di computer accessibile al pubblico, se tale persona sapeva o avrebbe dovuto sapere che l'opera era destinata alla distribuzione commerciale.

La sezione 101 del Copyright Act (17 U.S.C. § 101)[163] definisce il «guadagno economico» in maniera ampia: «[i]l termine 'guadagno finanziario' include la ricezione, o l'aspettativa di ricezione, di qualsiasi cosa di valore, compresa la ricezione di altre opere protette da copyright». Come si vedrà nel Capitolo III, tale ultima estensione è avvenuta per via del *No Electronic Theft Act* del 1997,[164] emanato dal Congresso a seguito del caso *US v. LaMacchia.*[165]

Infine, il *Protecting Lawful Streaming Act* del 2020, parte del *Consolidated Appropriations* Act del 2021 (Public Law No: 116-260),[166] aumenta significativamente le sanzioni penali per coloro che, intenzionalmente e a scopo di vantaggio commerciale o di guadagno finanziario privato, trasmettono in *streaming* illegalmente materiale protetto da copyright. In precedenza, invece, lo streaming illegale era considerato un reato minore (c.d. "*misdemeanor*").[167]

---

[162]17 U.S.C. § 506 (a): «Criminal Infringement: (1)In general: Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed— (A)for purposes of commercial advantage or private financial gain; (B)by the reproduction or distribution, including by electronic means, during any 180–day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or (C)by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution».

[163]17 U.S.C. § 101: «The term "financial gain" includes receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works».

[164] H.R.2265 - No Electronic Theft (NET) Act, 105th Congress (1997-1998).

[165]US v LaMacchia 871 F Supp 535 (D Mass 1994), per un approfondimento si veda il Capitolo III.

[166] Public Law 116–260—dec. 27, 2020.

[167]Cfr. FROMER, SPRIGMAN, *Copyright Law: Cases and Materials*, 2022, 608 s.

CAPITOLO II

LA TUTELA DEI DIRITTI DI PROPRIETÀ INTELLETTUALE NELL'ERA DIGITALE.

Premessa: la definizione di piattaforma digitale.

Con il termine «piattaforma digitale» («PD») si indica un insieme estremamente ampio e diversificato di servizi e strumenti digitali;[1] caratteristica comune di questi servizi è la creazione di mercati «a due lati o più lati» (c.d. *sides*) in cui gli utenti sono riuniti da un operatore di piattaforma per facilitare un'interazione (scambio di informazioni, transazione commerciale, ecc.).[2]

In termini generali, secondo una ricerca condotta, in prospettiva economica, dall' *European Parliamentary Research Service* («EPRS»)[3] , le piattaforme digitali possiedono le seguenti caratteristiche fondamentali: (I) offrono servizi digitali c.d. "*over the top*" agli utenti;[4] (II) sono o possono essere gestite come modelli di mercato a due o più lati (c.d. *sides*); (III) consentono di facilitare l'interazione complessiva tra i diversi *sides* del mercato.[5] Le peculiarità che caratterizzano le PD sono: (I) la capacità di facilitare ed estrarre valore dalle interazioni o transazioni

---

[1]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms, Panel for the Future of Science and Technology*, 2021, III.

[2]EUROPEAN COMMISSION, Commission Staff Working Document. *Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market*, 2016, 1.

[3]La missione dell'EPRS è fornire ai membri del Parlamento europeo, e se del caso alle commissioni parlamentari, un'analisi e una ricerca indipendente, obiettiva e autorevole sulle questioni politiche relative all'Unione europea, al fine di assisterli nel loro lavoro parlamentare. Per un approfondimento si veda: *https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis*

[4]«L'AGCOM definisce *Over-The-Top* (in acronimo OTT) le imprese che forniscono, attraverso la rete Internet, servizi, contenuti (soprattutto video) e applicazioni di tipo "*rich media*" (per esempio, le pubblicità che appaiono mentre si naviga in un sito web e che dopo una durata prefissata scompaiono). Esse traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi tramite concessionari agli utenti finali (ad esempio nel caso di Apple e del suo iTunes) o di spazi pubblicitari, come nel caso di Google e Facebook. Gli utenti possono accedere ai contenuti tramite qualsiasi tipo di unità con una connessione a banda larga. Tali imprese, prive di una propria infrastruttura, agiscono al di sopra delle reti, da cui il termine Over-The-Top. Il vantaggio delle OTT è che non hanno a proprio carico i costi relativi alla trasmissione ed alla gestione della rete (come per la televisione tradizionale via digitale terrestre e via digitale satellitare), che gli altri broadcaster normalmente sostengono. Si rivolgono inoltre a un mercato globale con spese di gestione e organici ridottissimi. Nel mondo pochi grandi gruppi OTT (Amazon, Facebook e Google) detengono il 75% della raccolta pubblicitaria su Internet. In Italia, nel 2019 la raccolta pubblicitaria delle piattaforme OTT ha superato la quota di pubblicità raccolta dalla radio, dalla stampa e dall'online non OTT messi insieme». Così, *https://it.wikipedia.org/wiki/Over-the-top*. Per un approfondimento si veda *https://www.agcom.it/documents/10179/539593/Allegato+20-05-2011/bd8d815d-38d8-4f75-9194-3059360b3244?version=1.0*

[5]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., III-IV.

dirette tra gli utenti; (II) la capacità di raccogliere, utilizzare ed elaborare una grande quantità di dati personali e non, al fine di ottimizzare e personalizzare il servizio e l'esperienza di ciascun utente;[6] (III) la capacità di costruire reti in cui ogni utente che si aggiunge migliorerà l'esperienza di tutti gli utenti già esistenti– i c.d. "*e*ffetti di rete";[7] (IV) la capacità di creare e modellare nuovi mercati in modo più efficiente portando di tal fatta benefici agli utenti; e (V) il ricorso alle tecnologie dell'informazione come mezzo per raggiungere tutti questi obiettivi.[8]

Tuttavia, queste caratteristiche sono presenti nella maggior parte delle piattaforme, ma non in tutte, con la conseguenza che sarebbe errato ancorare la definizione di «piattaforma digitale» alla presenza di tutti i requisiti succitati: infatti questi ultimi riflettono le diverse strategie economiche adottate, piuttosto che elementi costitutivi necessari per determinare se lo specifico servizio digitale si possa qualificare come piattaforma online.[9]

Inoltre, le PD si differenziano dai tradizionali modelli di business perché: (I) il valore generato dalla piattaforma è per la maggior parte generato online dai

[6]Tale capacità di aggregare i dati conferisce alle piattaforme un vantaggio informativo rispetto ai singoli utenti della piattaforma che causa un'asimmetria informativa tra le due parti: la piattaforma e l'utente.

[7]In virtù degli effetti di rete, generalmente, il valore del servizio è influenzato dal numero di utenti presenti. Si distinguono effetti di rete diretti e indiretti. Gli effetti di rete diretti o sullo stesso lato si verificano quando un numero crescente di utenti o clienti aumenta anche il valore del prodotto o servizio per lo stesso tipo di utente. Gli effetti di rete indiretti si verificano quando il valore del bene/servizio per l'utente appartenente ad un gruppo di clienti è in stretta dipendenza dalla presenza di utenti in un altro gruppo di clienti. Gli effetti indiretti di rete possono, poi, (I) essere negativi qualora la presenza di utenti in un altro gruppo abbia un effetto negativo sull'utilità tratta dall'utente del bene/servizio, (II) oppure positivi, laddove la presenza di utenti in un altro gruppo abbia un impatto positivo sul valore tratto dal consumatore del bene/servizio. Un ulteriore distinzione al riguardo riguarda gli effetti indiretti di rete unilaterali e bilaterali. Quanto agli effetti diretti bilaterali, questi ricorrono qualora i membri di un gruppo beneficino indirettamente della crescita del proprio gruppo in quanto ciò comporta un incentivo per l'altro gruppo ad aumentare il numero dei propri membri. È questo l'esempio il caso di un sito di e-commerce (come Amazon), in cui maggiore è la presenza di venditori, maggiore è il valore assegnato dei potenziali acquirenti al sito: dunque ciascun venditore beneficia indirettamente la presenza di altri operatori dal momento che ciò comporta un incremento del traffico sul sito web. Relativamente agli effetti indiretti di rete unilaterali, invece, questi si verificano nel caso in cui solo un versante benefici della crescita del numero di utenti nell'altro versante; e anzi ben potrebbe realizzarsi una situazione in cui l'aumento degli utenti all'interno di un gruppo potrebbe comportare effetti negativi per gli stessi.

[8]EUROPEAN COMMISSION, Commission Staff Working Document. *Online Platforms*, cit., 2.

[9]Ad esempio, le piattaforme online possono scegliere di sfruttare gli effetti di rete diretti e indiretti e le economie di scala, o addirittura operare senza nessuno di questi ultimi o solo uno di essi.

suoi utenti, piuttosto che dalla fornitura di un prodotto o servizio; (II) si basano su effetti di rete positivi.[10]

In effetti, molti studi economici sottolineano che la presenza di un forte effetto di rete indiretto[11] è una caratteristica fondamentale che distingue le PD dai mercati unilaterali; alcuni autori sostengono che è sufficiente che sia presente un effetto di rete indiretto unilaterale per determinare l'esistenza di una piattaforma, mentre altri si spingono fino a richiedere, come condizione necessaria, che entrambe le parti ne siano interessate.[12] Infine, sempre secondo la prospettiva economica le PD sono dei «*matchmaker*»[13] che attraggono due o più categorie di clienti o gruppi – i summenzionati *side* – consentendo loro di interagire a condizioni favorevoli; a seconda della piattaforma in questione, questi utenti possono rappresentare acquirenti, venditori, consumatori, aziende pubblicitarie, ecc. Non sorprende allora il rapporto sulle piattaforme digitali e il loro ruolo nella trasformazione digitale pubblicato dall'OCSE nel 2019, il quale definisce le piattaforme digitali come «servizi digitali che facilitano le interazioni tra due o più gruppi distinti ma interdipendenti di utenti (imprese o individui) che interagiscono attraverso il servizio via Internet ».[14]

Per concludere, dunque, analizzate le caratteristiche generali delle piattaforme digitali, sotto il profilo economico, quattro elementi sembrerebbero essere sufficienti e necessari affinché un'entità possa essere considerata una piattaforma digitale: (I) l'entità in questione offre un servizio, o un'infrastruttura, che altri soggetti possono utilizzare; (II) tale servizio, o infrastruttura, opera in modo digitale; (III) tale servizio, o infrastruttura, è destinato a consentire o facilitare l'interazione tra due o più (insiemi di) utenti (c.d. "multilateralità"); (IV) la presenza di effetti di rete su tale servizio, o infrastruttura.[15]

---

[10]Gli effetti di rete vengono definiti positivi, qualora, all'aumentare del numero di utenti che utilizzano la piattaforma, aumenta il valore della stessa. Caso paradigmatico sono le app di appuntamenti: tanto più sono gli utenti ad utilizzare la piattaforma, tanto più quella stessa piattaforma cresce di valora per gli utenti.

[11]Per una definizione vedi nota 10 Cap. II.

[12]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., 13.

[13]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., 11.

[14]OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation*, in *OECD Publishing*, 2019, 20.

[15]Una OP «è un servizio digitale che facilita le interazioni tra due o più gruppi distinti ma interdipendenti di utenti (aziende o individui) che interagiscono attraverso il servizio via Internet». Cfr. OECD, *An Introduction to Online Platforms*, cit., 21.

Vi è chi ritiene che le piattaforme unilaterali, ovverosia quelle che non consentono o facilitano l'interazione tra due o più insiemi di utenti,[16] vadano annoverate anch'esse all'interno del *genus* delle piattaforme digitali.[17] Ciononostante, ai fini del presente elaborato, si prenderanno in considerazione solo le piattaforme digitali caratterizzate dalla «multilateralità»: ci si riferisce in particolare ai i «servizi intermediario»[18] e le «piattaforme online».[19]

Ciò in quanto, è proprio il terzo dei requisiti succitati a rendere problematica la questione attinente all'imputazione di responsabilità penale in capo ai gestori delle piattaforme digitali: questi mettono a disposizioni uno spazio virtuale, all'interno del quale gli utenti hanno autonomia di azione, con la conseguenza che è possibile che questi commettano violazioni dei diritti di proprietà intellettuale senza la diretta compartecipazione della piattaforma. Data per certa la responsabilità penale diretta dell'utente, il dubbio risiede nell'estendibilità della stessa anche al gestore della piattaforma digitale per mezzo della quale l'utente ha commesso il reato. Tale questione verrà affrontata in modo più specifico nel corso del Capitolo III.

Conclusa così la disamina avente ad oggetto la nozione di «piattaforma digitale», da ora innanzi la dissertazione ripercorrerà le varie tappe della normativa

[16]Le piattaforme unilaterali operano fornitori unilaterali di contenuti e/o servizi. In termini economici sono considerate rivenditori o imprese verticalmente integrate (c.d. vertically integrated companies, «VIC»), a seconda, rispettivamente, che i prodotti offerti siano stati concesso in licenza da produttori terzi o fabbricati *in-house*, cioè internamente. Si pensi a Netflix – piattaforma digitale unilaterale attiva nel servizio di *streaming on-demand* di contenuti cinematografici – che opera contemporaneamente come rivenditore– nel momento in cui ottiene la licenza per la distribuzione digitale di film e serie tv prodotte da altri– e come VIC, quando offre contenuti di propria produzione.

[17]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., 13; DE STEEL, LAROUCHE, *An Integrated Regulatory Framework for Digital Networks and Services. A CERRE Policy Report*, 2016, 41 s.

[18]Tra i servizi intermediario rientrano (I) i servizi «mere conduit» consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione; (II) i servizi «caching», consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta; (III) i servizi «hosting», consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso. Così, l'art. 3 lett. g) del Regolamento (UE) 2022/2065. Per un approfondimento si veda il Capitolo III.

[19]Per piattaforma online s'intende un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico. Così, l'art. 3 lett. i) del Regolamento (UE) 2022/2065. Per un approfondimento si veda il Capitolo III.

nazionale e comunitaria avente ad oggetto la protezione dei diritti di proprietà intellettuale nell'era digitale.

Si analizzeranno dunque, dapprima, due Memorandum sulla protezione dei diritti di proprietà intellettuale,[20] per poi esaminare la Direttiva 2001/29/CE,[21] la Direttiva 2004/48/CE,[22] con le relative normative di attuazione, rinviando al Capitolo III la disamina della Direttiva 2000/31/EC, della Direttiva (UE) 2019/790, e il Regolamento EU 2022/2065, disciplinanti la responsabilità delle piattaforme digitali.

1. La tutela dei diritti di proprietà intellettuale nell'era digitale.

Come anticipato nell'introduzione della presente dissertazione, le piattaforme online costituiscono un ambiente prolifico per la diffusione di materiale illecito, generato in violazione i diritti di proprietà intellettuale dei rispettivi titolari, ciò pone minacce significative non solo a questi ultimi, ma anche alle imprese, ai consumatori e alla società in generale. In particolare, tale natura criminogena delle piattaforme è dovuto al fatto che Internet è usato da 5 miliardi di persone,[23] che il numero di *file* caricati è superiore a 15 trilioni,[24] che la condivisione di tali *file* avviene pressoché a costo zero e che spesso l'utente, creatore del contenuto, può nascondersi dietro l'anonimato; se a questo si aggiunge l'assenza di un controllo preventivo da parte delle piattaforme digitali,[25] è facile comprendere come Internet sia un «macrocosmo autosufficiente dove tutto è a disposizione di tutti in tempo reale»,[26] ivi compresi contenuti in violazione di legge. Si pensi al caso della vendita di prodotti contraffatti nei c.d. *marketplaces*, oppure alla promozione di siti web che vendono tali beni attraverso i servizi pubblicitari dei browser: questi sono

[20]Il Memorandum of Understanding on online advertising and intellectual property rights e il Memorandum of understanding on the sale of counterfeit goods on the internet.
[21]Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.
[22]La Direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale.
[23]Si veda: https://www.hdblog.it/internet/articoli/n554882/diffusione-internet-mondo-2022-trend-digitali/#:~:text=2022%20%2D%20HDblog.it-,Internet%20%C3%A8%20utilizzato%20da%20oltre%205%20miliardi,al%20mondo%3A%20il%20report%202022
[24]Si veda: https://www.cloudfiles.io/blog/how-many-files-are-there-in-the-world
[25]Per un approfondimento sull'esclusione di un controllo preventivo da parte dei gestori di piattaforme digitali, si veda il Capitolo III.
[26]TERRACINA, *La tutela penale del diritto d'autore e dei diritti connessi*, Torino, 2006.

fenomeni complessi che coinvolgono la produzione, la distribuzione e la vendita di prodotti contraffatti , che comportano diverse violazioni delle norme in materia di marchi e diritto d'autore - oltre alla potenziale inosservanza di altre normative applicabili (ad esempio, sulla vendita di farmaci contraffatti).[27]

Data la rilevanza della problematica in questione, il legislatore Europeo si è attivato al fine di regolare il mercato e fornire una soluzione al problema evidenziato. A tal fine, la normativa ha provveduto ad aumentare la responsabilità generale – lasciando, pur sempre, agli stati membri il compito di applicare la propria normativa sulla responsabilità civile o penale – degli ISP con specifico riguardo alla lotta alla distribuzione online di contenuti protetti da *copyright* o di prodotti contraffatti.

Già nel 2011 le principali piattaforme digitali insieme ad associazioni di categoria ed imprese,[28] sotto l'egida dalla Commissione Europea, hanno firmato il *Memorandum of understanding on the sale of counterfeit goods on the internet* (Memorandum d'intesa sulla vendita di merci contraffatte su Internet, «MoU I»).[29] Questo istituisce uno strumento volontario volto a prevenire offerte relative a merci contraffatte sui mercati online, migliorando le misure *notice-and-takeown*[30] e le misure proattive, tra le quali ad esempio vi rientra l'impegno, da parte delle *Internet platforms*, di considerare le notifiche inviate dai titolari dei diritti aventi ad oggetto la segnalazione delle identità dei s*ellers* che generalmente vendono beni contraffatti.[31] Inoltre, è previsto un reciproco scambio di informazioni tra le piattaforme Intenet e i titolari di diritti nell'ottica di una cooperazione volta a facilitare indagini e relative azioni di *enforcement* contro la vendita dei beni

[27]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., 37.
[28]Per conoscere i firmatari del Memorandum d'intesa sulla vendita di merci contraffatte su Internet, si veda: *https://ec.europa.eu/docsroom/documents/47395/attachments/1/translations/en/renditions/native*
[29]MEMORANDUM OF UNDERSTANDING ON THE SALE OF COUNTERFEIT GOODS ON THE INTERNET, 2011.
[30]Le misure di *notice-and-takedown* consentono, al titolare del diritto di proprietà intellettuale o dei diritti connessi, di segnalare alla piattaforma digitale l'esistenza di un contenuto in violazione di tali diritti (*notice*). A seguito di tale segnalazione, la piattaforma interessata, svolte le opportune verifiche, potrà decidere se rimuovere (*takedown*) o meno il contenuto segnalato, dandone opportuna giustificazione. Cfr. para 15, 16 e 17 Memorandum of understanding on the sale of counterfeit goods on the internetPer un approfondimento sulle misure *notice and take-down*, si rimanda al Capitolo III.
[31]MEMORANDUM OF UNDERSTANDING ON THE SALE OF COUNTERFEIT GOODS ON THE INTERNET, 2016, 4 s.

contraffatti.[32] Il MoU I è stato emendato nel giugno del 2016 per includere degli indicatori chiave di prestazione[33] (c.d. "*key performance indicators*", «KPIs») al fine di monitorare e misurare il successo del protocollo e, nel novembre del 2017, la Commissione ha pubblicato una panoramica sul funzionamento del *Memorandum*; la panoramica conclude il periodo di valutazione durante il quale sono stati misurati i progressi compiuti nel primo anno di lavoro del MoU emendato.

I risultati del lavoro svolto nell'ambito del MoU I sembrerebbero essere positivi: questi hanno dimostrato che il Memorandum ha contribuito efficacemente alla rimozione dei prodotti contraffatti dai mercati online.[34]

La Commissione Europea ha pubblicato finora tre relazioni sull'attuazione del MoU I;[35] l'ultimo rapporto del 2020 mostra che il Memorandum è uno strumento utile ed efficiente per contrastare la vendita di merci contraffatte su Internet e che «la cooperazione volontaria può fornire la flessibilità necessaria per discutere e fornire soluzioni efficaci».[36]

Il più grande vantaggio percepito del MoU I è il suo funzionamento come «laboratorio» in cui i firmatari possono «scambiare esempi pratici di misure proattive e preventive, procedure di *notice-and-takedown* e modi per condividere informazioni, ad esempio sui trasgressori recidivi».[37]

Tuttavia, alcuni firmatari hanno espresso riserve sull'impatto di tale strumento: un ampio gruppo di imprese ha infatti sottolineato che molte offerte di

---

[32]Cfr. para 28,29,30 Memorandum of understanding on the sale of counterfeit goods on the internet.
[33]In economia aziendale un indicatore chiave di prestazione (KPI – *Key Performance Indicators*) è un valore misurabile che dimostra l'efficacia con cui un'azienda sta raggiungendo gli obiettivi aziendali principali. Per un approfondimento si veda: *https://strategiedigitali.net/kpi-aziendali-definizione-significato-ed-esempi/#:~:text=Un%20indicatore%20chiave%20di%20prestazione%20(KPI%20%E2%80%93%20Key%20Performance%20Indicators),raggiungendo%20gli%20obiettivi%20aziendali%20principali*.
[34]Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit good via the internet, 2017.
[35]Cfr. Report from the Commission to the European Parliament and the Council on the Functioning of the Memorandum of Understanding on the sale of Counterfeit Goods via the Internet (2013); Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit good via the internet (2017); Report on the functioning of the Memorandum of Understanding on the sale of Counterfeit Goods on the internet (2020).
[36]Report on the functioning of the Memorandum of Understanding on the sale of Counterfeit Goods, cit., 37 (2020).
[37]Report on the functioning of the Memorandum of Understanding on the sale of Counterfeit Goods, cit., 38 (2020).

merci contraffatte sono ancora disponibili sui mercati online. Gli stessi poi ritengono che la cooperazione e lo scambio di informazioni con le piattaforme online non siano in linea con gli impegni assunti con il MoU I; sono state inoltre sollevate serie preoccupazioni sui benefici degli esercizi di raccolta dei dati KPIs. Nel gennaio 2020, tre imprese firmatarie, che operano nei settori della moda e dei beni di lusso, hanno deciso di ritirarsi dal Memorandum, in quanto ritenevano che i progressi non fossero stati sufficienti e che il livello delle offerte contraffatte presenti sui mercati digitali fosse ancora troppo elevato.

Per quanto riguarda gli esercizi di raccolta dei dati, in particolare, i firmatari hanno messo in dubbio l'utilità di confrontare direttamente i dati quantitativi forniti attraverso le finestre KPI, vista la dinamica dell'esercizio di raccolta, le differenze metodologiche e la mancanza di un *audit* affidabile.

Tuttavia, la maggioranza dei firmatari ha concordato sull'utilità di continuare a raccogliere dati, purché sia più facile, più trasparente e meno dispendioso in termini di risorse. Inoltre, i firmatari hanno ritenuto importante promuovere dialoghi «qualitativi» con particolare attenzione, ad esempio, alle nuove tendenze e ai risultati dei progetti pilota.[38]

Nel complesso, si può concludere che, sebbene il MoU I abbia fornito alcuni vantaggi, la sua efficacia – non entusiasmante – risente del basso numero di piattaforme online firmatarie e del loro scarso coinvolgimento; per tali motivi alcuni ritengono che, in futuro, più che concentrarsi su modifiche del testo del MoU I, sarebbe opportuno ragionare su come attirare un maggior grado di coinvolgimento e azione e delle piattaforme digitali e delle imprese.[39]

Se il MoU è principalmente rivolto a proteggere il titolare del marchio da sfruttamenti abusivi dei suoi diritti, non mancano altrettanti interventi di *soft law* volti a proteggere i titolari del diritto d'autore dalla potenziale diffusione, nel mercato online, di opere protette.

In particolare, uno dei maggiori problemi nella rimozione di contenuti online generati in violazione del diritto d'autore è rappresentato da siti *web* che offrono gratuitamente materiale protetto da diritto d'autore (ad esempio, libri, film,

[38]Report on the functioning of the Memorandum of Understanding on the sale of Counterfeit Goods, cit., 38 (2020).
[39]EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit., 41.

musica). La gratuità del servizio è resa possibile dalla vendita di spazi pubblicitari agli inserzionisti, disposti a pagare elevate somme di denaro in ragione dell'alto traffico generato dalla possibilità, per gli utenti, di usufruire di contenuti protetti senza pagarne il relativo prezzo.[40]

Al fine di fornire una risposta al problema in questione, le iniziative più recenti mirano a prosciugare i flussi di entrate pubblicitarie digitali di questi siti web, secondo l'approccio "*follow the money*"; in particolare, nel 2018,[41] sotto la guida dell'Unione Europea, un gruppo formato da inserzionisti, agenzie pubblicitarie, piattaforme pubblicitarie, editori e titolari di diritti di proprietà intellettuale[42] ha firmato il *Memorandum of Understanding on online advertising and intellectual property rights* (Memorandum d'intesa sulla pubblicità online e i diritti di proprietà intellettuale, «MoU II»)[43] per ridurre al minimo l'inserimento di pubblicità su siti web e applicazioni mobili in cui sono presenti, tra gli altri, contenuti che violano il diritto d'autore.

Inoltre, il MoU II stabilisce obblighi particolari per gli intermediari pubblicitari,[44] imponendo loro di (i) assicurarsi che i loro termini contrattuali consentano l'uso di strumenti per la verifica dei contenuti, l'invio di pubblicità e la rendicontazione, in modo che la pubblicità non venga inserita in siti web che violano i diritti di proprietà intellettuale; (ii) adottare misure ragionevoli per la rimozione di tali annunci una volta identificati; (iii) adottare politiche sui diritti di proprietà intellettuale che descrivano lo strumento e le misure adottate per conformarsi al MoU II; (iv) riferire annualmente alla Commissione e agli altri firmatari sulle misure intraprese per conformarsi al MoU II e sulla loro efficacia.

---

[40]Cfr. EUIPO, *Digital Advertising*, cit., 5.

[41]Per un *excursus* su ogni report del Memorandum, si veda: *https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property rights/memorandum-understanding-online-advertising-and-ipr_en#:~:text=The%20Memorandum%20of%20understanding%20on,copyright%20or%20disseminate%20counterfeit%20goods*.

[42]Per un approfondimento sui firmatari del Memorandum d'intesa sulla pubblicità online e i diritti di proprietà intellettuale, si veda: *https://ec.europa.eu/docsroom/documents/53618/attachments/1/translations/en/renditions/native*

[43]Il Memorandum d'intesa non è giuridicamente vincolante e non crea alcuna responsabilità contrattuale o precontrattuale, né alcun diritto o obbligo, sebbene i firmatari si impegnino a intraprendere le azioni previste dal Protocollo. La «sanzione» in caso di inadempienza è l'espulsione o, come recita il Protocollo d'intesa, «l'invito a ritirarsi» dal Protocollo stesso.

[44]Essi sono definiti dal MoU come «firmatari direttamente coinvolti nell'acquisto, nella vendita o nell'intermediazione della vendita o dell'acquisto di spazi pubblicitari. Si veda, MEMORANDUM OF UNDERSTANDING ON ONLINE ADVERTISING AND INTELLECTUAL PROPERTY RIGHTS, cit., 3.

Nell'agosto 2020 la Commissione ha pubblicato la prima relazione sull'attuazione del MoU II[45] da cui risulta che: (i) i firmatari hanno convenuto che il MoU II promuove le buone prassi e funziona in modo soddisfacente grazie all'impegno dei partecipanti;[46] (ii) la quota di pubblicità delle imprese europee sui siti web che violano i diritti di proprietà intellettuale è diminuita del 12% e la pubblicità dei grandi marchi è scesa dal 62% al 50% nel settore del gioco d'azzardo– sono state inoltre individuate tendenze al ribasso relative ai grandi marchi e agli intermediari pubblicitari dell'UE;[47] (iii) i firmatari ritengono che non vi sia alcuna necessità apparente di modificare il testo del MoU II;[48] (iv) la condivisione di competenze, il rafforzamento della cooperazione con le autorità pubbliche e la sensibilizzazione a livello nazionale, dell'UE e internazionale sono considerate fondamentali per diffondere le buone prassi e facilitare l'adesione al MoU II.[49]

Con l'analisi dei due *Memorandum* si conclude la disamina degli interventi di *soft law* adottati dall'UE per fronteggiare le violazioni dei diritti di proprietà intellettuale commesse tramite (o dal)le piattaforme digitali.

1.1. La Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, recepita dal d.lgs. n. 68 del 2003.

Appena un anno dopo l'emanazione della Direttiva 2000/31/EC– c.d. "*E-commerce Directive*", che verrà esaminata nel Capitolo III, la quale disciplina per la prima volta la responsabilità degli ISP in relazione ai contenuti illeciti generati dagli utenti (c.d. "*user generated content*")–, il legislatore comunitario ha emanato un'ulteriore direttiva – la Direttiva 2001/29/CE –, per realizzare «[u]n quadro giuridico armonizzato in materia di diritto d'autore e di diritti connessi, creando una maggiore certezza del diritto e prevedendo un elevato livello di protezione della proprietà intellettuale»,[50] al fine di promuovere «notevoli investimenti in attività creatrici ed innovatrici, segnatamente nelle infrastrutture delle reti, e di

[45]Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights.
[46]Report on the functioning of the Memorandum of Understanding on online advertising, cit., 14.
[47]Report on the functioning of the Memorandum of Understanding on online advertising, cit., 14.
[48]Report on the functioning of the Memorandum of Understanding on online advertising, cit., 14.
[49]Report on the functioning of the Memorandum of Understanding on online advertising, cit., 14.
[50]Considerando (4) della Direttiva 2001/29/CE.

conseguenza una crescita e una maggiore competitività dell'industria europea per quanto riguarda sia la fornitura di contenuti che le tecnologie dell'informazione».[51]

Per quanto riguarda l'oggetto della Direttiva, l'obiettivo generale era quello di adattare la legislazione sul diritto d'autore alle nuove tecnologie, in particolare a Internet, e di attuare gli obblighi internazionali derivanti da due trattati dell'OMPI (o WIPO):[52] il trattato dell'OMPI sul diritto d'autore (WCT)[53] e il trattato dell'OMPI sulle performance e fonogrammi (WPTT).[54]

I diritti connessi al diritto d'autore presi in considerazione dalla Direttiva sono tre: (I) diritto di riproduzione,[55] (II) diritto di comunicazione al pubblico,[56] (III) diritto di distribuzione,[57] e il minimo comune denominatore disciplinato dalla Direttiva con riferimento a tali diritti– nonostante le eccezioni previste dall'articolo 5–[58] è che gli Stati Membri devono riconoscere ai titolari degli stessi il diritto esclusivo di autorizzare o vietare la riproduzione «diretta o indiretta, temporanea o permanente, in qualunque modo o forma, in tutto o in parte»,[59] la comunicazione al pubblico «su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente»[60] e la distribuzione al «pubblico dell'originale delle loro opere o di loro copie, attraverso la vendita o in altro modo».[61] Con riferimento a cosa debba intendersi per «comunicazione al pubblico», bisogna sottolineare come la Corte di Giustizia dell'Unione Europea, nella causa C-610/15,[62] rispondendo alla prima questione pregiudiziale sollevata

[51] Considerando (4) della Direttiva 2001/29/CE.
[52]FALLENBÖCK, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions*, in International Journal of Communications Law and Policy, 2003, 34.
[53]WIPO Copyright Treaty, 1996.
[54]WIPO Performances and Phonograms Treaty, 1996.
[55]Art. 2 Direttiva 2001/29/CE, art. 1 d.lgs. n. 68 del 2003 che sostituisce l'art. 13 della l. n. 633 del 1941.
[56]Art. 3 Direttiva 2001/29/CE; art. 2 d.lgs. n. 68 del 2003 che sostituisce l'art. 16 della l. n. 633 del 1941.
[57]Art. 4 Direttiva 2001/29/CE; art. 3 d.lgs. n. 68 del 2003 che sostituisce l'art. 17 della l. n. 633 del 1941.
[58]Per un approfondimento sulle eccezioni previste dall'articolo 5 cfr. FALLENBÖCK, *On the Technical Protection of Copyright*, cit., 42 s.
[59]Art. 2 Direttiva 2001/29/CE.
[60]Art. 3 Direttiva 2001/29/CE.
[61]Art. 4 Direttiva 2001/29/CE.
[62]Cfr. CGUE, 14 giugno 2017, *Stichting Brein v. Ziggo BV*, causa C-610/15.

dalla *Hoge Raad der Nederlanden* (Corte suprema dei Paesi Bassi, giudice del rinvio) ha individuato «svariati criteri complementari, di natura non autonoma e interdipendenti fra loro»[63] in presenza dei quali la condotta di «comunicazione al pubblico» può ritenersi presente. Ci si riferisce a: (I) il ruolo imprescindibile dell'utente e il carattere intenzionale del suo intervento,[64] (II) la rilevanza del numero di destinatari potenziali,[65] (III) le modalità tecniche di comunicazione,[66] ed infine (IV) il carattere lucrativo della comunicazione.[67]

Inoltre, la Corte ha ritenuto i gestori della piattaforma «The Pirate Bay» direttamente responsabili in quanto, nonostante le opere protette fossero diffuse dagli *user* della piattaforma e non dai suoi gestori, questi ultimi «intervengono con piena cognizione delle conseguenze del proprio comportamento, al fine di dare accesso alle opere protette, indicizzando ed elencando su tale piattaforma i file torrent che consentono agli utenti della medesima di localizzare tali opere e di condividerle nell'ambito di una rete tra utenti (peer-to-peer)»[68], aggiungendo come «senza la messa a disposizione e la gestione da parte dei suddetti amministratori di una siffatta piattaforma, le opere in questione non potrebbero essere condivise dagli utenti o, quantomeno, la loro condivisione su Internet sarebbe più complessa».[69]

Proprio da quest'ultimo passaggio è possibile notare come la Corte valorizzi il «ruolo imprescindibile [dei gestori della piattaforma] nella messa a disposizione delle opere in questione»[70], con la conseguenza che l'imprescindibilità può anche derivare dal grado di facilità con cui le opere si reperiscono sul *web*.[71] In presenza di tali condizioni sembra dunque potersi affermare un regimen di diretta responsabilità « non solo dell'utente che commette l'illecito, ma anche del gestore

[63]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 25.
[64]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 26.
[65]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 27.
[66]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 28: «un'opera protetta, per essere qualificata come «comunicazione al pubblico», deve essere comunicata secondo modalità tecniche specifiche, diverse da quelle fino ad allora utilizzate o, in mancanza, deve essere rivolta ad un «pubblico nuovo», vale a dire a un pubblico che non sia già stato preso in considerazione dai titolari del diritto d'autore nel momento in cui hanno autorizzato la comunicazione iniziale della loro opera al pubblico».
[67]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 29.
[68]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 36.
[69]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 36.
[70]Cfr. CGUE, 14 giugno 2017, *Stichting Brein*, già citata, para. 37.
[71]SCALZINI, *Hyperlinking e violazione del diritto d'autore nell'evoluzione giurisprudenziale europea*, in *Analisi giuridica dell'economia*, 2, 2017, 657.

del *provider*,[72] che si contrappone al regime di «responsabilità secondaria» che si avrà modo di analizzare nel Capitolo III.

Procedendo poi con l'analisi del capo III rubricato «tutela delle misure tecnologiche e delle informazioni sul regime dei diritti», il legislatore comunitario dimostra di aver scorto le potenzialità della società dell'informazione, ma di non essere ancora pienamente al corrente delle potenziali minacce presenti sul web in quanto solo uno è l'articolo che si (pre)occupa delle violazioni del diritto d'autore commesse per il tramite di un intermediario –[73] motivo per cui tale direttiva sarà modificata dalla Direttiva (UE) 2019/790, per il cui approfondimento si rinvia al Capitolo III.

Così, l'articolo 6 della Direttiva 2001/29/CE tenta di rafforzare l'efficacia delle misure di protezione, rendendo illegale l'elusione delle stesse.[74] In particolare, il disposto impone agli Stati membri di prevedere adeguata protezione contro l'elusione di efficaci misure tecnologiche eventualmente apposte dal titolare del diritto d'autore; elusione effettuata da persone «consapevoli, o che si possano ragionevolmente presumere consapevoli, di perseguire tale obiettivo».[75]

Sempre lo stesso articolo, al paragrafo 2, impone il medesimo obbligo di protezione contro «la fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio, la pubblicità per la vendita o il noleggio o la detenzione a scopi commerciali di attrezzature, prodotti o componenti o la prestazione di servizi", che abbiano la finalità di eludere o facilitare l'elusione di misure tecnologiche, per tali dovendosi intendere "tutte le tecnologie, i dispositivi o componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti, su opere o altri materiali protetti, non autorizzati dal titolare del diritto d'autore o del diritto connesso al diritto d'autore, così come previsto dalla legge o dal diritto *sui generis* previsto al capitolo III della direttiva 96/9/CE».[76]

---

[72]SCALZINI, *Hyperlinking e violazione del diritto d'autore*, cit., 658.
[73]Ci si riferisce, in particolare, all'art. 8 para. 3 della Direttiva 2001/29/CE la quale chiede agli Stati membri di assicurarsi «che i titolari dei diritti possano chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto d'autore o diritti connessi».
[74]FALLENBÖCK, *On the Technical Protection of Copyright*, cit., 7.
[75]Art. 6 Direttiva 2001/29/CE.
[76]Art. 6, para. 3, Direttiva 2001/29/CE.

Tali misure sono considerate «efficaci» se «l'uso dell'opera o di altro materiale protetto sia controllato dai titolari tramite l'applicazione di un controllo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o di altro materiale protetto, o di un meccanismo di controllo delle copie, che realizza l'obiettivo di protezione».[77]

L'articolo 7 della Direttiva in disamina, poi, impone agli Stati membri di prevedere un'adeguata protezione giuridica contro chiunque, senza averne diritto, compia consapevolmente gli atti di (I) «rimuovere o alterare qualsiasi informazione elettronica sul regime dei diritti»;[78] o di «distribuire, importare a fini di distribuzione, diffondere per radio o televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti ai sensi della presente direttiva o del capitolo III della direttiva 96/9/CE, dalle quali siano state rimosse o alterate senza averne diritto le informazioni elettroniche sul regime dei diritti»,[79] qualora l'agente sia consapevole, o si possa ragionevolmente presumere che sia consapevole, che con essi «induce, rende possibile, agevola o dissimula una violazione di diritti d'autore o diritti connessi previsti dalla legge o del diritto sui generis di cui al capitolo III della direttiva 96/9/CE».

Per «informazioni sul regime dei diritti» s'intende, ai sensi del paragrafo 2 dell'articolo 7, «qualunque informazione fornita dai titolari dei diritti che identifichi l'opera o i materiali protetti di cui alla presente direttiva o coperti dal diritto sui generis di cui al capitolo III della direttiva 96/9/CE, l'autore o qualsiasi altro titolare dei diritti, o qualunque informazione circa i termini e le condizioni di uso dell'opera o di altri materiali nonché qualunque numero o codice che rappresenti tali informazioni».

Infine, si conclude l'esame della Direttiva con l'articolo più rilevante, seppur molto generale, rispetto all'oggetto di tale elaborato: l'articolo 8 (3) infatti impone agli Stati Membri di assicurarsi che «i titolari dei diritti possano chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto d'autore o diritti connessi».

[77] Art. 6, para. 3, Direttiva 2001/29/CE.
[78] Art. 7 lett. a) Direttiva 2001/29/CE.
[79] Art. 7 lett. b) Direttiva 2001/29/CE.

Tale Direttiva è stata recepita nel nostro ordinamento per via del d.lgs. n. 68 del 2003, che, nel recepire gli articoli 2, 3, 4 della Direttiva 2001/29/CE, ha, sostanzialmente, sostituito gli articoli 13, 16, 17 della legge n. 633 del 1941.[80]

Nella ricezione degli articoli 6 e 7 della Direttiva, il d.lgs. n. 68 del 2003 ha poi introdotto gli articoli 102-*quater* e 102-*quinquies* nella legge n. 633 del 1941.[81]

Infine, per ciò che riguarda l'articolo 8 (3), l'articolo 24 del d.lgs. in disamina sostituisce l'articolo 163 della legge 633 del 1941, secondo cui «il titolare di un diritto di utilizzazione economica può chiedere che sia disposta l'inibitoria di

[80]Art. 13 l. n. 633 del 1941: «Il diritto esclusivo di riprodurre ha per oggetto la moltiplicazione in copie diretta o indiretta, temporanea o permanente, in tutto o in parte dell'opera, in qualunque modo o forma, come la copiatura a mano, la stampa, la litografia, l'incisione, la fotografia, la fonografia, la cinematografia ed ogni altro procedimento di riproduzione». Art. 16 l. n. 633 del 1941: «1. Il diritto esclusivo di comunicazione al pubblico su filo o senza filo dell'opera ha per oggetto l'impiego di uno dei mezzi di diffusione a distanza, quali il telegrafo, il telefono, la radio, la televisione ed altri mezzi analoghi e comprende la comunicazione al pubblico via satellite, la ritrasmissione via cavo, nonché le comunicazioni al pubblico codificate con condizioni particolari di accesso; comprende, altresì, la messa a disposizione del pubblico dell'opera in maniera che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente. 2. Il diritto di cui al comma 1 non si esaurisce con alcun atto di comunicazione al pubblico, ivi compresi gli atti di messa a disposizione del pubblico». Art. 17 l. n. 633 del 1941: «1. Il diritto esclusivo di distribuzione ha per oggetto la messa in commercio o in circolazione, o comunque a disposizione, del pubblico, con qualsiasi mezzo ed a qualsiasi titolo, dell'originale dell'opera o degli esemplari di essa e comprende, altresì, il diritto esclusivo di introdurre nel territorio degli Stati della Comunità europea, a fini di distribuzione, le riproduzioni fatte negli Stati extracomunitari. 2. Il diritto di distribuzione dell'originale o di copie dell'opera non si esaurisce nella Comunità europea, se non nel caso in cui la prima vendita o il primo atto di trasferimento della proprietà nella Comunità sia effettuato dal titolare del diritto o con il suo consenso. 3. Quanto disposto dal comma 2 non si applica alla messa a disposizione del pubblico di opere in modo che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente, anche nel caso in cui sia consentita la realizzazione di copie dell'opera. 4. Ai fini dell'esaurimento di cui al comma 2, non costituisce esercizio del diritto esclusivo di distribuzione la consegna gratuita di esemplari delle opere, effettuata o consentita dal titolare a fini promozionali, ovvero di insegnamento o di ricerca scientifica».

[81]Art. 102-*quater* l. n. 633 del 1941: «1. I titolari di diritti d'autore e di diritti connessi nonché del diritto di cui all'art. 102-bis, comma 3, possono apporre sulle opere o sui materiali protetti misure tecnologiche di protezione efficaci che comprendono tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti. 2. Le misure tecnologiche di protezione sono considerate efficaci nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o del materiale protetto, ovvero sia limitato mediante un meccanismo di controllo delle copie che realizzi l'obiettivo di protezione. 3. Resta salva l'applicazione delle disposizioni relative ai programmi per elaboratore di cui al capo IV sezione VI del titolo I». Art. 102-*quinquies* l. n. 633 del 1941: «1. Informazioni elettroniche sul regime dei diritti possono essere inserite dai titolari di diritti d'autore e di diritti connessi nonché del diritto di cui all'art. 102-bis, comma 3, sulle opere o sui materiali protetti o possono essere fatte apparire nella comunicazione al pubblico degli stessi. 2. Le informazioni elettroniche sul regime dei diritti identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti. Tali informazioni possono altresì contenere indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali, nonché qualunque numero o codice che rappresenti le informazioni stesse o altri elementi di identificazione».

qualsiasi attività che costituisca violazione del diritto stesso, secondo le norme del codice di procedura civile concernenti i procedimenti cautelari». Tale articolo, tuttavia, non contiene nessun riferimento all'«intermediario», come invece richiesto dall'articolo 8 (3) della Direttiva; sarà solo con l'attuazione della Direttiva 2004/48/CE, che ci si accinge ad esaminare nel prossimo paragrafo, che il legislatore porrà rimedio a tale errore.[82]

1.2. La Direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale.

Se con la Direttiva 2001/29/CE il legislatore comunitario aveva scorto solo in parte i pericoli che Internet poteva cagionare sulla protezione del diritto d'autore e diritti connessi – andando a prevedere adeguate tutele per le misure tecnologiche di protezione –, poco tempo più tardi lo stesso legislatore sembra assumere maggiore consapevolezza della pericolosità del *web* non solo riguardo al diritto d'autore, bensì alla più generale categoria dei diritti di proprietà intellettuale.

Per tale motivo, tre anni dopo l'emanazione della Direttiva 2001/29/CE, il legislatore comunitario decide di migliorare ulteriormente la protezione di tali diritti contro le minacce di Internet attraverso la Direttiva 2004/48/CE (c.d. "Direttiva *IPRED*"), volta a mitigare il rischio che «in assenza di misure efficaci che assicurino il rispetto dei diritti di proprietà intellettuale, l'innovazione e la creazione [possano essere] scoraggiate, e gli investimenti, [contratti]".[83]

In particolare, tale Direttiva viene emanata nell'ambito della strategia della Commissione, dettagliata da una comunicazione nell'anno 2000,[84] per il miglioramento e l'intensificazione della lotta alla contraffazione e alla pirateria nel mercato unico.[85]

Era infatti «necessario assicurare che il diritto sostanziale in materia di proprietà intellettuale, [allora come oggi] ampiamente parte dell'acquis comunitario, [fosse] effettivamente applicato nella Comunità».[86] In proposito, è

[82]Ci si riferisce all'articolo 10 del d.lgs. n. 140 del 2006 il quale, recependo l'articolo 9 (1) (a) della Direttiva 2004/48/CE, modifica l'articolo 163 della l. n. 633 del 1941 inserendo il riferimento all'intermediario.
[83]Considerando (3) Direttiva 2004/48/CE.
[84]Comunicazione della Commissione, del 30 novembre 2000, sul seguito da dare al Libro verde sulla lotta alla contraffazione e alla pirateria nel mercato interno.
[85]SVENSSON, LARSON, *Social Norms and Intellectual Property, Online norms and European Legal Development*, in *Research Report in Sociology of Law*, Vol. 1, 2009, 17.
[86]Considerando (3) Direttiva 2004/48/CE.

evidente come «gli strumenti per assicurare il rispetto dei diritti di proprietà intellettuale rivestono un'importanza capitale per il successo del mercato interno».[87]

Per tale motivo l'articolo 9 (1) (a) della Direttiva 2004/48/CE ha previsto, coerentemente con l'articolo 8 (3) della Direttiva 2001/29/CE, che le competenti autorità giudiziarie possano, su richiesta dell'attore, emettere nei confronti di un intermediario, i cui servizi sono utilizzati da terzi per violare un diritto di proprietà intellettuale, «un'ingiunzione interlocutoria volta a prevenire qualsiasi violazione imminente di un diritto di proprietà intellettuale, o a vietare, a titolo provvisorio e, imponendo se del caso il pagamento di una pena pecuniaria suscettibile di essere reiterata, ove sia previsto dalla legislazione nazionale, il proseguimento di asserite violazioni di tale diritto, o a subordinare l'azione alla costituzione di garanzie finalizzate ad assicurare il risarcimento del titolare». Tali misure provvisorie risultano essere essenziali per una tutela efficace in favore dei titolari dei diritti, poiché in caso di violazione è essenziale agire rapidamente, soprattutto nel caso in cui vi sia di mezzo un prestatore di servizi della società dell'informazione.[88]

Tale Direttiva è stata recepita dal legislatore italiano tramite il decreto legislativo n. 140 del 2006,[89] il quale, tra le altre cose,[90] rimedia all'errore commesso dal legislatore nel 2003, come si accennava, inserendo all'articolo 163 della legge n. 633 del 1941 il riferimento all'intermediario;[91] in particolare, oggi l'articolo 163 prevede che «il titolare di un diritto di utilizzazione economica può chiedere che sia disposta l'inibitoria di qualsiasi attività, *ivi comprese quelle costituenti servizi prestati da intermediari*, che costituisca violazione del diritto stesso secondo le norme del codice di procedura civile concernenti i procedimenti cautelari».

[87]Considerando (3) Direttiva 2004/48/CE.
[88]ALMBORG, *Counterfeiting and Piracy, From a right holders perspective*, 16.
[89]Decreto Legislativo n. 140 del 2006, «Attuazione della direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale».
[90]Il d. lgs.n. 140 del 2006 modifica varie norme nell'ottica di recepire il disposto dell'articolo 9 (1) (a) della Direttiva. Cfr. art. 2 d. lgs.n. 140 del 2006 che sostituisce l'articolo 156 della l. n. 633 del 1941, art. 16 d. lgs.n. 140 del 2006 che modifica l'articolo 124 della d. lgs. n. 30 del 2005, art. 19 d. lgs.n. 140 del 2006 che modifica l'articolo 131 della d. lgs. n. 30 del 2005.
[91]Art. 10 d. lgs. n. 140 del 2006.

La valutazione della Direttiva IPRED effettuata dalla, allora, Comunità Europea, ha evidenziato che «a livello nazionale vengono utilizzate nozioni diverse di 'intermediario'».[92]

In risposta a ciò, l'allora CE ha emanato specifiche linee guida sull'interpretazione della Direttiva *IPRED*, chiarendo che qualsiasi operatore economico che fornisca servizi in grado di essere utilizzati da altre persone per violare i diritti di proprietà intellettuale può rientrare nell'ambito della nozione di intermediario dell'IPRED.[93]

Pertanto, le piattaforme online, come i *marketplace online* e le piattaforme di *social network*, rientrano nella nozione di intermediario e possono essere potenzialmente soggetti a ingiunzioni emesse dalle competenti autorità giudiziarie, su richiesta dell'attore.[94]

È bene sottolineare come le ingiunzioni contro le piattaforme/intermediari online possono essere emesse dall'autorità giudiziaria a prescindere dall'esistenza di una sentenza che ne accerta la responsabilità, con la conseguenza che possono essere emesse anche contro un intermediario innocente.[95]

Ciò risulta coerente con la disposizione di cui all'articolo 14 (3) della *E-commerce Directive*, che si avrà modo di analizzare nel prossimo Capitolo, secondo cui l'esenzione di responsabilità applicabile agli *hosting providers* non esclude la possibilità delle autorità di richiedere comunque la cessazione o la prevenzione della violazione allo stesso provider.

---

[92]EUROPEAN COMMISSION, Commission staff Working Document. Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, 12 e 21.

[93]EUROPEAN COMMISSION, Commission staff Working Document. Guidance on certain aspects of Directive 2004/48/EC, cit., 13.

[94]Cfr. CGUE, 12 luglio 2011, *L'Oréal e Altri v eBay*, causa C- 324/09, para. 131. Nello stesso senso CGUE, 16 febbraio 2012, *Sabam v. Netlog*, C-360-10, para. 28: «Occorre altresì rammentare che, secondo gli articoli 8, paragrafo 3, della direttiva 2001/29 e 11, terza frase, della direttiva 2004/48, i titolari di diritti di proprietà intellettuale possono chiedere un provvedimento inibitorio nei confronti dei gestori di piattaforme di reti sociali in linea, come la Netlog, che agiscono in qualità di intermediari ai sensi delle suddette disposizioni, dato che i loro servizi possono essere utilizzati dagli utenti di simili piattaforme per violare i diritti di proprietà intellettuale».

[95]Cfr. CGUE, 12 luglio 2011, *L'Oréal*, già citata, para 127.

Tuttavia, tali ingiunzioni non possono equivalere a un obbligo generale di sorveglianza, poiché contrasterebbe con l'articolo 15 della E-commerce Directive, come chiarito dalla CGUE nel caso Sabam.[96]

Ancora, con riferimento all'ingiunzione di rimozione, una questione spinosa riguardante tale istituto, che sembra aver trovato soluzione, riguardava l'efficacia dell'ingiunzione di rimozione del contenuto illecito dal *provider*: ci si chiedeva, invero, se tale ingiunzione di rimozione a carico dell'ISP avesse efficacia anche nei confronti di altri *providers* che ospitavano lo stesso contenuto illecito o se la parte presumibilmente lesa avrebbe dovuto presentare un'altra istanza di rimozione.[97]

Su tale interrogativo si è pronunciato il Tribunale di Torino, con ordinanza del 2 Giugno 2015, con la quale è stato stabilito che «quando il titolare di un diritto d'autore abbia indicato ad un *hosting provider* che il contenuto di un Url vìola i suoi diritti e l'ISP lo abbia rimosso, il medesimo ISP ha un obbligo generale di rimuovere il medesimo contenuto quando questo venga rimesso in linea in tutto o in parte, senza che il titolare dei diritti abbia un onere di riavviare il procedimento della diffida previa: e la relativa responsabilità dell'ISP nei confronti del titolare è quella c.d. del contatto sociale e dei corrispondenti obblighi di protezione dei diritti altrui».[98]

Nello stesso senso si è pronunciato il Tribunale di Milano, con ordinanza del 12 aprile 2018, che ha stabilito come, a seguito di un'ingiunzione pronunciata dal giudice, i *providers* coinvolti nel relativo procedimento giudiziario siano tenuti, *pro-futuro*, ad attivarsi per limitare l'accesso al materiale illecito oggetto del procedimento anche se presenti in pagine o siti internet diversi da quelli colpiti

[96]CGUE, 16 febbraio 2012, *Sabam*, già citata, para 33-34: «33. Di conseguenza, le medesime norme devono rispettare, segnatamente, l'articolo 15, paragrafo 1, della direttiva 2000/31, che vieta alle autorità nazionali di adottare misure che impongano ad un prestatore di servizi di hosting di procedere ad una sorveglianza generalizzata sulle informazioni che esso memorizza (v., per analogia, sentenza Scarlet Extended, cit., punto 35). 34. A questo riguardo, la Corte ha già dichiarato che siffatto divieto abbraccia, in particolare, le misure nazionali che obblighino un prestatore intermedio, come un prestatore di servizi di hosting, a realizzare una sorveglianza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale. Peraltro, un siffatto obbligo di sorveglianza generale sarebbe incompatibile con l'articolo 3 della direttiva 2004/48, il quale enuncia che le misure contemplate da detta direttiva devono essere eque, proporzionate e non eccessivamente costose (v. sentenza Scarlet Extended, cit., punto 36)»

[97]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei providers di Internet nell'incerta giurisprudenza europea*, in *Il Foro Italiano*, 6, 2019, 2076.

[98]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee*, cit., 2076.

dall'ingiunzione di rimozione.[99] Ciò è stato considerato coerente con l'istituto della c.d. "ingiunzione dinamica".[100]

Infine, rimanendo in tema di misure cautelari, è degna di nota la pronuncia della Suprema Corte nel caso *The Pirate Bay* –[101] già citato – secondo la quale è legittimo il provvedimento con cui il g.i.p. disponga il sequestro preventivo del sito Internet qualora il suo gestore concorra nel reato di diffusione illecita di materiale protetto dal diritto d'autore ex articolo 171-*ter* comma 2, lett. a-*bis*).[102]

Si può così ritenere concluso questo secondo capitolo, il quale ha descritto in linea generale come il legislatore comunitario, e successivamente quello italiano, hanno aumentato la tutela dei diritti di proprietà intellettuale a fronte delle opportunità e minacce prospettate dalla digitalizzazione. Il prossimo capitolo si occuperà di analizzare la responsabilità delle piattaforme digitali in caso di pubblicazione di contenuti illeciti – tra cui lo sfruttamento abusivo dei diritti di proprietà intellettuale – generati dagli utenti. Si ripercorreranno dunque le tre tappe comunitarie aventi ad oggetto tale disciplina: la Direttiva 2000/31/EC, la Direttiva (UE) 2019/790– con le relative normative di attuazione – e il Regolamento EU 2022/2065. L'elaborato si concluderà con l'analisi, in ambito nazionale, della disciplina penalistica e civilistica applicabile a tali piattaforme con qualche cenno, infine, comparatistico.

---

[99]Cfr. Trib. Milano, Sez. Specializzata In Materia D'impresa – A –, Ordinanza del 12 aprile 2018: «una volta identificata la condotta ingiunta, ciò basti a rendere il provvedimento cautelare immediatamente esecutivo e a impedire che la condotta così descritta venga reiterata, pena l'applicazione delle misure coercitive su richiesta del creditore, che si assumerà tutte le responsabilità connesse all'allegazione delle violazioni ascritte al debitore. D'altra parte, se fosse imposto l'intervento del giudice per ogni violazione successivamente constatata, nessuna ingiunzione potrebbe essere mai essere emessa pro-futuro, contraddicendo la natura stessa di questa tipologia di condanna, ontologicamente proiettata a impedire la prosecuzione e la reiterazione degli illeciti a venire (in tal senso, si vedano T Milano, ord. 8 maggio 2017)».

[100]La possibilità di ricorrere all'ingiunzione dinamica trova collocazione nella Comunicazione del 29 novembre 2017 della Commissione UE contenente le linee guida per l'interpretazione di determinati aspetti della Direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale.

[101]Cfr. Cass. pen., cit., n. 49437/2009.

[102]Nel caso di specie, la condotta penalmente rilevante di «indicizzazione» è stata quella di aggregare i contenuti: «l'aggregatore di *feed*, detto anche lettore di *feed* o semplicemente aggregatore, è un software o una applicazione web che raccoglie contenuti web in un unico spazio per una consultazione facilitata. Gli aggregatori riducono il tempo e gli sforzi necessari per seguire regolarmente aggiornamenti di un sito web e permettono di creare uno spazio di informazione unico». Così, MERLA, *Diffusione abusiva di opere in internet e sequestro preventivo del sito web: il caso "The Pirate Bay"*, Nota a Cass. sez. III pen. 23 dicembre 2009, n. 49437, in *Il Diritto dell'informazione e dell'informatica*, 3, 2010, 451.

CAPITOLO III

DALLA DIRETTIVA 2000/31/EC AL REGOLAMENTO (UE) 2022/2065: LA RESPONSABILITÀ DELLE PIATTAFORME DIGITALI.

Premessa.

Nel capitolo precedente si è avuto modo di esporre come l'avvento dell'Internet abbia avuto un impatto significativo per la protezione della proprietà intellettuale: numerosi sono stati gli interventi del legislatore comunitario finalizzati a proteggere i titolari di tali diritti. Al contempo, le potenzialità dell'Internet non minacciano solo questa categoria di diritti: ogni diritto, anche quelli fondamentali, è potenzialmente suscettibile di essere leso in rete.

Per tale motivo il legislatore comunitario ha emanato dapprima la Direttiva 2000/31/EC, per poi implementarla tramite la Direttiva (UE) 2019/790 – la quale ha un *focus* specifico sul diritto d'autore – per poi, da ultimo, emanare il Regolamento 2022/2065 per disciplinare diritti e doveri delle piattaforme digitali ogni qualvolta, per loro tramite, sia leso un diritto soggettivo (tra i quali ovviamente vi rientrano i diritti di proprietà intellettuale). Dunque, quest'ultimo capitolo avrà l'obiettivo di passare in rassegna il contenuto delle tre fonti sopracitate, cogliendone differenze e innovazioni. Dopodiché si tenterà di sviluppare il tema della responsabilità delle piattaforme digitali, così definito, in ambito domestico, esaminando applicazioni della disciplina penalistica e civilistica per poi, infine, condurre uno studio comparato. Si badi bene che tali fonti hanno come destinatarie alcune tipologie di «piattaforme digitali» nel senso definito all'inizio del secondo capitolo: ci si riferisce, in particolare, ai «servizi intermediari» e alle «piattaforme online», già citati.

1. La Direttiva 2000/31/EC dell'8 giugno 2000 (c.d. *E-commerce Directive*), recepita dal d.lgs. n. 70 del 2003.

In risposta alla nascita di internet negli anni 90', l'allora Comunità Europea, attraverso la Direttiva 2000/31/EC dell'8 giugno del 2000 (c.d. "Direttiva *E-commerce*" o "*E-commerce Directive*") disciplina, per la prima volta, la responsabilità dei servizi intermediari per i contenuti illegali generati dai propri

utenti o *user*. Il motivo principale sottostante tale regolazione fu il crescere del contenzioso avente come convenuti i «prestatori di servizi della società dell'informazione» – c.d. *Internet Service Provider* ("ISP"), già citati –[1]: le persone danneggiate dal comportamento illegale degli utenti di Internet citarono in giudizio tutti quei prestatori o, *providers,* che non esercitavano un controllo preventivo di legalità sui contenuti pubblicati mediante i servizi da questi offerti.

Ciò ha portato alla questione circa l'attribuzione della responsabilità legale degli ISP. Come anticipato nel corso dei Capitoli precedenti, nonché nell'introduzione all'elaborato, sebbene vi sia un ampio consenso sui benefici dell'innovazione che Internet ha contribuito a portare nelle nostre vite, i problemi che possono derivare dalla pubblicazione di contenuti illegali hanno numerose conseguenze negative per la nostra società ed economia.[2]

Ai fini di tale elaborato, una delle questioni più rilevanti riguarda la diffusione di contenuti illegali, o in quanto contraffatti– e quindi in violazione delle norme sui marchi– o in quanto protetti dal diritto d'autore. Tra le tre *species* del diritto di proprietà intellettuale analizzate nei capitoli precedenti, infatti, marchio e diritto d'autore risultano essere quelli più minacciati dall'avvento di Internet.

Queste nuove sfide e il modo in cui le piattaforme le affrontano hanno un impatto significativo sui diritti fondamentali online. Dunque, l'emanazione della Direttiva sopra citata volta a disciplinare la responsabilità degli ISP aveva come fine il bilanciamento di tre obiettivi: (I) prevenire il danno derivante dalla diffusione di contenuti illegali; (II) proteggere la libertà di espressione e di informazione; e (III) incoraggiare l'innovazione tecnologica e la crescita economica generale.

Ai fine della dissertazione, risulta sufficiente analizzare il capo II, sezione 4, *i.e.* gli articoli 12-15, dell'*E-commerce Directive* i quali disciplinano, in maniera generica, la c.d. *notice and take-down procedure*[3] su un ampio spettro di problemi

[1]Gli artt. 2 Direttiva 2000/31/EC e d.lgs. n. 70 del 2003, definiscono gli ISP come «la persona fisica o giuridica che presta un servizio della società dell'informazione». Un «servizio della società dell'informazione» è un «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»; questa definizione è fornita dall'art. 1, punto 2, della direttiva n. 98/34/CE, come modificata dalla direttiva n. 98/48/CE, nonché dall'art. 1 comma 1 lett. b l. 21 giugno 1986, n. 317, richiamati rispettivamente dalla *E-commerce Directive* e dal d.lgs. n. 70 del 2003 di attuazione.

[2]Cfr. VAN HOBOKEN, KELLER, *Design Principles for Intermediary Liability Laws*, 2019, 2.

[3]La procedura *notice and take-down* consiste nella rimozione di un contenuto da un sito web o da una piattaforma Internet su richiesta del titolare die diritti che si assumono violati. In particolare, si

legali. Infatti, tale procedura si applica per contenuti illegali che spaziano dalla violazione della *privacy* alla violazione della proprietà intellettuale. Ogni contenuto che risulta essere illegale in base al diritto europeo o al diritto interno di ogni singolo Stato Membro dovrà essere soggetto a rimozione da parte della piattaforma digitale che «ospita» tale contenuto.

Come si avrà modo di vedere, la Direttiva in disamina sarà modificata dal Regolamento EU 2022/2065: dunque, d'ora innanzi, nell'esplicazione del suo contenuto, si utilizzerà il tempo passato. La Direttiva divideva i prestatori dei servizi della società dell'informazione in tre categorie, i cui diritti e doveri di ciascuno venivano disciplinati dagli articoli 12, 13 e 14.

L'articolo 12 della Direttiva 2000/31/EC,[4] che disciplinava l'attività dei prestatori di servizi di «semplice trasporto» (o «*mere conduit*»),[5] richiedeva agli Stati membri di provvedere affinché il prestatore di servizi di *mere conduit* non

---

fa riferimento alla procedura adottata dagli Stati Uniti, nel 1998, all'interno del *Digital Millenium Copyright Act* («DMCA»): un meccanismo articolato che si connota per i tempi determinati di attivazione del provider e per l'intervento di diverse figure. Esso attribuisce un ruolo pregnante all'oggetto della contestazione, alla garanzia del contraddittorio tra le diverse parti interessate e al contenuto informativo che debba essere pubblicato dai *providers* nelle proprie pagine web, per assicurare a coloro che assumano essere stati lesi la trasparenza della procedura. Il legislatore europeo non disciplina i dettagli relativa alla procedura nella Direttiva *E-commerce*, lasciando libertà agli stati membri. Tuttavia, come si avrà modo di vedere, il Regolamento EU 2022/2065 introduce una procedura chiara, vincolante per tutti gli stati membri.

[4]Art. 12 Direttiva 2000/31/EC: «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non sia responsabile delle informazioni trasmesse a condizione che egli: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; e c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al paragrafo 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione».

[5]I *mere conduit* sono provider che trasmettono contenuti di terzi su una rete o forniscono accesso alla rete stessa. All'interno dei *mere conduit* rientrano a titolo esemplificativo le compagnie telefoniche che forniscono la connessione a internet agli utenti. Cfr. BELLAN, *Per una reasonable liability: critiche alla responsabilità oggettiva degli internet service provider e tutela dei diritti*, in *Il dir. ind.*, 3, 2012. «A titolo di esempio, i servizi intermediari di semplice trasporto includono categorie generiche di servizi quali i punti di interscambio internet, i punti di accesso senza fili, le reti private virtuali, i risolutori e servizi di DNS, i registri dei nomi di dominio di primo livello, i registrar, le autorità di certificazione che rilasciano certificati digitali, il Voice over IP e altri servizi di comunicazione interpersonale». Così il considerando (29) del Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un Mercato Unico dei Servizi Digitali e che modifica la Direttiva 2000/31/CE (Regolamento sui Servizi Digitali).

fosse considerato responsabile delle informazioni trasmesse a meno che: (I) egli non avesse dato origine alla trasmissione; (II) egli non avesse selezionato il destinatario della trasmissione; e (III) egli non avesse selezionato né modificato le informazioni trasmesse. Dunque, tali condizioni dovevano ricorrere cumulativamente affinché l'ISP si fosse potuto considerare esente da responsabilità. Il comma 3 stabiliva che comunque «Il presente articolo lascia[va] impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione».

L'articolo 13[6] regolava poi diritti e obblighi del prestatore di servizi di «memorizzazione temporanea» («*caching provider*»),[7] prevedendo la loro esenzione da responsabilità qualora (I) non avesse modificato le informazioni; (II) si fosse conformato alle condizioni di accesso alle informazioni; (III) si fosse conformato alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; (IV) non avesse interferito con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel

[6]Art. 13 Direttiva 2000/31/EC: «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore, d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, e e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso. 2. Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione».

[7]I caching provider sono provider che memorizzano in modo automatico, intermedio e temporaneo contenuti di terzi al fine di rendere più efficace il loro successivo inoltro ad altri destinatari, a richiesta degli stessi. «L'attività di memorizzazione è tipica del processo di funzionamento dei motori di ricerca come Google, Bing o Yahoo!». Cfr. BELLAN, *Per una reasonable liability*, cit. «Esempi generici di servizi intermediari di memorizzazione temporanea includono la sola fornitura di reti per la diffusione di contenuti, proxy inversi o proxy di adattamento dei contenuti. Tali servizi sono fondamentali per garantire una trasmissione fluida ed efficiente delle informazioni fornite su internet». Così il considerando (29) del Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un Mercato Unico dei Servizi Digitali e che modifica la Direttiva 2000/31/CE (Regolamento sui Servizi Digitali).

settore per ottenere dati sull'impiego delle informazioni, e (V) avesse agito prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena fosse effettivamente venuto a conoscenza del fatto che le informazioni sono fossero state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni fosse stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne avesse disposto la rimozione o la disabilitazione dell'accesso.

L'articolo 14,[8] regolante l'attività fornita dal prestatore di servizi di «memorizzazione potenzialmente definitiva» («*Hosting provider*»),[9] al paragrafo 1 richiedeva agli Stati membri di provvedere affinché tale *provider* non fosse considerato responsabile delle «informazioni memorizzate a richiesta di un destinatario del servizio», a condizione che egli: (I) non fosse effettivamente al corrente del fatto che l'attività o l'informazione fosse illecita e, riguardo ad azioni risarcitorie, non fosse al corrente di fatti o di circostanze che rendevano manifesta l'illegalità dell'attività o informazione, o (II) non appena ne fosse venuto al corrente, avesse agito immediatamente per rimuovere le informazioni o

[8]Art. 14 Direttiva 2000/31/EC: «1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

[9]«Gli hosting provider memorizzano potenzialmente definitivi contenuti generati da terzi su loro richiesta. La definizione è molto ampia: esistono hosting provider che ospitano prevalentemente video (You-Tube, Vimeo o lo stesso Libero Video oggetto della decisione in commento), hosting provider che ospitano prevalentemente foto (Picasa o Flickr), hosting provider che ospitano testi (un qualsiasi forum in internet) e hosting provider che ospitano diverse tipologie di contenuti multimediali (Facebook, che ospita testi, immagini e video, o Wikipedia, che ospita testi e immagini)». Cfr. BELLAN, *Per una reasonable liability*, cit. «Esempi di 'servizi di memorizzazione di informazioni' (*hosting*) includono categorie di servizi quali nuvola informatica, memorizzazione di informazioni di siti web, servizi di referenziazione a pagamento o servizi che consentono la condivisione di informazioni e contenuti online, compresa la condivisione e memorizzazione di file». Così il considerando (29) del Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un Mercato Unico dei Servizi Digitali e che modifica la Direttiva 2000/31/CE (Regolamento sui Servizi Digitali).

disabilitarne l'accesso. Al comma 3, lo stesso articolo 14 lasciava «impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

Infine, l'articolo 15 («Assenza dell'obbligo generale di sorveglianza»),[10] come facilmente intuibile dalla rubrica, richiedeva agli Stati membri di non imporre nessun obbligo generale di sorveglianza sulle informazioni da essi stessi trasmesse o memorizzate, né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Ciononostante, il comma 2 stabiliva come gli Stati membri avrebbero potuto stabilire in capo ai prestatori di servizi della società dell'informazione l'obbligo di informare senza indugio la pubblica autorità competente di presunte attività illecite dei destinatari dei loro servizi o di comunicare alle autorità competenti, a loro richiesta, informazioni che avrebbero consentito l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.

Tale Direttiva è stata trasposta nel nostro ordinamento per mezzo del d.lgs. n. 70 del 2003:[11] presupposto comune di queste due discipline è la mancanza di un obbligo di controllo preventivo in capo ai provider, reso impossibile a causa del numero dei contenuti generati dagli utenti trasmessi o memorizzati dagli stessi *provider*.

Tale decreto non fa altro che attuare in maniera pedissequa il contenuto della Direttiva, disciplinando le tipologie di *providers* succitate, con i rispettivi diritti e

[10]Art. 15 Direttiva 2000/31/EC: «1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati».

[11]D.lgs. n. 70 del 2003, «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».

obblighi, rispettivamente agli articoli 14 (prestatori di servizi di «*mere conduit*»),[12] 15 (prestatori di servizi di «*caching*»)[13] e 16 (prestatori di servizi di «*hosting*»).[14]

L'articolo 17 d.lgs. n. 70 del 2003[15] prevede, al pari dell'articolo 15 della *E-commerce Directive*, inoltre una clausola generale valida per tutte e tre le

[12]Art. 14 d.lgs. n. 70 del 2003: «1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse».

[13]Art. 15 d.lgs. n. 70 del 2003: «1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

[14]Art. 16 d.lgs. n. 70 del 2003: «1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

[15]Art. 17 d.lgs. n. 70 del 2003: «1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo

tipologie di provider: nessun ISP è assoggettato ad un obbligo generale di sorveglianza su informazioni e contenuti che trasmette o memorizza, né a un obbligo generale di ricercare in modo attivo fatti o circostanze che facciano presumere la presenza di contenuti o attività illecite.

In secondo luogo, tutti gli ISP sono tenuti a (I) informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora siano a conoscenza di presunte attività o informazioni illecite; e (II) fornire senza indugio, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione del destinatario dei servizi coinvolto in attività illecite. Infine, sempre ai sensi dell'articolo 17 d.lgs. n. 70 del 2003, i *providers* sono considerati responsabili per gli *user generated content* nei casi in cui (I) una volta richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non abbiano agito prontamente per impedire l'accesso a un contenuto illecito; ovvero se (II) avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicurano l'accesso, non abbiano provveduto a informarne l'autorità competente.

1.1. Un adeguato bilanciamento tra diritti fondamentali: libertà di espressione e diritto d'autore.

Le potenzialità di Internet e gli annessi rischi cui la presente dissertazione ha fatto più volte cenno, venivano in rilievo poco dopo l'emanazione della *E-commerce Directive*: tra il 2005 e 2006, in Svezia, nasce uno dei più grandi servizi di f*ile-sharing* al mondo, il sito *web* denominato «The Pirate Bay» («TPB») che consentiva agli utenti di scambiarsi *file torrent*[16] illeciti, «pirata» per l'appunto, in quanto protetti dal diritto d'autore e in assenza di qualsivoglia autorizzazione o licenza.

avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente».

[16]Si fa riferimento a «*file* di piccole dimensioni, creabili da qualsiasi utente, che recano, codificate secondo un certo algoritmo, le informazioni di riferimento utili a condividere e a scaricare (download) su un personal computer altri file, inclusi quelli eventualmente contenenti materiale coperto da diritto d'autore (prodotti audiovisivi di intrattenimento, software proprietario, libri in formato digitale, e così via)». Così, DI TODARO, *Il caso "The Pirate Bay" tra libertà di espressione e diritto d'autore*, Nota a Corte eur. Dir. Uomo sez. V 19 febbraio 2013 (Fredrik Neij e Peter Sunde Kolmisoppi c. Svezia), in *Giurisprudenza costituzionale*, 6, 2014, 4787 s.

Pochi anni più tardi, i gestori del *provider* venivano accusati dal pubblico ministero di aver concorso nella realizzazione di reati disciplinati dal Copyright Act svedese, in quanto avrebbero favorito le violazioni commesse in via diretta dagli utenti. Le condotte incriminate, nel caso di specie, consistevano nel (I) favorire gli utenti la possibilità di caricare i file illeciti tramite il proprio *website*; (II) rendere accessibile una banca dati collegata ad un intero catalogo di file protetti che gli utenti avrebbero potuto scaricare; (III) rendere disponibili i mezzi per consentire agli utenti di contattarsi a vicenda attraverso il sito TPB.

Il giudizio nazionale svedese si concludeva nel novembre del 2010 con sentenza della Corte d'appello che confermava l'attività di promozione e facilitazione tenuta da TPB attraverso i propri strumenti di *file-sharing*.

Rinviando ai paragrafi successivi l'analisi inerente alla responsabilità penale delle piattaforme digitali, il presente elaborato vuole qui soffermarsi sulla concreta tensione esistente tra due diritti fondamentali: da un lato il diritto d'autore e dall'altro il diritto alla libertà di espressione. Tale tensione risulta non poco problematica: non è un caso che gli imputati del procedimento penale svedese, una volta condannati in via definitiva, decidevano di ricorrere alla Corte europea dei diritti dell'uomo («Corte EDU») che il 13 marzo 2013 emanava una sentenza che offre spunti interessanti, nonostante non risolva definitivamente la questione.

I ricorrenti, in particolare, lamentavano la violazione dell'articolo 10 della Convenzione europea dei diritti dell'uomo («CEDU»), il quale per l'appunto tutela il diritto alla libertà di espressione:[17] in particolare, gli amministratori del *provider* sostenevano che la condanna della Corte di Stoccolma ledeva il diritto a «ricevere e fornire informazioni o idee senza che vi possa essere ingerenza».

Tuttavia, la Corte EDU – pur riconoscendo come nel caso di specie la condanna dei ricorrenti costituiva un'ingerenza da parte dello Stato nell'esercizio

[17]Art. 10 CEDU: « 1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza ingerenza alcuna da parte delle autorità pubbliche e senza considerazione di frontiera. Il presente articolo non impedisce che gli Stati sottopongano a un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione. 2. L'esercizio di queste libertà, comportando doveri e responsabilità, può essere sottoposto a determinate formalità, condizioni, restrizioni o sanzioni previste dalla legge e costituenti misure necessarie in una società democratica, per la sicurezza nazionale, l'integrità territoriale o l'ordine pubblico, la prevenzione dei disordini e dei reati, la protezione della salute e della morale, la protezione della reputazione o dei diritti altrui, o per impedire la divulgazione di informazioni confidenziali o per garantire l'autorità e la imparzialità del potere giudiziario».

del diritto alla libertà di espressione –[18] dichiarava l'inammissibilità del ricorso in quanto la repressione penale di violazioni del diritto d'autore sarebbe giustificata in virtù della posizione di tutela di cui i titolari del diritto sono beneficiari: nello specifico, il ragionamento della Corte EDU si fondava sulla sussunzione dei diritti di proprietà intellettuale all'interno della più ampia categoria del diritto di proprietà – diritto fondamentale al pari del diritto alla libertà di espressione –[19] ex articolo 1 del Protocollo addizionale n. 1.

Come sempre accade in ipotesi di tal tipo, lo strumento più idoneo alla risoluzione del conflitto tra due diritti fondamentali è il c.d. "giudizio di prevalenza", operato nel caso di specie dal giudice *de quo* e considerato, dalla Corte EDU, coerente con il testo della CEDU.

Bisogna sottolineare come il criterio distintivo nel caso di specie sia peculiare: infatti, la Corte EDU ritiene preminente il diritto d'autore rispetto al diritto di libertà di espressione, non tanto per una assoluta supremazia del primo rispetto al secondo, quanto piuttosto in ragione della natura delle informazioni che venivano trasmesse tramite TPB – nel caso di specie film e opere musicali – incapaci di essere considerate come una piena manifestazione del diritto alla libertà di espressione.[20] In altre parole, l'articolo 10 CEDU risulta violato ogni qualvolta vi sia un'ingerenza con l'attività di diffusione di informazioni relative a file condivisi tra gli *user*, a meno che però tale ingerenza non sia prevista dalla legge e abbia uno scopo legittimi e necessario all'interno di una società democratica.[21]

Sembra dunque che la potenziale collisione tra questi due diritti vada risolta caso per caso a seconda della tipologia e natura delle informazioni condivise tramite il *provider*: in via generale, sembra potersi affermare che tanto più queste ultime saranno diretta e piena espressione della libertà di

[18]DI TODARO, *Il caso "The Pirate Bay" tra libertà di espressione e diritto d'autore*, cit., 4789.
[19]Non è un caso che anche la Carta di Nizza inserisce la proprietà intellettuale all'interno dei diritti fondamentali ex articolo 17 comma 2.
[20]Cfr. DI AGOSTA, *Il caso "Pirate Bay" arriva alla Cedu: spunti per una riflessione sulla responsabilità degli "internet service provider", tra libertà d'espressione e reati in materia di "copyright"*, Nota a Corte eur. Dir. Uomo sez. V 13 marzo 2013 (Neij e Sunde Kolmisoppi c. Svezia), in *Cassazione penale*, 10, 2013, 3377 s.: «incapaci di generare un pressione sociale paragonabile all'espressione del dibattito politico inteso quale precipitato essenziale della protezione offerta ex art. 10".
[21]DI TODARO, *Il caso "The Pirate Bay" tra libertà di espressione e diritto d'autore*, cit., 4787.

manifestazione del pensiero quanto più ridotti saranno i margini per imputare ai gestori del prestatore dei servizi della società dell'informazione una responsabilità penale; tuttavia, non è possibile offrire una conclusione assoluta anche in virtù di tutti gli altri diritti fondamentali che potrebbero venire in rilievo nel caso di specie.

2. La Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale– e che modifica le direttive 96/9/CE e 2001/29/CE–, recepita dal d.lgs. n. 177 del 2021.

L'evoluzione tecnologica di Internet avvenuta nell'ultima decade, ha reso la *E-commerce Directive* inidonea a fronteggiare le problematiche derivanti dalla condivisione di file (c.d. "*file sharing*") protetti dal diritto d'autore. Al fine di colmare tale *gap*, il legislatore comunitario ha emanato la Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE, quest'ultima già analizzata nel Capitolo precedente.[22]

In particolare, così come inizialmente fatto dalla *E-commerce Directive*, anche la Direttiva in questione interviene nella tematica concernente la responsabilità dei *providers*: ciò in quanto i «rapidi sviluppi tecnologici continuano a trasformare il modo in cui le opere e altri materiali sono creati, prodotti, distribuiti e sfruttati, mentre emergono costantemente nuovi modelli di business e nuovi attori».[23]

Non a caso oggetto della Direttiva risulta essere l'armonizzazione del «quadro giuridico dell'Unione applicabile al diritto d'autore e ai diritti connessi nell'ambito del mercato interno, tenendo conto in particolare degli utilizzi digitali e transfrontalieri dei contenuti protetti»;[24] ma ciò che più interessa ai fini della dissertazione risulta essere il Capo 2, intitolato «Utilizzi specifici di contenuti protetti da parte di servizi online», ed in particolare l'articolo 17 («Utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti online»). Questo, in particolare, introduce una nuova figura di *provider* per far

[22]La prima relativa alla tutela giuridica delle banche dati, la seconda sull'armonizzazione di alcuni spetti del diritto d'autore e dei diritti connessi nella società dell'informazione.
[23]Considerando (3) Direttiva (UE) 2019/790.
[24]Art. 1 Direttiva (UE) 2019/790.

fronte agli sviluppi socio-tecnologici che tanto incidono in materia di diritto d'autore (non a caso il diritto d'autore s'intende *tecnology-driven*).[25] Tale figura è denominata «prestatore di servizi di condivisione di contenuti online».[26]

Tale *provider* sarà considerato responsabile della violazione delle norme in materia di diritto d'autore se, non avendo ottenuto alcuna autorizzazione dal titolare –ad esempio mediante licenza–, compie atti di «comunicazione al pubblico», compresa la messa a disposizione del pubblico, di opere e altri materiali protetti dal diritto d'autore.

Tuttavia, il prestatore di servizi di condivisione di contenuti online, non sarà considerato responsabile se, cumulativamente, riesca a dimostrare (I) «di aver compiuto i massimo sforzi per ottenere un'autorizzazione»,[27] (II) di «aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti»,[28] e in ogni caso (III) di «aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro»,[29] in modo conforme al punto (II).

Dunque, queste sono le condizioni in presenza delle quali il *provider* può essere esentato da responsabilità. Al fine di stabilire se il *provider* si sia conformato ai succitati obblighi, la Direttiva demanda al giudice di considerare a titolo esemplificativo, (I) «la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o altri materiali caricati dagli utenti del servizio» e (II) «la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi».[30]

[25]Con tale espressione s'intende il fatto che la disciplina autoriale è molto suscettibile al continuo mutamento del contesto tecnologico ed economico.
[26]Art. 17 Direttiva (UE) 2019/790. Si tratta di piattaforme che concedono l'accesso a contenuti caricati dagli utenti (ad esempio, Youtube), divenute ormai una delle principali fonti di accesso ai contenuti protetti.
[27]Art. 17 para. 4 lett. a) Direttiva (UE) 2019/790.
[28]Art. 17 para. 4 lett. b) Direttiva (UE) 2019/790.
[29]Art. 17 para. 4 lett. c) Direttiva (UE) 2019/790.
[30]Art. 17, para. 5 lett. a) e b) Direttiva (UE) 2019/790.

Scopo della Direttiva è quello di ridurre il c.d. "*value gap*", cioè la differenza fra il valore che questi providers ricavano dallo sfruttamento di contenuti protetti (ad esempio, come si è già visto, attraverso pubblicità, vedi infra Capitolo II, par. 1.) e i proventi versati ai titolari dei diritti.

Le tutele al diritto d'autore appena viste sono accompagnate da garanzie per evitare che siano compromessi gli altri diritti e interessi coinvolti, come libertà di informazione, comunicazione e impresa.[31]

L'articolo 17, dunque, non sembra imporre ai *providers* l'adozione di misure specifiche per prevenire il caricamento, da parte degli utenti, di materiale illecito. Nonostante il legislatore, dunque, non oneri i prestatori di servizi della società dell'informazione di controllare *ex ante* i contenuti caricati nella rete, sembra che, di fatto, i *provider* comunque tentino di limitare l'ingresso di materiale illeciti sui propri servizi. Tuttavia, per ovvi motivi legati all'impossibilità di far svolgere tale opera da un essere umano, a causa dei milioni di *upload* di file giornalieri, sembra gli unici strumenti idonei a perseguire tale scopo siano quelli di riconoscimento automatico dei contenuti illeciti mediante algoritmi, che consentono di comparare i contenuti a quelli presenti in un database: si badi bene però che tali strumenti rischiano di creare meccanismi di censura anche di contenuti anche perfettamente legali a causa dei *bias* che possono venire ad esistenza.[32] D'altronde, questi sistemi rilevano corrispondenze tra i file, e non violazioni al diritto d'autore: ad esempio, non possono valutare se un caricamento è legittimo in virtù di un'eccezione o difesa al diritto d'autore (quali, ad esempio, la critica o la parodia).

Con questa consapevolezza, e per assicurare un bilanciamento tra diritto d'autore e libertà di informazione ed espressione, la Direttiva ha previsto diverse garanzie. Innanzitutto, i *providers* sono tenuti ad istituire meccanismi di reclamo perché gli utenti possano contestare la rimozione dei contenuti caricati.[33]

---

[31]Si vedano ad esempio i considerando (54), (70) della Direttiva (UE) 2019/790.
[32]Cfr. SARTOR, LOREGGIA, *The Impact of Algorithms for Online Content Filtering or Moderation, Policy Department for Citizens' Rights and Constitutional Affairs*, 2020, 46 s. Nello stesso senso, EUROPEAN PARLIAMENTARY RESEARCH SERVICE'S STUDY, *Liability of online platforms*, cit.,11: «a general obligation to adopt automated filtering and content recognition should be excluded – as it would lead to over-detection and infringements of users' freedoms and fundamental rights».
[33]Cfr. considerando (70) e art. 17, para. 9, Direttiva (UE) 2019/790.

In secondo luogo, gli utenti devono potersi avvalere di determinate eccezioni – come la critica o parodia, per l'appunto – al diritto d'autore. Le linee guida della Commissione chiariscono il comportamento che i *providers* devono adottare per assicurare che gli usi legittimi siano effettivamente fatti salvi, non essendo sufficiente che i caricamenti legittimi vengano ripristinati dopo essere stati rimossi. In altre parole, i prestatori di servizi della società dell'informazione devono evitare assolutamente una rimozione dei contenuti legittimi, in quanto un nuovo *upload* successivo ad una previa rimozione non fornirebbe idoneo ristoro all'utente censurato.

Pertanto, i prestatori dovrebbero predisporre blocchi automatizzati tramite algoritmi solo per i contenuti di manifesta illiceità, mentre gli altri dovrebbero essere ammessi online, potendo diventare oggetto di verifica umana *ex post*, laddove vi fosse una segnalazione dei titolari dei diritti.

Sono previste anche garanzie a tutela della libertà di impresa e della concorrenza, per evitare che gli obblighi compromettano l'ingresso e il consolidamento sul mercato di nuovi prestatori. Operatori più piccoli e con meno risorse potrebbero avere, infatti, più difficoltà ad adottare le tecnologie necessarie a conformarsi ai nuovi obblighi.

Per tale motivo il nuovo regime si applica ai «grandi» operatori, cioè quelli che danno accesso a un «grande quantità»[34] di contenuti e che «svolgono un ruolo importante sul mercato dei contenuti online, in concorrenza con altri servizi di contenuti online».[35]

È inoltre previsto un regime di responsabilità mitigato per i «nuovi» prestatori di servizi di condivisione di contenuti online, che abbiano un fatturato e un pubblico limitati.[36]

[34]Art. 2, para. 6, Direttiva (UE) 2019/790.
[35]Cfr. considerando (62) Direttiva (UE) 2019/790.
[36]Art. 17, para. 6, Direttiva (UE) 2019/790: «Gli Stati membri dispongono che, con riferimento ai nuovi prestatori di servizi di condivisione di contenuti online i cui servizi sono disponibili al pubblico nell'Unione da meno di tre anni e che hanno un fatturato annuo inferiore a 10 milioni di EUR calcolati in conformità della raccomandazione 2003/361/CE della Commissione (20), le condizioni in virtù del regime di responsabilità di cui al paragrafo 4 siano limitate alla conformità alla lettera a) del paragrafo 4 e alla circostanza di aver agito tempestivamente, in seguito alla ricezione di una segnalazione sufficientemente motivata, per disabilitare l'accesso alle opere o ad altri materiali notificati o rimuovere dai loro siti web tali opere o altri materiali. Se il numero medio di visitatori unici mensili di tali prestatori di servizi supera i 5 milioni, calcolati sulla base del precedente anno civile, essi devono dimostrare altresì di aver compiuto i massimi sforzi per impedire

Inoltre, la Direttiva impone agli *online content-sharing service providers* («OCSSP») di adottare garanzie procedurali per ridurre al minimo i rischi di un filtraggio ampio e di un blocco eccessivo. In effetti, essi hanno l'obbligo di mettere in atto misure rapide ed efficaci che consentano agli utenti di presentare un reclamo contro il blocco o la rimozione di contenuti. I reclami devono essere trattati senza ritardi ingiustificati e le decisioni di disabilitare l'accesso o rimuovere i contenuti caricati devono essere soggette a revisione umana.

Rimane salvo, così come previsto dalla *E-commerce Directive*, l'esenzione da qualsiasi obbligo generale di sorveglianza.[37]

L'articolo 17 succitato è stato recepito in modo assai fedele in Italia dal d.lgs. n. 177 del 2021 – [38] decreto di ricezione della Direttiva in disamina–, il quale ha introdotto il Titolo II-*quater* nella legge n. 633 del 1941, intitolato «Utilizzo di contenuti protetti da parte dei prestatori di servizi di condivisione di contenuti online», all'interno del quale vengono inseriti gli articoli 102-*sexies* a 102-*decies*: ai fini del presente elaborato è sufficiente l'analisi degli articoli 102-*sexies*, 102-*septies* e 102-*decies*.

L'articolo 102-*sexies*[39] definisce innanzitutto la nozione di «prestatore di servizi di condivisione di contenuti online". Esso è un prestatore di servizi della

l'ulteriore caricamento di opere o di altri materiali oggetto della segnalazione per i quali i titolari dei diritti abbiano fornito informazioni pertinenti e necessarie».

[37]Art. 17, para. 8, Direttiva (UE) 2019/790.

[38]D.lgs. n. 177 del 2021, «Attuazione della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE».

[39]Art. 102-*sexies* l. n. 633 del 1941: «1. Ai fini del presente Titolo si intende per prestatore di servizi di condivisione di contenuti online un prestatore di servizi della società dell'informazione che presenta cumulativamente i seguenti requisiti: a) ha come scopo principale, o tra i principali scopi, di memorizzare e dare accesso al pubblico a grandi quantità di opere o di altri materiali protetti dal diritto d'autore; b) le opere o gli altri materiali protetti sono caricati dai suoi utenti; c) le opere o gli altri materiali protetti sono organizzati e promossi allo scopo di trarne profitto direttamente o indirettamente. 2. Non sono considerati prestatori di servizi di condivisione di contenuti online ai sensi del presente Titolo quelli che danno accesso alle enciclopedie online senza scopo di lucro, ai repertori didattici o scientifici senza scopo di lucro, nonché le piattaforme di sviluppo e di condivisione di software open source, i fornitori di servizi di comunicazione elettronica, i prestatori di mercati online, di servizi cloud da impresa a impresa e di servizi cloud che consentono agli utenti di caricare contenuti per uso personale, salvo che il mercato online o il servizio cloud consenta di condividere opere protette dal diritto d'autore tra più utenti. 3. I prestatori di servizi di condivisione di contenuti online, quando concedono l'accesso al pubblico a opere protette dal diritto d'autore o ad altri materiali protetti caricati dai loro utenti, compiono un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico per i quali devono ottenere un'autorizzazione dai titolari dei diritti, anche mediante la conclusione di un accordo di licenza, ottenuta direttamente o tramite gli organismi di gestione collettiva e le entità di gestione indipendente di cui al decreto legislativo del 15 marzo 2017, n. 35. 4. L'autorizzazione di cui al comma 3 include gli atti compiuti dagli utenti

società dell'informazione che deve essere in possesso dei seguenti requisiti: (I) il soggetto ha come scopo principale di memorizzare e dare accesso al pubblico a grandi quantità di opere o di altri materiali protetti dal diritto d'autore; (II) le opere o gli altri materiali protetti sono caricati dagli utenti; e infine (III) le opere o gli altri materiali protetti sono organizzati e promossi allo scopo di trarne profitto sia direttamente che indirettamente. Rientrano, altresì, i prestatori di mercato online o di servizio cloud che consenta di condividere tra più utenti opere protette.

È precisato, inoltre che non possono essere considerati come prestatori di servizi di condivisione di contenuti online: (I) i prestatori che danno accesso alle enciclopedie online ed ai repertori didattici o scientifici senza scopo di lucro; (II) le piattaforme di sviluppo e di condivisione di *software open source*; (III) i fornitori di servizi di comunicazione elettronica; (IV) i prestatori di mercati online, (V) i prestatori di servizi cloud da impresa a impresa; (VI) i prestatori di servizi *cloud* che consentono agli utenti di caricare contenuti per uso personale.

Tali *providers*, sempre ai sensi dell'articolo 102-*sexies*, compiono un «*atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico*» quando concedono l'accesso a opere protette dal diritto d'autore o ad altri materiali protetti caricati dai loro utenti.

Per svolgere tale attività in modo lecito, ovviamente, questa figura di provider deve acquisire l'autorizzazione da parte del titolare di diritto d'autore, anche mediante licenza; se così non accade, ecco che si applica l'articolo 102-*septies*,[40] fedele all'articolo 17 della Direttiva: nel caso di mancata acquisizione

---

che caricano sulla piattaforma del prestatore di servizi opere protette dal diritto d'autore quando non agiscono per scopi commerciali o la loro attività non genera ricavi significativi. 5. Non si applica la limitazione di responsabilità di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ai casi di cui al presente Titolo».

[40]Art. 102-*septies* l. n. 633 del 1941: «1. I prestatori di servizi di condivisione di contenuti online, in mancanza dell'autorizzazione di cui all'articolo 102-sexies, sono responsabili per gli atti non autorizzati di comunicazione al pubblico e di messa a disposizione del pubblico di opere e di altri materiali protetti dal diritto d'autore, salvo che dimostrino di avere soddisfatto cumulativamente le seguenti condizioni: a) aver compiuto i massimi sforzi per ottenere un'autorizzazione secondo elevati standard di diligenza professionale di settore; b) aver compiuto, secondo elevati standard di diligenza professionale di settore i massimi sforzi per assicurarsi che non sono rese disponibili opere e altri materiali specifici per i quali hanno ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; c) avere, dopo la ricezione di una segnalazione sufficientemente motivata da parte dei titolari dei diritti, tempestivamente disabilitato l'accesso o rimosso dai propri siti web le opere o gli altri materiali oggetto di segnalazione e aver compiuto, secondo il livello di diligenza richiesto alla lettera b), i massimi sforzi per impedirne il caricamento in futuro. 2. Per stabilire, secondo il principio di proporzionalità, se il prestatore di servizi di condivisione di contenuti online è esente da

dell'autorizzazione, i *providers* sono considerati responsabili per gli atti di comunicazione al pubblico e di messa a disposizione del pubblico non autorizzati.

La responsabilità è tuttavia esclusa, come prevede l'articolo 17 della Direttiva, quando i prestatori di servizi di condivisione di contenuti online riescono a dimostrare di aver compiuto i massimi sforzi per: (I) ottenere un'autorizzazione secondo elevati standard di diligenza professionale di settore; (II) impedire che non siano rese disponibili opere e altri materiali per i quali hanno ricevuto le informazioni dai titolari dei diritti; (III) disabilitare l'accesso o rimuovere dai propri siti web le opere o gli altri materiali oggetto di segnalazione ed interdirne il caricamento in futuro – da segnalare che l'intervento deve avvenire «tempestivamente» dopo la ricezione di una motivata segnalazione da parte dei titolari dei diritti.

Per poter escludere la responsabilità del prestatore, l'art. 102-*septies* dispone che vanno presi in considerazione i seguenti criteri di valutazione: (I) la tipologia, il pubblico e la dimensione del servizio; (II) la tipologia di opere o di altri materiali caricati dagli utenti; (III) la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi. La clausola di esenzione di responsabilità non trova applicazione quando il prestatore pone in essere atti diretti a facilitare la pirateria in materia di diritto d'autore, divenendo dunque non più soggetto terzo e intermediario ma co-autore della violazione sullo stesso piano dell'autore diretto.

Infine, l'articolo 102-*decies*[41] consente al titolare del diritto d'autore di richiedere al prestatore di servizi di condivisione di contenuti online di disabilitare

responsabilità, sono presi in considerazione, con valutazione caso per caso, anche la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o di altri materiali caricati dagli utenti del servizio, nonché la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi. In ogni caso, non è esente da responsabilità il prestatore di servizi di condivisione di contenuti online che pratica o facilita la pirateria in materia di diritto d'autore. 3. I prestatori di servizi di condivisione di contenuti online forniscono tempestivamente ai titolari dei diritti, su richiesta di questi ultimi, informazioni complete e adeguate sulle modalità di attuazione delle disposizioni di cui al comma 1 e, quando sono stati conclusi accordi di licenza tra i prestatori di servizi e i titolari dei diritti, informazioni sull'utilizzo dei contenuti oggetto degli accordi. 4. L'applicazione delle disposizioni del presente Titolo non comporta un obbligo generale di sorveglianza».

[41] Art. 102-*decies* l. n. 633 del 1941: «1. Quando i titolari dei diritti chiedono al prestatore di servizi di condivisione di contenuti online di disabilitare l'accesso a loro specifiche opere o ad altri materiali o di rimuoverli, indicano i motivi della richiesta. Le decisioni sulla richiesta di disabilitazione o la rimozione dei contenuti sono soggette a verifica umana. Il prestatore dà immediata comunicazione agli utenti dell'avvenuta disabilitazione o rimozione. 2. I prestatori di servizi di condivisione di contenuti online istituiscono e rendono disponibili agli utenti dei servizi meccanismi di reclamo

l'accesso o rimuovere le opere o materiali connessi: i legittimati sono tuttavia tenuti a motivare la loro richiesta. Dopodiché, il *provider* dovrà (I) dare immediata comunicazione agli utenti dell'avvenuta disabilitazione o rimozione e (II) istituire e rendere disponibili meccanismi di reclamo.

La norma prescrive che i contenuti oggetto di contestazione devono rimanere disabilitati in pendenza della decisione sul reclamo. La decisione adottata dal prestatore di servizi può essere contestata con ricorso presentato all'Autorità per le garanzie nelle comunicazioni («AGCOM») che è tenuta ad adottare apposite linee guida per la gestione dei meccanismi di reclamo. Rimane comunque salvo il diritto di ricorrere all'autorità giudiziaria.

Il prossimo paragrafo si occuperà dell'analisi del nuovo Regolamento EU 2022/2065, che, d'ora innanzi verrà assunto come fonte principale per la disciplina attinente alla responsabilità delle piattaforme digitali, in particolare dei «servizi intermediario» e «piattaforme online» come visto nella premessa del precedente Capitolo. Infine, si procederà a sviluppare il tema della responsabilità delle piattaforme in ambito domestico, approfondendo dapprima la disciplina penalistica e civilistica per poi, infine, condurre un'analisi comparatistica.

3. Il Regolamento EU 2022/2065 sui servizi digitali: il *Digital Service Act*.

Le iniziative legislative nazionali degli Stati membri volte ad attuare e recepire la Direttiva *E-commerce* avevano risolto in parte i problemi individuati ma avevano al contempo condotto ad una maggiore frammentazione normativa nell'UE. Ciò ha comportato un aumento dei costi di *compliance* per le piattaforme digitali che operano a livello transfrontaliero.

Pertanto, nel dicembre 2020 la Commissione Europea, mossa anche da tutta la serie di evoluzioni socio-tecnologiche degli ultimi vent'anni di cui si è discusso nei paragrafi precedenti, ha proposto due iniziative legislative per aggiornare le

celeri ed efficaci per la contestazione della decisione di disabilitazione dell'accesso o di rimozione di specifiche opere o di altri materiali da essi caricati. A tal fine l'Autorità per le garanzie nelle comunicazioni adotta apposite linee guida. 3. Nelle more della decisione sul reclamo, i contenuti in contestazione rimangono disabilitati. 4. La decisione adottata dal prestatore di servizi di condivisione di contenuti online a seguito del reclamo di cui al comma 2 può essere contestata con ricorso presentato all'Autorità per le garanzie nelle comunicazioni, secondo le modalità da essa definite tramite regolamento, da adottare entro sessanta giorni dalla data di entrata in vigore della presente disposizione. È fatto salvo il diritto di ricorrere all'autorità giudiziaria».

norme che regolano i servizi digitali nell'UE: il *Digital Services Act*, già citato, e il *Digital Markets Act* («DMA»).[42]

Il 25 marzo 2022 è stato raggiunto un accordo politico sul *Digital Markets Act* e il 23 aprile 2022 sul *Digital Services Act*. Insieme formano un unico insieme di nuove regole che saranno applicabili in tutta l'Unione Europea per creare uno spazio digitale più sicuro e aperto.

Il Regolamento DSA è stato emanato il 19 ottobre 2022 e mira a creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi digitali. Il DSA sarà dunque direttamente applicabile in tutta l'UE e si applicherà quindici mesi dopo l'entrata in vigore.

Oggi, lo si ripete, gli utenti di Internet sono esposti a beni, contenuti o servizi illegali online e tutte le decisioni riguardo la loro rimozione sono per lo più a discrezione delle piattaforme. L'impatto maggiore proviene da quelle piattaforme che sono diventate spazi quasi pubblici per la comunicazione e il commercio: si pensi ai social media quali Instagram/Facebook/Twitter/TikTok per la comunicazione o ad Amazon ed Ebay per il commercio.

Il Regolamento contiene, *inter alia*, (I) misure per contrastare i beni, i servizi o i contenuti illegali online, attraverso un meccanismo – simile a quello previsto dalla *E-commerce Directive* – che consente agli utenti di segnalare tali contenuti e alle piattaforme di collaborare con i c.d. "segnalatori attendibili"[43] o "*trusted flaggers"* ; (II) crea garanzie efficaci per gli utenti, tra cui la possibilità di contestare le decisioni di moderazione dei contenuti delle piattaforme[44]; (III) impone misure di trasparenza per le piattaforme digitali di grandi dimensioni, anche per quanto riguarda gli algoritmi utilizzati per la raccomandazione. [45]

Va sottolineato che gli articoli 4, 5 e 6 del DSA – inerenti la responsabilità dei «servizi intermediario», quali i «*mere conduit*», i «*caching providers*» e gli «*hosting providers*» – ricalcano esattamente le disposizioni degli articoli 12, 13 e

[42]Digital Markets Act («DMA»), il nuovo regolamento della UE per combattere le pratiche di mercato sleali e le distorsioni della concorrenza da parte delle Big Tech. Per un approfondimento si veda: *https://ec.europa.eu/commission/presscorner/detail/it/IP_22_6423*.
[43]Per un approfondimento sui segnalatori attendibili cfr. considerando (61) e art. 22 Regolamento (UE) 2022/2065.
[44]Art. 20 Regolamento (UE) 2022/2065.
[45]Artt. 69 e 72 Regolamento (UE) 2022/2065.

14 della E-commerce Directive su analizzati.[46] Allo stesso modo l'articolo 8 del DSA («Assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti»), richiama l'articolo 15 della E-commerce Directive, citato, anch'esso, in precedenza.

Le novità più importanti in materia di responsabilità delle piattaforme previste dal nuovo Regolamento, sono contenute all'interno della Sezione 2 – ed in particolare agli articoli 16-17 – e all'interno della Sezione 3 – ed in particolare agli articoli 20-21 – che impongono ai servizi intermediari e alle piattaforme online l'obbligo di gestire i reclami contro i contenuti illegali generati dagli utenti. [47] Ai fini di un'esposizione maggiormente fluida, verranno inizialmente analizzati gli articoli 16,17 e 20,21, per concludere con l'articolo 19 e rinviando la disamina dell'articolo 18 al paragrafo che tratterà della responsabilità penale delle piattaforme digitali (vedi *infra* 3.1.3). Si badi bene sin da ora che la Sezione 2 si applica ai «prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online»: da ciò ne deriva l'apparente esclusione dei *mere conduit* provider, i quali sono definiti dallo stesso Regolamento all'articolo 3 come servizi di «trasmissione» di informazioni e non di «memorizzazione»;[48] la Sezione 3,

[46]È prevista tuttavia una sola differenza, con riferimento agli *hosting providers*: infatti l'articolo 6 del DSA aggiunge un paragrafo, secondo cui «Il paragrafo 1 [concernente i casi di esenzione della responsabilità del *provider*] non si applica in relazione alla responsabilità prevista dalla normativa in materia di protezione dei consumatori per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, qualora tali piattaforme online presentino informazioni specifiche o rendano altrimenti possibile l'operazione specifica in questione in modo tale da indurre un consumatore medio a ritenere che le informazioni, o il prodotto o il servizio oggetto dell'operazione, siano forniti dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo».

[47]Si badi che la Sezione 2 si applica ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online, mentre la Sezione 3 alle sole piattaforme online.

[48]Art. 3 Regolamento lett. g) (UE) 2002/2065: «Ai fini del presente regolamento si applicano le definizioni seguenti: […] g) «servizio intermediario»: uno dei seguenti servizi della società dell'informazione: i) un servizio di semplice trasporto (cosiddetto «mere conduit»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione; ii) un servizio di memorizzazione temporanea (cosiddetto «caching»), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta; iii) un servizio di memorizzazione di informazioni (cosiddetto «hosting»), consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso».

invece, si applica alle sole piattaforme online, considerate, sempre dall'articolo 3 del DSA come *species* dei servizi di memorizzazione di informazioni.[49]

3.1. La nuova procedura di *notice and take-down*: gli articoli 16-17, 20-21.

Il nuovo meccanismo di ricorso procedurale previsto dal Regolamento si compone di diverse fasi: il primo passo, ai sensi dell'articolo 16 DSA («Meccanismo di segnalazione e azione»), è la notifica di contenuti illegali ricevuta dai servizi di memorizzazione di informazioni (i.e., *caching* e *hosting providers*), comprese le piattaforme online, che devono predisporre «meccanismi [di facile accesso e di semplice utilizzo] per consentire a qualsiasi persona o ente di notificare loro la presenza nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali»;[50] la seconda fase, *ex* articolo 17 DSA

[49]Art. 3 Regolamento lett. i) (UE) 2002/2065: «Ai fini del presente regolamento si applicano le definizioni seguenti: […] i) «piattaforma online»: un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

[50]Art. 16 Regolamento (UE) 2022/2065: «1. I prestatori di servizi di memorizzazione di informazioni predispongono meccanismi per consentire a qualsiasi persona o ente di notificare loro la presenza nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali. Tali meccanismi sono di facile accesso e uso e consentono la presentazione di segnalazioni esclusivamente per via elettronica. 2. I meccanismi di cui al paragrafo 1 sono tali da facilitare la presentazione di segnalazioni sufficientemente precise e adeguatamente motivate. A tal fine i prestatori di servizi di memorizzazione di informazioni adottano le misure necessarie per consentire e facilitare la presentazione di segnalazioni contenenti tutti gli elementi seguenti: a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della direttiva 2011/93/UE; d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute. 3. Si considera che le segnalazioni di cui al presente articolo permettono di acquisire una conoscenza o consapevolezza effettiva ai fini dell'articolo 6 in relazione alle specifiche informazioni in questione qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità della pertinente attività o informazione senza un esame giuridico dettagliato. 4. Se la segnalazione contiene un'informazione di contatto elettronica della persona o dell'ente che l'ha presentata, il prestatore di servizi di memorizzazione di informazioni invia senza indebito ritardo una conferma di ricevimento della segnalazione a tale persona o ente. 5. Senza indebito ritardo il prestatore notifica inoltre a tale persona o ente la propria decisione in merito alle informazioni cui si riferisce la segnalazione, fornendo informazioni sulle possibilità di ricorso disponibili in relazione a tale decisione. 6. I prestatori di servizi di memorizzazione di informazioni trattano le segnalazioni ricevute nell'ambito dei meccanismi di cui al paragrafo 1 e adottano le loro decisioni in merito alle informazioni cui tali segnalazioni si

(«Motivazione»), si verifica se la piattaforma decide di restringere la visibilità del contenuto o di disabilitarne l'accesso, perché, in tal caso, i «prestatori di servizi di memorizzazione di informazioni forniscono a tutti i destinatari del servizio interessati una motivazione chiara e specifica per le […] restrizioni imposte […]».[51]

Già queste due fasi presentano delle novità rispetto alla disciplina contenuta nella *E-Commerce Directive* e relativo decreto di ricezione (lo si ricorda, il d.lgs. n. 70 del 2003): si richiede, infatti, esplicitamente, ai titolari delle piattaforme digitali, di predisporre dei meccanismi grazie ai quali il titolare dei diritti può notificare la loro lamentata lesione (cosa che con la Direttiva UE 2019/79 avveniva solo con

---

riferiscono in modo tempestivo, diligente, non arbitrario e obiettivo. Qualora usino strumenti automatizzati per tali processi di trattamento o decisione, nella notifica di cui al paragrafo 5 essi includono informazioni su tale uso».

[51]Art. 17 Regolamento (UE) 2022/2065: «1. I prestatori di servizi di memorizzazione di informazioni forniscono a tutti i destinatari del servizio interessati una motivazione chiara e specifica per le seguenti restrizioni imposte a motivo del fatto che le informazioni fornite dal destinatario del servizio costituiscono contenuti illegali o sono incompatibili con le proprie condizioni generali: a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; c) la sospensione o la cessazione totale o parziale della prestazione del servizio; d) la sospensione o la chiusura dell'account del destinatario del servizio. 2. Il paragrafo 1 si applica solo se le pertinenti coordinate elettroniche sono note al prestatore. Esso si applica al più tardi dalla data a partire dalla quale la restrizione è imposta, indipendentemente dal motivo o dal modo in cui è imposta. Il paragrafo 1 non si applica se le informazioni sono contenuti commerciali ingannevoli ad ampia diffusione. 3. La motivazione di cui al paragrafo 1 contiene almeno le informazioni seguenti: a) l'informazione che indichi se la decisione comporti la rimozione delle informazioni, la disabilitazione dell'accesso alle stesse, la retrocessione o la limitazione della visibilità delle informazioni oppure la sospensione o la cessazione dei pagamenti in denaro relativi a tali informazioni o imponga altre misure di cui al paragrafo 1 in relazione alle informazioni, e, ove opportuno, la portata territoriale della decisione e la sua durata; b) i fatti e le circostanze su cui si basa la decisione adottata, compresa, ove opportuno, l'informazione che indichi se la decisione sia stata adottata in base a una segnalazione presentata a norma dell'articolo 16 oppure sia stata basata su indagini volontarie di propria iniziativa e, ove strettamente necessario, l'identità del notificante; c) ove opportuno, informazioni sugli strumenti automatizzati usati per adottare la decisione, ivi compresa l'informazione che indichi se la decisione sia stata adottata in merito a contenuti individuati o identificati per mezzo di strumenti automatizzati; d) se la decisione riguarda presunti contenuti illegali, un riferimento alla base giuridica invocata e una spiegazione delle ragioni per cui l'informazione è considerata contenuto illegale in applicazione di tale base giuridica; e) se la decisione si basa sulla presunta incompatibilità delle informazioni con le condizioni generali del prestatore di servizi di memorizzazione di informazioni, un riferimento alla clausola contrattuale invocata e una spiegazione delle ragioni per cui le informazioni sono ritenute incompatibili con tale clausola; f) informazioni chiare e di facile comprensione sui mezzi di ricorso a disposizione del destinatario del servizio in relazione alla decisione, in particolare, se del caso, attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria. 4. Le informazioni fornite dai prestatori di servizi di memorizzazione di informazioni a norma del presente articolo devono essere chiare e facilmente comprensibili e il più possibile precise e specifiche tenuto conto delle circostanze del caso. In particolare, le informazioni devono essere tali da consentire ragionevolmente al destinatario del servizio interessato di sfruttare in modo effettivo le possibilità di ricorso di cui al paragrafo 3, lettera f). 5. Il presente articolo non si applica agli ordini di cui all'articolo 9».

riferimento agli OCSSP) ; in secondo luogo, il titolare della piattaforma, nel caso in cui decidesse di rimuovere o limitare il contenuto segnalato deve indicare le ragioni di tale scelta.

Se ciò può sembrare innovativo, le due fasi successive, disciplinate dagli articoli 20-21 del DSA, ossia, rispettivamente, il «Sistema interno di gestione dei reclami» e la «Risoluzione extragiudiziale delle controversie», lo sono ancor di più. Si badi che questi due articoli, contenuti nella Sezione 3, si applicano alle sole piattaforme online, come già anticipato.

L'articolo 20 DSA[52] stabilisce, infatti, che le piattaforme online devono fornire un sistema interno di gestione dei reclami efficace, di facile accesso e di semplice utilizzo per il «destinatario del servizio» (cioè l'autore del contenuto incriminato) e per le «comprese le persone o gli enti che hanno presentato una segnalazione», che «consenta loro di presentare per via elettronica e gratuitamente reclami contro la decisione presa dal fornitore della piattaforma online».

[52]Art. 20 Regolamento (UE) 2022/2065: «1. I fornitori di piattaforme online forniscono ai destinatari del servizio, comprese le persone o gli enti che hanno presentato una segnalazione, per un periodo di almeno sei mesi dalla decisione di cui al presente paragrafo, l'accesso a un sistema interno di gestione dei reclami efficace, che consenta loro di presentare per via elettronica e gratuitamente reclami contro la decisione presa dal fornitore della piattaforma online all'atto del ricevimento di una segnalazione o contro le seguenti decisioni adottate dal fornitore della piattaforma online a motivo del fatto che le informazioni fornite dai destinatari costituiscono contenuti illegali o sono incompatibili con le condizioni generali: a) le decisioni che indicano se rimuovere le informazioni o disabilitare l'accesso alle stesse o se limitarne la visibilità; b) le decisioni che indicano se sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari; c) le decisioni che indicano se sospendere o cessare l'account dei destinatari; d) le decisioni che indicano se sospendere, cessare o limitare in altro modo la capacità di monetizzare le informazioni fornite dai destinatari. 2. Il periodo di almeno sei mesi di cui al paragrafo 1 del presente articolo decorre dal giorno in cui il destinatario del servizio è stato informato della decisione a norma dell'articolo 16, paragrafo 5, o dell'articolo 17. 3. I fornitori di piattaforme online provvedono affinché i loro sistemi interni di gestione dei reclami siano di facile accesso e uso e affinché consentano e agevolino la presentazione di reclami sufficientemente precisi e adeguatamente motivati. 4. I fornitori di piattaforme online gestiscono i reclami presentati attraverso il loro sistema interno di gestione dei reclami in modo tempestivo, non discriminatorio, diligente e non arbitrario. Se un reclamo contiene motivi sufficienti per indurre il fornitore della piattaforma online a ritenere che la sua decisione di non dare seguito alla segnalazione sia infondata o che le informazioni oggetto del reclamo non siano illegali né incompatibili con le condizioni generali, o se tale reclamo contiene informazioni indicanti che il comportamento del reclamante non giustifica le misure adottate, il fornitore della piattaforma online annulla senza indebito ritardo la decisione di cui al paragrafo 1. 5. I fornitori di piattaforme online comunicano senza indebito ritardo ai reclamanti la loro decisione motivata relativa alle informazioni cui si riferisce il reclamo e la possibilità di risoluzione extragiudiziale delle controversie di cui all'articolo 21 e le altre possibilità di ricorso a loro disposizione. 6. I fornitori di piattaforme online provvedono affinché le decisioni di cui al paragrafo 5 siano prese con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati».

L'articolo 20, paragrafo 4, stabilisce che se il fornitore della piattaforma ritiene che il reclamo presentato da una delle parti contenga «motivi sufficienti per indur[la] […] a ritenere che la sua decisione di non dare seguito alla segnalazione sia infondata o che le informazioni oggetto del reclamo non siano illegali né incompatibili con le condizioni generali, o se tale reclamo contiene informazioni indicanti che il comportamento del reclamante non giustifica le misure adottate», lo stesso fornitore della piattaforma annulla «senza indebito ritardo la decisione di cui al paragrafo 1.».

Ai sensi dell'articolo 21, il fornitore della piattaforma online, dovrà offrire una «risoluzione extragiudiziale della controversia», facilmente accessibile sulla sua interfaccia online, chiara e di facile uso, ai «destinatari del servizio» (ancora una volta, l'autore del contenuto incriminato) e alle «persone o gli enti che hanno presentato una segnalazione». L'organismo che conduce il procedimento extragiudiziale deve soddisfare i requisiti fondamentali previsti dal paragrafo 3.

L'articolo 21, paragrafo 2, stabilisce che «[l]'organismo di risoluzione extragiudiziale delle controversie certificato non ha il potere di imporre una risoluzione della controversia vincolante per le parti».

Questo è, in sintesi, il modo in cui il regolamento DSA disciplina la *notice and take-down procedure*.

Va sottolineato che la Commissione UE, spinta da alcuni commentatori,[53] ha cambiato rotta rispetto a quanto disciplinato nella proposta di DSA. Infatti, quest'ultima procedura in due fasi (artt. 20-21 DSA, che corrispondono agli artt. 17-18 della proposta DSA) era prevista solo per i «destinatari del servizio» che avrebbero potuto presentare reclami «contro [determinate decisioni] adottate dalla piattaforma online a motivo del fatto che le informazioni fornite dai destinatari [avrebbero costituito] contenuti illegali o sono incompatibili con le sue condizioni generali».

Le decisioni considerate erano (I) le decisioni di rimuovere le informazioni o disabilitare l'accesso alle stesse; (II) le decisioni di sospendere o cessare in tutto

[53]Cfr. EIFERT, METZGER, SCHWEITZER, WAGNER, *Taming the Giants: The DMA/DSA Package*, in *Kluwer Law International*, 2021, 1010 ss.

o in parte la prestazione del servizio ai destinatari; (III) le decisioni di sospendere o cessare l'account dei destinatari.

Quindi, poiché l'articolo 18 della proposta di DSA, che disciplinava la «risoluzione extragiudiziale delle controversie», era destinato ad essere applicato solo ai «destinatari del servizio ai quali [erano] rivolte le decisioni di cui all'articolo 17, paragrafo 1» (ossia l'autore del contenuto incriminato o il proprietario dell'account), lo stesso rimedio extragiudiziale non veniva garantito alla parte danneggiata.

Pertanto, mentre la parte lesa (le vittime, ad esempio, di violazione del diritto d'autore) aveva il diritto di avviare la procedura di rimozione dei contenuti illegali ai sensi dell'articolo 14 della proposta di DSA (che corrisponde all'attuale articolo 16 delle DSA), la stessa parte rimaneva esclusa dal successivo procedimento ai sensi dell'articolo 18. Dunque, in sintesi, la proposta di DSA non offriva nessun rimedio extragiudiziale alla vittima che attraverso la procedura prevista dall'articolo 14 della proposta (l'attuale articolo 16 del Regolamento) aveva inviato una segnalazione, a seguito della quale, tuttavia, il fornitore della piattaforma online non ravvisava elementi idonei alla restrizione o sospensione del contenuto oggetto di tale segnalazione.

In conclusione, l'unico rimedio a disposizione della parte lesa era quello di intentare una causa in tribunale o di chiedere a un tribunale un provvedimento cautelare che ordinasse alla piattaforma di rimuovere il contenuto illecito.
Questa differenza tra i rimedi a disposizione dell'autore del contenuto illecito e della parte lesa è stata definita «sistema asimmetrico del meccanismo di ricorso»,[54] e risulta superato dalla disciplina sopra esposta.

[54]Cfr. EIFERT, METZGER, SCHWEITZER, WAGNER, *Taming the Giants*, cit., 1010 s.

Ai sensi dell'articolo 19,[55] infine, questi ultimi due articoli, 20 e 21, non si applicano poi alle microimprese e piccole imprese così come definite nella Raccomandazione della Commissione 2003/361/CE.[56]

Dato che l'articolo 18 verrà analizzato nei paragrafi successivi (vedi infra 3.1.3.), si può ritenere conclusa la disamina relativa alla disciplina unionale in materia di responsabilità delle piattaforme digitali.

Nei prossimi paragrafi si procederà a sviluppare il tema della responsabilità delle piattaforme in ambito domestico, approfondendo dapprima la disciplina penalistica e civilistica per poi, infine, condurre un'analisi comparatistica.

4. La responsabilità delle piattaforme in ambito domestico: la disciplina penalistica, civilistica e cenni comparatistici.

Come si è accennato, il nuovo Regolamento dell'Unione Europea, coerentemente con le Direttive ad esso antecedenti – su esaminate –, non definisce cosa debba intendersi per contenuto «illegale». È ovvio che uno *user generated content* sarà illegale nel momento in cui viola la normativa di uno Stato Membro. I prossimi paragrafi non si occuperanno, naturalmente, di analizzare il diritto penale e civile speciale, ovverosia le singole norme che rendono un determinato tipo di contenuto «illegale» o meno. Infatti, le norme di diritto penale speciale a tutela della proprietà intellettuale sono già state analizzate nel corso del Capitolo I.

Ci si occuperà piuttosto di capire quali istituti del diritto penale e civile generale siano applicabili alle piattaforme digitali; in particolare, due sono gli istituti generali attinenti la responsabilità dell'agente (in questo caso, non l'utente, bensì la piattaforma digitale), potenzialmente applicabili alternativamente: nello specifico, relativamente alla disciplina penalistica ci si chiede se la responsabilità

[55]Art. 19 Regolamento (UE) 2022/2065: «1. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE. La presente sezione, ad eccezione dell'articolo 24, paragrafo 3, non si applica ai fornitori di piattaforme online che si sono precedentemente qualificati come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE nel corso dei 12 mesi successivi alla perdita di tale qualifica a norma dell'articolo 4, paragrafo 2, della medesima raccomandazione, tranne quando sono piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33. 2. In deroga al paragrafo 1 del presente articolo, la presente sezione si applica ai fornitori di piattaforme online che sono stati designati come piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che si qualifichino come microimprese o piccole imprese».

[56]Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese.

della piattaforma sia da inquadrarsi (I) nella fattispecie di omesso impedimento del reato *ex* articolo 40 comma 2 c.p. oppure nella fattispecie di concorso omissivo nel reato commissivo dell'utente, secondo il combinato disposto degli articoli 40 comma 2 e 110 del codice penale; relativamente alla disciplina civilistica, ci si chiede invece se alla piattaforma sia da imputare una responsabilità contrattuale ai sensi dell'articolo 1218 c.c. o, invece, una responsabilità aquiliana, *ex* articolo 2043 c.c. con le diverse differenze di disciplina che ne derivano.

4.1. La responsabilità penale dell'Internet Service Provider: tra omesso impedimento e concorso omissivo nel reato commissivo dell'utente.

Il maremoto tecnologico sollevato dall'avvento di Internet ha cambiato ogni aspetto della nostra quotidianità: quasi ogni attività è – e se non lo è, lo sarà – esperibile sulla rete. Non sarebbe errato sostenere che tale fenomeno tecnologico ha avuto rilevanti ripercussioni anche sulla meta-realtà, ed in particolare su una categoria: il diritto.[57]

Dal punto di vista del diritto penale, è stato da alcuni sostenuto che la classica e tradizionale configurazione degli istituti penalistici poco si adatti all'avvento di un fenomeno così rivoluzionario.[58] Tuttavia, all'interno del rapporto tra le trasformazioni avvenute nell'ultimo ventennio e le categorie penalistiche bisogna distinguere tra ciò che è davvero nuovo e ciò che invece può essere assoggettato ai principi classici e tradizionali.[59]

A tale proposito, tra le trasformazioni che si pongono in forte tensione con le categorie penalistiche tradizionali e che hanno imposto aggiornamenti della loro configurazione, vi è l'oggetto del presente elaborato: e cioè il tema della responsabilità penale delle piattaforme digitali. Un tema, questo, che impone un vero e proprio ripensamento di alcuni istituti penalistici tradizionali «generali», e più precisamente un ripensamento del concetto di «condotta tipica» in contesti

[57]TERRACINA, *La tutela penale del diritto d'autore*, cit., 144.
[58]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in *Dir. pen. e proc.*, vol. 19, 5, 2013, 600.
[59]BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 600.

caratterizzati da automatismi tecnologici e del concetto di «responsabilità per concorso omissivo nel reato altrui».[60]

Prima di approfondire il tema delle problematiche poste dalla responsabilità penale delle piattaforme in ambito domestico, è opportuno evidenziare alcune peculiarità che rendono l'Internet una realtà unica.

Anzitutto bisogna distinguere due diversi tipi di attività: (I) quelle riguardanti l'ingresso dei contenuti nella rete e (II) quelle che riguardano la loro permanenza. Con riferimento all'ingresso dei contenuti nella rete, vengono in gioco la condotta di accesso alla rete (fornita dai c.d. *access providers*) e quella di trasmissione di dati (fornita dai *mere conduit*); riguardo alla permanenza viene in gioco il concetto di memorizzazione (attività fornita dai *caching providers*, *hosting providers* e dalle piattaforme online, così come definite dal DSA).

In secondo luogo, bisogna considerare come tali attività possono essere svolte secondo modalità totalmente automatizzate, in cui un coinvolgimento umano è limitato al solo momento iniziale, oppure secondo modalità non totalmente automatizzate, in cui un comportamento tenuto da un essere umano è comunque necessario.

Infine, è necessario sottolineare che l'attività svolta dal *provider*– che abbiamo già definito come colui che offre servizi della società dell'informazione– non è di per sé pericolosa.

Da questo quadro così delineato emerge come, riguardo alla tensione tra trasformazioni tecnologiche e diritto penale, si pongano soprattutto due problemi: da un lato, la configurazione della condotta tipica (rilevante ai fini dell'integrazione della fattispecie criminosa) nell'ambito di attività totalmente automatizzate; dall'altro, il problema dell'impedimento del reato ma non solo – e non tanto– al momento dell'ingresso del contenuto illecito nella rete in una prospettiva *ex ante* (che presupporrebbe dei doveri di vigilanza, che come si è avuto modo di vedere sono esclusi dalla legge), quanto piuttosto nella prospettiva *ex post*, cioè nel periodo di permanenza e protrazione del reato su Internet dopo che la piattaforma digitale

[60]BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 601.

abbia avuto modo di conoscere dell'esistenza, sui propri servizi, del contenuto illecito.[61]

Per ragioni attinenti alla fluidità dell'elaborato i problemi appena menzionati verranno affrontati nel seguente ordine: (I) in primo luogo verrà analizzato il problema dell'omesso impedimento del reato *ex ante* ai sensi dell'articolo 40 comma 2 c.p.; (II) in secondo luogo si discorrerà della tipicità della condotta in contesti totalmente automatizzati e infine (III) verrà affrontato il problema della responsabilità *ex post* derivante dalla permanenza e protrazione del reato su Internet.

4.1.1. L'inapplicabilità dell'articolo 40, comma 2 c.p.: nessun dovere di vigilanza per i *providers*.

Come anticipato, una delle principali tensioni con le categorie penalistiche generali nate dall'evoluzione di Internet riguarda la possibilità di imputare alla piattaforma digitale una responsabilità penale da omesso impedimento del reato *ex* articolo 40 co. 2 c.p. secondo cui «[n]on impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo».

Affinché una responsabilità da omesso impedimento del reato sia ascrivibile ad un determinato soggetto – nel caso di specie, al gestore della piattaforma – è necessario che in capo ad esso sia individuabile un obbligo giuridico di impedire il reato oppure una c.d. "posizione di garanzia".

Occorre, in tal senso, distinguere le posizioni di garanzia dagli obblighi giuridici di impedire il reato: (I) per posizione di garanzia si intende una particolare relazione che intercorre tra un soggetto e alcuni beni meritevoli di protezione (c.d. "posizioni o obblighi di protezione") oppure tra un soggetto e determinate fonti di pericolo sulle quali il soggetto ha una sorta di signorìa – o meglio, un legame sostanziale – che gli consente di esercitare un'attività di controllo (c.d. "posizioni o obblighi di controllo"); (II) per obbligo giuridico di impedire il reato s'intende l'individuazione di un comportamento determinato che il soggetto è tenuto ad adottare per proteggere il bene meritevole di tutela o controllare la fonte pericolosa da cui può derivare un pregiudizio.[62]

[61]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 601.
[62]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 602.

È chiaro, dunque, come tra posizione di garanzia e obbligo giuridico di impedire il reato esista una sorta di rapporto *genus* a *species*, con la conseguenza inevitabile che all'assenza di posizioni di garanzia corrisponde un'assenza di obblighi giuridici di impedire il reato.[63]

Dunque, vien da chiedersi se in capo al *provider* possa configurarsi una posizione di garanzia dalla quale far discendere obblighi giuridici di impedire il reato, siano essi di protezione o di controllo.

Secondo dottrina maggioritaria, [64] rispetto al *provider* non solo non si configurano obblighi giuridici di impedire il reato, ma nemmeno posizioni di garanzia, né di controllo, né di protezione: (I) sotto il primo profilo, non solo manca una norma che fondi un generale obbligo di impedire i reati degli utenti, ma inoltre, il legislatore italiano, recependo la Direttiva 2000/31/EC con il d.lgs. n. 70 del 2003, ha escluso – come abbiamo avuto modo di vedere ad inizio capitolo – un obbligo generale di mera sorveglianza (articolo 17 d.lgs. n. 70 del 2003), né tantomeno il DSA apporta delle innovazioni al riguardo;[65] (II) sotto il secondo profilo, se in capo al prestatore di servizi della società dell'informazione si assume una posizione di controllo, non solo, da un lato, l'utente non ha peculiarità che lo rendono di per sé pericoloso, ma dall'altro lato il *provider* non ha alcun legame sostanziale (quella «signorìa» di cui sopra) con la fonte pericolosa, cioè l'utente; se invece, in capo al *provider*, si assume una posizione di protezione, non sembra sia configurabile come bene giuridico da proteggere una "rete sana", rispetto al quale il *provider* assume una posizione di protezione da ogni fonte di pericolo.[66]

---

[63]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 602.

[64]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 602. Nello stesso senso anche DI AGOSTA, *Il caso "Pirate Bay" arriva alla Cedu: spunti per una riflessione sulla responsabilità degli "internet service provider", tra libertà d'espressione e reati in materia di "copyright"*, Nota a Corte eur. Dir. Uomo sez. V 13 marzo 2013 (Neij e Sunde Kolmisoppi c. Svezia), in *Cassazione penale*, 10, 2013, 3379 s.; INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?, Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*. In: (a cura di): LUPÁRIA, Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale, Milano, 2012, 34.
Nello stesso senso TERRACINA, *La tutela penale del diritto d'autore*, cit., 162 s.

[65]«Inoltre, un obbligo di impedimento non si può ricavare né dagli obblighi di rimozione degli effetti derivanti da reati già realizzati (v. ad esempio artt. 14, comma, 3, 15, comma 2 e 16, comma 3, d.lgs. n. 70/2003), né dagli obblighi di segnalazione di illeciti (v. art. 17, comma 2, d.lgs. n. 70/2003, e art. 14-ter, l. n. 269/1998): oltre ad avere questi ultimi finalità diverse, orientate alla collaborazione con le autorità, entrambe queste tipologie di obbligo presuppongono attività illecite già verificatesi». Così, BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 602.

[66]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 602.

Per concludere, dunque, in capo al *provider*, mancano poteri per impedire il verificarsi dei reati non solo di fatto – per impossibilità di esercitare il controllo sui contenuti –, ma anche giuridici: da un lato, infatti, la disciplina di cui agli articoli 14 ss. d.lgs. n. 70 del 2003 e del nuovo Regolamento DSA, consente al *provider* di impedire l'accesso al materiale immesso dagli utenti e di rimuoverli solo a seguito di richiesta della persona offesa – o dell'autorità giudiziaria o amministrativa, o ancora dei segnalatori attendibili –, oppure qualora tali contenuti risultino manifestamente illeciti; dall'altro, il *provider* non ha obblighi né di protezione, né di controllo, in quanto mancano, rispettivamente, sia beni da proteggere particolarmente vulnerabili (una «rete sana»), sia una relazione tra *provider* e fonte pericolosa (l'utente).[67]

4.1.2. La mancanza della tipicità della condotta in contesti totalmente automatizzati.

Posto che, come si vedrà, risulta pacifica, tanto in ambito domestico che comunitario, l'esistenza di una responsabilità in capo al prestatore del servizio della società dell'informazione– per i reati commessi attraverso le sue strutture – quando questo tiene un atteggiamento «attivo», tocca adesso affrontare la questione sulle caratteristiche della condotta tipica in contesti totalmente automatizzati.

È indubbio che, ai fini di inquadrare una responsabilità penale in capo al *provider*, è necessaria una condotta diversa e ulteriore rispetto al comportamento «totalmente automatico». Di fondamentale importanza risulta dunque capire quale sia il *discrimen* per distinguere una condotta totalmente automatica, che non fa sorgere alcuna sorta di responsabilità, da un comportamento «parzialmente automatico» passibile di sanzione penale.

Su questo punto, assodata la responsabilità dei *blogger* o coordinatori di *forum*[68] che hanno potere di filtro o moderazione, esistono due diverse interpretazioni: da una parte l'indicizzazione, la selezione e l'organizzazione dei

[67] Un esempio può essere utile a comprendere meglio quest'ultimo caso: si pensi all'assenza di un obbligo di controllo in capo alle forze dell'ordine. La funzione di prevenzione esercitate dallo Stato tramite le forze dell'ordine non muove dalla premessa che tutti i cittadini siano pericolosi da tenere di continuo sotto controllo. Da ciò ne consegue che l'omissione delle forze dell'ordine sarà incriminabile solo attraverso una fattispecie ad hoc. Tale discorso vale dunque, a fortiori per i *service providers*. Così, TERRACINA, *La tutela penale del diritto d'autore*, cit., 165.
[68] INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 20 s.

contenuti vengono considerate *quid pluris* con la conseguenza che è sufficiente che il *provider* intervenga in qualche modo sulla circolazione dei contenuti affinché la condotta possa essere qualificata come tipica, e dunque punibile; dall'altra si ritiene necessario scomporre ulteriormente le singole attività – di indicizzazione, selezione e organizzazione dei contenuti – per verificare se al loro interno siano presenti automatismi o no.[69]

Dunque, scegliere il criterio da adottare per definire una determinata condotta come totalmente automatica o meno risulta determinante: se ci si muove in una prospettiva civilistica che identifica il totale automatismo con una totale neutralità del *provider*, sarebbe sufficiente individuare un interesse economico in capo all'operatore per considerarlo responsabile; se al contrario il totale automatismo si fa coincidere con la mancanza di una condotta umana previamente finalizzata a legarsi alla condotta dell'utente, allora la responsabilità penale dell'*Internet Service Provider* si potrà escludere tutte le volte in cui l'operatore abbia predisposto dei dispositivi che operano in modo predefinito rispetto all'attività dell'utente. In ossequio al principio di *extrema-ratio* che permea la materia del diritto penale generale, la presente dissertazione avvalora quest'ultima interpretazione.

Dunque, in caso di condotte totalmente automatizzate non è possibile parlare di *provider* «attivo»: ciò esclude la responsabilità dello stesso per assenza della condotta tipica. Si badi bene, però, che ciò non toglie che al *provider* possa imputarsi una responsabilità omissiva dello stesso rispetto ad un reato già verificatosi – e commesso dall'utente – e del quale la piattaforma venga a conoscenza. Il successivo paragrafo si occuperà di analizzare quest'ultima ipotesi.

4.1.3. La soluzione della responsabilità *ex post*, rispetto a un reato già commesso.

L'ultima questione problematica viene dunque ad esistenza: quella relativa alla responsabilità del *provider* rispetto a reati già commessi dagli utenti. In questa ipotesi vengono alla luce tutte quelle disposizioni del Regolamento DSA e del d.lgs. n. 70 del 2003 che impongono alle piattaforme digitali di rimuovere dal proprio

[69]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 605.

server i contenuti illeciti memorizzati o di limitare l'accesso ai siti che contengono tale materiale: ci si riferisce all'articolo 18 («Notifica di sospetti reati»)[70] e 51(3)(b) del DSA[71] e agli articoli 14, comma 3, 15, comma 2 e 16, comma 3 del decreto succitato, secondo cui «l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle sue attività, impedisca o ponga fine alle violazioni commesse».

Inoltre, l'art. 14-*quater* della legge n. 269 del 1998[72] chiarisce come «i fornitori di connettività alla rete internet, al fine di impedire l'accesso ai siti segnalati dal Centro[73], sono obbligati ad utilizzare gli strumenti di filtraggio e le relative soluzioni tecnologiche».

[70]Art. 18 Regolamento (UE) 2022/2065: «1. Qualora venga a conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone, il prestatore di servizi di memorizzazione di informazioni informa senza indugio le autorità giudiziarie o di contrasto dello Stato membro o degli Stati membri interessati in merito ai propri sospetti, fornendo tutte le informazioni pertinenti disponibili. 2. Se non è in grado di individuare con ragionevole certezza lo Stato membro interessato, il prestatore di servizi di memorizzazione di informazioni ne informa Europol o le autorità di contrasto dello Stato membro in cui il suo rappresentante legale risiede o è stabilito, o entrambi. Ai fini del presente articolo, lo Stato membro interessato è lo Stato membro in cui si sospetta che sia stato commesso, si stia commettendo o sarà probabilmente commesso il reato o lo Stato membro in cui risiede o si trova il presunto autore del reato oppure lo Stato membro in cui risiede o si trova la vittima del presunto reato».

[71]Art. 51, para. 3, lett. b), Regolamento (UE) 2022/2065: «Ove necessario per lo svolgimento dei loro compiti ai sensi del presente regolamento, qualora siano stati esauriti tutti gli altri poteri previsti dal presente articolo per far cessare la violazione e a quest'ultima non sia stato posto rimedio o prosegua e causi un danno grave che non può essere evitato mediante l'esercizio di altri poteri previsti dal diritto dell'Unione o nazionale, i coordinatori dei servizi digitali dispongono anche, nei confronti dei fornitori di servizi intermediari che ricadono nella competenza del loro Stato membro, del potere di adottare le misure seguenti: […] b) se il coordinatore dei servizi digitali ritiene che un fornitore di servizi intermediari non si sia sufficientemente conformato agli obblighi di cui alla lettera a) e che alla violazione non sia stato posto rimedio o prosegua e causi un danno grave e integri un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, chiedere all'autorità giudiziaria competente del suo Stato membro di ordinare la restrizione temporanea dell'accesso al servizio interessato dalla violazione da parte dei destinatari o, unicamente qualora ciò non sia tecnicamente fattibile, la restrizione dell'accesso all'interfaccia online del fornitore di servizi intermediari sulla quale ha luogo la violazione».

[72]L. n. 269 del 1998, «Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù'».

[73]Centro nazionale per il contrasto della pedopornografia sulla rete Internet, disciplinato dall'art. 14-*bis* l. 269/1998 che recita «[p]resso l'organo del Ministero dell'interno di cui al comma 2 dell'articolo 14, è istituito il Centro nazionale per il contrasto della pedopornografia sulla rete Internet, di seguito denominato 'Centro', con il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi della rete internet e di altre reti di comunicazione, nonché i gestori e gli eventuali beneficiari dei relativi pagamenti».

Infine, l'art. 163 della legge n. 633 del 1941 stabilisce che «il titolare di un diritto di utilizzazione economica può chiedere che sia disposta l'inibitoria di qualsiasi attività che costituisca violazione del diritto stesso, secondo le norme del codice di procedura civile concernenti i procedimenti cautelari».

Secondo alcuni[74], l'inottemperanza agli ordini inquadrati dalle norme succitate integra fattispecie omissive proprie[75] incentrate sulla norma di cui all'art. 388 c.p., il quale punisce chiunque realizzi una serie di comportamenti al fine di sottrarsi all'adempimento degli obblighi stabiliti mediante un provvedimento dell'autorità giudiziaria, c.d. "mancata esecuzione dolosa di un provvedimento del giudice".

Tale dissertazione non intende condividere tale lettura in quanto ridurrebbe l'applicabilità delle fattispecie penali ai soli casi nei quali sia presente «un provvedimento dell'autorità giudiziaria», con l'esclusione di ogni rilevanza penale nei casi in cui il provvedimento venga emesso da un'autorità amministrativa o altra entità comunque capace di inviare comunicazioni «qualificate».

Per tale motivo ci si sente di sostenere una lettura diversa, e più ardita, avanzata da altri:[76] questa configurerebbe una responsabilità concorsuale del *provider* non tanto per omesso impedimento *ex ante* del reato (che abbiamo visto non essere possibile a causa della mancanza di posizioni di garanzia in capo al *provider*), quanto invece per omesso impedimento di protrazione *ex post* del reato stesso: in particolari settori, ad esempio riguardo la tutela del diritto d'autore, è stato affermato che «l'interpretazione sistematica di queste disposizioni non esclude la responsabilità penale dell'ISP […], essendo egli dotato di un effettivo potere-dovere di interferenza per impedire la prosecuzione delle violazioni».[77]

Tale lettura è particolarmente interessante: si può ritenere infatti che, una volta che il *provider* sia venuto a conoscenza della presenza di un reato sulla rete commesso dall'utente – conoscenza derivante da una comunicazione qualificata

[74]Cfr. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 34 s.
[75]Sono reati omissivi propri quelli nei quali il legislatore reprime il mancato compimento di un'azione giuridicamente doverosa, indipendentemente dal verificarsi o meno di un evento come conseguenza dell'omissione.
[76]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 606; DI AGOSTA, *Il caso Pirate Bay arriva alla CEDU*, cit., 3381.
[77]Cfr. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet*, Milano, 2010, 458

(provvedimento dell'autorità giudiziaria o amministrativa o dei nuovi *trusted flaggers*)–, si venga a creare quel legame sostanziale tra *provider* e fonte pericolosa (non l'utente potenziale *reo*, ma la rete, che dopo la memorizzazione del contenuto illecito diviene «pericolosa»)[78] che contraddistingue le posizioni di garanzia, e crea in questo caso obblighi di controllo in capo al *provider* che risulta dotato di poteri fattuali e giuridici, adesso sì, di interdizione. Si parla in tal caso di concorso mediante omissione nel reato commissivo compiuto da altri. A confermare la bontà di tale lettura è stata la stessa Suprema Corte che, correggendo il precedente orientamento volto ad escludere una responsabilità penale degli *Internet Service Provider* sugli *user-generated content*[79] (nel caso di specie, commenti diffamatori), individua nel gestore del sito un concorrente del reato di diffamazione in quanto avrebbe dovuto eliminare il commento diffamatorio dopo aver ricevuto una mail che chiariva la natura diffamatoria del commento stesso.[80]

Resta ora da capire quando scatta l'obbligo di attivarsi a rimuovere il contenuto illecito o limitare l'accesso al materiale, attivazione in mancanza della quale, per l'appunto, può scaturire la responsabilità penale del *provider* per omesso impedimento di protrazione *ex post* del reato.

Le norme succitate fanno espresso riferimento all'esistenza di un provvedimento dell'autorità giudiziaria o amministrativa; tuttavia, altre disposizioni fanno riferimento alla conoscenza dell'illecito anche a seguito di una mera comunicazione pur sempre qualificata, a nulla rilevando l'esistenza di un vero e proprio provvedimento: si tratta dell'articolo 16 co. 2 lett. b del d.lgs. n. 70 del 2003 il quale stabilisce che il prestatore di un servizio della società dell'informazione – che consiste nella memorizzazione di informazioni fornite da

[78]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 606. Nello stesso senso anche TERRACINA, *La tutela penale del diritto d'autore*, cit., 185: «Deve, infine, tenersi in considerazione il fatto che, come già accennato, nel nostro ordinamento penale la responsabilità ai sensi del capoverso dell'art. 40 c.p. appare ammissibile solamente in relazione alla protezione di diritti fondamentali quali la vita o l'incolumità fisica e non certo per interessi di carattere patrimoniale quali quelli tutelati dalla LDA. Diverso potrebbe apparire il discorso nell'ipotesi in cui, una volta individuata l'attività illecita posta in essere attraverso *Internet* venga invitato il *provider* a provvedere con i mezzi tecnici a sua disposizione a rimuoverla dalla Rete. In questo caso, infatti, potrebbe configurarsi una sorta di 'messa in mora' del *provider* alla quale, in una prospettiva *de iure condendo*, potrebbe ricollegarsi una qualche responsabilità penale».

[79]Tale opinabile orientamento affermava infatti che il d.lgs. n. 70 del 2003 di attuazione della *E-commerce Directive*, disciplinando unicamente la responsabilità civile dell'ISP, avesse implicitamente escluso la relativa responsabilità penale.

[80]Cfr. Cass. pen., Sez. V, 14 luglio 2016, n. 54946.

un destinatario del servizio – non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore «non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso».

Con l'emanazione del nuovo Regolamento *Digital Service Act*, il legislatore comunitario ha ampliato la cerchia di soggetti capaci di inviare comunicazioni «qualificate» al titolare della piattaforma digitale: ci si riferisce al segnalatore attendibile, al coordinatore dei servizi digitali[81] e alla Commissione stessa.

Si evidenzia inoltre come, lo stesso Regolamento, all'articolo 18, istituisce, in capo al *provider*, un obbligo giuridico di informare senza indugio le autorità giudiziarie o di contrasto dello Stato membro o degli Stati membri interessati – o, in mancanza, l'Europol o le autorità di contrasto dello Stato membro in cui il suo rappresentante legale risiede o è stabilito –, in merito ai propri sospetti, fornendo tutte le informazioni pertinenti disponibili.

Si badi bene, però, che tale obbligo nasce qualora il *provider* venga a conoscenza di informazioni che facciano sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una «minaccia per la vita o la sicurezza di una o più persone»: tale obbligo non verrebbe ad esistenza nel caso di violazioni della proprietà intellettuale, salvi casi eccezionali.[82]

Dunque, il *discrimen* risulta essere il carattere qualificato della comunicazione, a prescindere dall'esistenza di un vero e proprio provvedimento; ciò che infatti va evitato è che una responsabilità penale venga imputata quando il *provider* acquisisce la conoscenza del contenuto illecito o autonomamente o tramite comunicazioni provenienti da soggetti privi di autorità, cioè in presenza di situazioni incerte e opinabili (tuttavia in tali casi, come si vedrà, è possibile imputare una responsabilità civile).[83]

Se infatti l'obbligo di rimuovere il contenuto illecito o limitare l'accesso al materiale scattasse in queste ipotesi, pena una responsabilità di carattere penale si

[81]Il coordinatore dei servizi digitali è un'autorità indipendente che sarà responsabile della vigilanza dei servizi di intermediazione stabiliti nel proprio Stato membro e/o del coordinamento con autorità specializzate nel settore. A tal fine potrà infliggere sanzioni o anche ammende.
[82]Si pensi, ad esempio, alla vendita di farmaci contraffatti.
[83]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 606

verificherebbe il c.d. "dilemma del provider", che consiste in una alternativa: ritenere esistente l'illecito e quindi rimuovere il contenuto, esponendosi così, sul piano privatistico al rischio di pretese risarcitorie dell'utente, nonché sul piano pubblicistico ad una censura privata lesiva del diritto di libertà d'espressione; oppure ritenere l'illecito inesistente e quindi non rimuovere, esponendosi però al rischio di concorrere nel reato tramite la responsabilità omissiva di protrazione del reato *ex post* di cui sopra.

In conclusione, sembra dunque potersi affermare come il gestore della piattaforma digitale possa essere imputato di una responsabilità penale ogniqualvolta, a seguito di una comunicazione o segnalazione «qualificata» nei termini su descritti, che fa sorgere in lui una posizione di garanzia – nella specie, posizioni controllo, a causa del legame sostanziale che si crea tra *provider* e fonte pericolosa (la rete) –, ometta di rimuovere il contenuto illecito, o limitarne l'accesso concorre mediante omissione nel reato imputabile all'utente.

Conclusa così l'analisi della responsabilità penale dell'*Internet Service Provider*, il prossimo paragrafo tratterà della loro responsabilità civile.

4.2. La responsabilità civile dell'Internet Service Provider.

Nell'analizzare la responsabilità civile del *provider* non si può prescindere dal richiamare il già più volte citato d.lgs. n. 70 del 2003: gli articoli 14-16 infatti, precedentemente analizzati, ne tracciano la disciplina.

Come anticipato, gli articoli 14, 15 e 16 del d.lgs. n. 70 del 2003 distinguono tre differenti comportamenti del *provider* che richiedono altrettanti differenti requisiti per fondare una responsabilità: (I) l'articolo 14 disciplina il comportamento di accesso e trasmissione dati (c.d. "*mere conduit*"), rispetto al quale il provider risulta responsabile se è presente un *quid pluris*, e cioè dà origine alla trasmissione, seleziona il destinatario della trasmissione oppure seleziona o modifica le informazioni trasmesse (tutte attività che consentono al provider di conoscere l'illecito senza ricevere una comunicazione qualificata); (II) l'articolo 16 regola il comportamento di "memorizzazione duratura" (c.d. "*hosting*"), rispetto al quale l'ISP può essere ritenuto responsabile a prescindere dal *quid pluris* di cui sopra, e cioè quando «sia effettivamente a conoscenza del fatto che l'attività l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al

corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione»,[84] oppure quando, avendo ricevuto una comunicazione dalle autorità competenti, non abbia agito immediatamente per «rimuovere le informazioni o per disabilitarne l'accesso»;[85] (III) l'articolo 15 disciplina infine il comportamento di «memorizzazione temporanea» (c.d. "*caching*"), che si colloca a metà strada tra l'accesso e trasmissione dati, da un lato, e memorizzazione duratura, dall'altra: coerentemente a ciò, il legislatore, ai fini dell'imputazione di responsabilità civile, prevede da un lato un *quid pluris ex* articolo 15, co. 1, lettere da a) a d),[86] e dall'altro una conoscenza anche non qualificata *ex* articolo 15, co.1, lettera e).[87]

Tuttavia, nonostante lo sforzo posto in essere dal Legislatore Comunitario prima, e Italiano poi, rispettivamente con la Direttiva 200/31/CE e il suo decreto di ricezione d.lgs. n. 70 del 2003, i principi ivi stabiliti in materia di responsabilità civile degli *Internet Service Provider*, succitati, sono stati spesso reinterpretati da dottrina e giurisprudenza in modo tale da minarne la certezza applicativa.[88]

In particolare, due sono le ipotesi che consentono di imputare una responsabilità civile in capo al *provider*: (I) una prima ipotesi si verifica qualora il prestatore di servizi della società dell'informazione tenga una condotta «attiva»; (II) una seconda ipotesi, alternativa alla prima, richiede la conoscenza dell'illecito da parte del *provider*; a differenza però di quanto appena visto in materia di responsabilità penale, in cui non è sufficiente la «mera» conoscenza dell'illecito ma è necessario che tale conoscenza derivi da una comunicazione «qualificata», nell'ambito della responsabilità civile è necessaria ma allo stesso tempo sufficiente

[84]Art. 16 lett. a) d.lgs. n. 70 del 2003.
[85]Art. 16 lett. b) d.lgs. n. 70 del 2003.
[86]Il *quid pluris* di cui alle lettere a) - d) cui ci si riferisce attiene, rispettivamente, alle condotte di modificare le informazioni, conformarsi alle condizioni di accesso alle informazioni, conformarsi alle norme di aggiornamento delle informazioni indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese nel settore, interferire con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni. In presenza di tali condotte l'ISP, che offre un servizio di *caching*, è imputabile di responsabilità.
[87]Ai sensi della lettera e), l'ISP che offre un servizio di *caching*, è responsabile se non agisce prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.
[88]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee*, cit., 2074.

la pura e schietta conoscenza dell'illecito a prescindere dalla fonte da cui deriva tale conoscenza. Si procederà, dunque, nei prossimi paragrafi ad analizzare entrambe le ipotesi succitate, per poi infine esaminare quale tipologia di responsabilità civile – se aquiliana o contrattuale – sia da imputare al gestore della piattaforma digitale.

4.2.1. L'hosting provider «attivo».

Negli anni successivi all'entrata in vigore del d.lgs. n. 70 del 2003, la Giurisprudenza ha contribuito alla creazione di una nuova figura di *provider*, in aggiunta alle figure analizzate precedentemente: si tratta del c.d. "*hosting attivo*" che si caratterizza per fare «qualcosa di più» rispetto alla mera attività di ospitare un contenuto, ad esempio perché lo indicizza, lo controlla o lo promuove.[89]

In *Reti Televisive Italiane S.p.A. c. Italia On Line S.r.l.*[90], l'approccio non neutro di Italia On Line s.r.l. ("IOL") rispetto ai contenuti condivisi dagli utenti ospitati sul c.d. "Portale IOL" ha condotto il Tribunale di Milano a escludere l'esenzione di responsabilità prevista dall'articolo 16 d.lgs. n. 70 del 2003, dovendosi applicare l'articolo 17 del medesimo decreto anche all'hosting attivo. Infatti, IOL avrebbe disatteso gli obblighi previsti da quest'ultima norma in quanto, pur messo al corrente dell'illiceità dei video ospitati dalla diffida di RTI, non ha agito di conseguenza rimuovendoli o limitandone l'accesso.

Ciò detto, risulta particolarmente importante definire la distinzione tra hosting «attivo» e «passivo» e analizzare il momento – e modo – in cui un *provider* viene a conoscenza dell'illiceità dei contenuti che ospita, dato il regime di responsabilità che da quel momento in avanti incomberà sull'ISP. Come anticipato, il Tribunale di Milano non ha applicato le esenzioni *ex* articolo 16 del d.lgs. n. 70

[89]«In effetti la situazione attuale rende evidente che le modalità di prestazione di tale servizio - ormai del tutto comuni ai soggetti che svolgono attività analoghe - si sono distaccate dalla figura individuata nella normativa comunitaria, mentre i servizi offerti si estendono ben al di là della predisposizione del solo processo tecnico che consente di attivare e fornire "accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione", finendo nell'individuare (se non un vero e proprio content provider, soggetto cioè che immette contenuti propri o di terzi nella rete e che dunque risponde di essi secondo le regole comuni di responsabilità) una diversa figura di prestatore di servizi non completamente passivo e neutro rispetto all'organizzazione della gestione dei contenuti immessi dagli utenti (cd. hosting attivo), organizzazione da cui trae anche sostegno finanziario in ragione dello sfruttamento pubblicitario connesso alla presentazione (organizzata) di tali contenuti». Cfr. Trib. Milano, 7 giugno 2011, n. 7680.

[90]Cfr. Trib. Milano, cit., 7680/2011.

del 2003 in quanto IOL è stato considerato «hosting attivo»: tale attribuzione è stata giustificata sulla base del considerando 42 della Direttiva *E-commerce*, secondo cui le esenzioni di responsabilità a favore degli ISP per contenuti generati dagli utenti, riguardano quei *providers* la cui attività «è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni [...] memorizzate»[91] – c.d. "principio di neutralità tecnica".

Diverse decisioni domestiche[92] hanno fatto riferimento alla categoria di «*hosting* attivo», tutte concordi sull'inapplicabilità delle esenzioni di cui all'articolo 16 del d.lgs. n. 70 del 2003 ai *providers* che non abbiano tenuto condotte neutre nei confronti dei contenuti generati dagli utenti. Tali principi sono stati riconosciuti anche in ambito comunitario, dalla Corte di Giustizia in due sentenze riguardanti, rispettivamente, la memorizzazione di messaggi pubblicitari da parte di Google[93] e la memorizzazione di oggetti destinati alla vendita all'asta da parte di Ebay.[94]

---

[91] Considerando (42) Direttiva 2000/31/CE: «Le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate».

[92]Il Trib. di Roma, con sentenza 10 gennaio 2019, n. 693, (c.d. caso Vimeo) ha statuito che va considerato *hosting* attivo non solo chi manipola i contenuti oggetto dei suoi servizi, ma anche chi svolge un'attività che va al di là della semplice predisposizione di un processo tecnico e neutrale consistente, ad esempio: (i) nella selezione, organizzazione ed indicizzazione del materiale trasmesso; (ii) nell'operare come un sito di condivisione video; (iii) nel mettere a disposizione dei propri utenti un motore di ricerca interno e (iv) nel ricavare un lucro dallo sfruttamento pubblicitario dei contenuti così selezionati ed organizzati.

[93]CGUE, 23 marzo 2010, Google France, già citata: «L'art. 14 della direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), deve essere interpretato nel senso che la norma ivi contenuta si applica al prestatore di un servizio di posizionamento su Internet qualora detto prestatore non abbia svolto un ruolo attivo atto a conferirgli la conoscenza o il controllo dei dati memorizzati. Se non ha svolto un siffatto ruolo, detto prestatore non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi».

[94]CGUE, 12 luglio 2011, *L'Oréal, già citata*: «L'art. 14, n. 1, della direttiva del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico»), deve essere interpretato nel senso che esso si applica al gestore di un mercato online qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati. Detto gestore svolge un ruolo siffatto allorché presta un'assistenza che consiste in particolare nell'ottimizzare la presentazione delle offerte in vendita di cui trattasi o nel promuoverle. Quando non ha svolto un ruolo attivo nel senso indicato al comma precedente e

Chiarito come un *hosting provider* può essere considerato responsabile per i contenuti immessi dagli user, se «attivo», resta da capire quando tale attributo può imputarsi al *provider*. Il Tribunale di Milano, nel caso succitato, ha considerato IOL un hosting attivo in quanto: (I) forniva e organizzava un sistema automatico di servizi pubblicitari che permetteva l'associazione di messaggi promozionali ai video degli utenti; (II) faceva sottoscrivere ai suoi utenti dei contratti che prevedevano una licenza non esclusiva per l'esercizio dei diritti di riproduzione e adattamento inerenti ai video caricati, una manleva in caso di richieste risarcitorie dovute all'illiceità degli stessi e il diritto di IOL di rimuoverli se in violazione dei diritti di terzi; (III) aveva predisposto un servizio di «segnala abuso» tramite il quale i detentori dei diritti potevano indicare i video ospitati e richiedere una rimozione selettiva; (IV) forniva un servizio automatico di «video correlati» consistente nella visualizzazione, a lato o sotto il video in riproduzione, di altri contenuti a esso in qualche modo associati.[95]

La correttezza dell'analisi del Tribunale di Milano va valutata in base all'idoneità delle quattro condotte appena elencate a porre IOL al di fuori della categoria di *hosting provider* così come prevista dal considerando 42 della Direttiva. Ciò potrebbe avvenire, secondo la Corte di Giustizia, se il *provider* «anziché limitarsi ad una fornitura neutra [del servizio], mediante un trattamento puramente tecnico e automatico dei dati forniti dai suoi clienti, svolge[sse] un ruolo attivo atto a conferirgli una conoscenza o un controllo di tali dati».[96]

Dunque, due sarebbero gli elementi, alternativi, che consentirebbero di qualificare un *provider* come «attivo»: la conoscenza o il controllo dei «dati» immessi nella rete dagli utenti. Ebbene, secondo parte di dottrina,[97] gli elementi

---

dunque la sua prestazione di servizio rientra nell'ambito di applicazione dell'art. 14, n. 1, della direttiva 2000/31, il gestore di un mercato online, in una causa che può comportare una condanna al pagamento di un risarcimento dei danni non può tuttavia avvalersi dell'esonero dalla responsabilità previsto nella suddetta disposizione qualora sia stato al corrente di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità delle offerte in vendita di cui trattasi e, nell'ipotesi in cui ne sia stato al corrente, non abbia prontamente agito conformemente al n. 1, lett. b), del suddetto art. 14».

[95]Cfr. BELLAN, *Per una reasonable liability*, cit., 255 s.

[96]CGUE, 23 marzo 2010, *Google France*, già citata, para. 114 e 120; CGUE, 12 luglio 2011, *L'Oréal,* già citata, para. 113.

[97]Cfr. BELLAN, *Per una reasonable liability*, cit., 255 s.

individuati dal Tribunale di Milano non sembrano fondare la conoscenza o il controllo di IOL sui video generati dagli utenti.

Riguardo la «conoscenza», quella parte di dottrina ritiene che il Tribunale di Milano lasci intendere che IOL abbia saputo dell'esistenza dei video illeciti solo successivamente alla ricezione della diffida di RTI.

La questione risulta più complessa con riferimento al «controllo», termine ampio che può essere oggetto di varie interpretazioni. Tuttavia, la Corte di Giustizia, pur non avendolo espressamente definito, ha fatto riferimento a due criteri interpretativi utili al fine di carpire il significato del termine. Il primo criterio è quello secondo cui l'esclusione delle esenzioni di responsabilità va valutata caso per caso, non potendo essere «intrappolata» sotto una regola rigida: in particolare, bisogna tenere conto delle «modalità concrete della fornitura del servizio» da parte del *provider*.[98] Il secondo criterio interpretativo guarda alla natura dei comportamenti che non sono idonei a conferire al *provider* «controllo» e «conoscenza» sui contenuti: la Corte spiega come rientrino in questa categoria i trattamenti meramente tecnici e automatici dei contenuti degli utenti da parte del provider.

Tornando al caso IOL, il Tribunale di Milano ha riconosciuto che il servizio (offerto dal *provider*) si svolgeva su base automatica e tecnica, *i.e.* senza intervento umano. Ciò è indice di mancanza di «controllo» in capo a IOL. Lo stesso può e deve dirsi per la messa a disposizione del servizio «segnala abuso», già citato. Si tratta, infatti, di un servizio automatico che il Tribunale di Milano interpreta come «un impegno alla verifica della legittimità dei contenuti immessi autonomamente dagli utenti ove vi fosse una segnalazione in tal senso». Tale interpretazione non sembra essere condivisibile: se da un lato è vero che in assenza di segnalazione non c'è spazio per interventi umani discrezionali da parte del *provider*, e che una segnalazione può metterlo nella posizione di conoscere o controllare il contenuto segnalato (e, lo si ripete, ciò può ingenerare una responsabilità), d'altro lato, tuttavia, la mera messa a disposizione del servizio di segnalazione non ingenera nel *provider* una conoscenza o un controllo sui contenuti generati dagli utenti. Dunque,

[98]CGUE, 23 marzo 2010, Google France, già citata, para. 119. Nello stesso senso, CGUE, 12 luglio 2011, *L'Oréal,* già citata, para. 115 e 117.

scopo della dissertazione è quello di chiarire come, coerentemente con il considerando 42 della *E-commerce Directive*, non può esistere una responsabilità oggettiva in capo al *provider*, fatta eccezione per i casi in cui abbiano conoscenza o controllo dei contenuti illeciti generati dagli utenti (nel qual caso saranno «attivi»). La qualifica di *provider* «attivo», dunque, può essere giustificata solo sulla base di comportamenti che consentono concretamente all'ISP di conoscere o controllare i contenuti illeciti di cui trattasi.

Per tali motivi, il presente elaborato supporta quel filone della dottrina[99] secondo cui applicare a IOL, nel caso di specie, una responsabilità oggettiva sulla base degli elementi tecnici, automatici e passivi individuati dal Tribunale nel corso dell'istruttoria non è condivisibile.

Uno dei contributi più importanti in materia è fornito dalla Suprema Corte, con le sentenze 19 marzo 2019, n. 7708-7709,[100] c.d. "sorelle", poiché vertenti di fatto su situazioni analoghe. La Corte, muovendosi coerentemente con quanto stabilito dalle già citate sentenze della Corte di Giustizia e dalla comunicazione della Commissione Europea COM (2017) 555 del 28 settembre 2017,[101] ripete come la nozione di «*hosting provider* attivo» debba essere riferita a tutte quelle fattispecie che esulano da una attività dei prestatori di servizi della società dell'informazione che sia di ordine meramente tecnico, automatico e passivo.[102]

---

[99]Cfr. BELLAN, *Per una reasonable liability*, cit., 256.

[100]Cfr. Cass. Civ., Sez. I, 19 marzo 2019, n.7708; Cass. Civ., Sez. I, 19 marzo 2019, n.7709.

[101] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Lotta ai contenuti illeciti online: verso una maggiore responsabilizzazione delle piattaforme online.

[102]Cass. Civ., cit., 7708/2019: «La giurisprudenza recente della Corte di giustizia dell'Unione Europea ha accolto la nozione di "hosting provider attivo", riferita a tutti quei casi che esulano da un'"attività dei prestatori di servizi della società dell'informazione (che) sia di ordine meramente tecnico, automatico e passivo, con la conseguenza che detti prestatori non conoscono nè controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi", mentre "(p)er contro, tali limitazioni di responsabilità non sono applicabili nel caso in cui un prestatore di servizi della società dell'informazione svolga un ruolo attivo", richiamando a tal fine il considerando 42 della direttiva (Corte di giustizia UE 7 agosto 2018, Cooperatieve Vereniging SNB-REACT U.A. c. Deepak Mehta, C-521/17, punti 47 e 48, relativa alla responsabilità di un privato, prestatore di servizi di locazione e registrazione di indirizzi IP che consentivano di utilizzare anonimamente nomi di dominio e siti internet: egli aveva registrato circa 38.000 nomi di dominio internet, che utilizzavano illecitamente segni identici ai marchi appartenenti ad alcuni suoi membri, nonché siti internet sui quali erano illecitamente vendute merci recanti tali segni; Corte di giustizia UE 11 settembre 2014, C-291/13, Sotiris Papasavvas, spec. p. 44; Corte di giustizia UE 12 luglio 2011, C-324/09, L'Orèal c. eBay, cit., punti 112, 113, 116, 123, con riguardo al gestore di un mercato online, il quale svolge un "ruolo attivo" allorché presta un'assistenza che consiste nell'ottimizzare la presentazione delle offerte in vendita o nel promuoverle; Corte di giustizia UE 23 marzo 2010, da C-236/08 a C-238/08, Google c. Luis Vuitton, punti 112, 113, 114 e 120). Con l'ovvia precisazione

La Corte di Cassazione, in particolare, affronta il tema della responsabilità dell'*hosting provider* e del *caching provider*, disciplinate dagli articoli 12 e 14 della Direttiva, nonché dagli articoli 14 e 16 del d.lgs. n. 70 del 2003, articoli che, come testimonia il caso IOL su analizzato, negli anni hanno dimostrato una crescente inadeguatezza a fronte delle trasformazioni di Internet.[103]

Tant'è che negli ultimi anni, la tendenza pretoria ad allargare le maglie di tale disciplina, in favore di un ampliamento dell'ambito di responsabilità dei *provider*, si è diffusa tanto in ambito comunitario quanto in ambito domestico. Ciò, si spiega in ragione del fatto che la complessità tecnica delle attività svolte dai *provider*, nel tempo è aumentata fortemente, e, allo stesso tempo, sono aumentate – grazie all'evoluzione tecnologica – le possibilità per gli stessi di contrastare le attività illecite commesse online da parte degli *user*, in maniera più efficiente e meno invasiva rispetto ai diritti fondamentali della libertà di espressione e di pensiero di questi ultimi.

La Suprema Corte nella due sentenze succitate, consapevole della situazione di incertezza venutasi a creare negli ultimi anni, sente il dovere di affermare la «esigenza di trovare una nuova dogmatica universalmente fruibile, oltre le dogmatiche municipali»,[104] e di sottolineare che «gli esponenti dell'accademia e delle corti, nei rispettivi ruoli, sono chiamati a preservare il valore della certezza del diritto: il che passa anche attraverso la riconduzione ad un sistema concettuale efficiente delle norme di derivazione europea».[105]

---

che la disposizione di cui all'art. 14, comma 1, della direttiva 2000/31/CE deve essere "interpretata non soltanto in considerazione del suo tenore letterale, ma anche del suo contesto e degli scopi perseguiti dalla normativa di cui essa fa parte" (Corte di giustizia UE 12 luglio 2011, C-324/09, L'Orèal c. eBay, cit. punto 111). Ancora di recente, la Corte di giustizia UE (sent. 14 giugno 2017, C-610/15, Stichting Brein), ha affermato che la fornitura e la gestione di una piattaforma di condivisione online, come quella ivi considerata, è atto di comunicazione, ai sensi dell'art. 3, paragrafo 1, della direttiva 2001/29/CE; sebbene in detto giudizio i gestori della piattaforma non fossero parti. La Comunicazione della Commissione Europea COM (2017) 555 del 28 settembre 2017, intitolata "Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online", ha preso parimenti atto dell'orientamento della Corte di giustizia, secondo cui la deroga alla responsabilità di cui all'art. 14 della direttiva è disponibile solo per i prestatori di servizi di hosting "che non rivestono un ruolo attivo" (p. 11). Detta nozione può ormai ritenersi, dunque, un approdo acquisito in ambito comunitario».

[103]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee*, cit., 2073.
[104]Cfr. Cass. Civ., cit., 7708/2019.
[105]Cfr. Cass. Civ., cit., 7708/2019.

In sede di applicazione delle norme riguardanti la responsabilità del *provider*, l'aspetto oggetto di interpretazioni contrastanti è stato il principio di neutralità tecnica, già citato:[106] secondo il Considerando 42 della Direttiva, come si è visto, l'immunità del *provider* opera solo se il prestatore del servizio di Internet, rispetto al materiale condiviso dallo *user*, abbia svolto attività di ordine meramente «tecnico, automatico e passivo», e allo stesso tempo «non conosce, né controlla le informazioni trasmesse o memorizzate».

La conseguenza è dunque la seguente: se non ricorrono tali condizioni, recepite dagli articoli 12-15 della Direttiva e articoli 14-16 del d.lgs. n. 70 del 2003, l'ISP rimane esposto alla disciplina generale della responsabilità civile, perdendo il *favor legis* condizionato, costituito dal regime di immunità appena visto.

Dunque, affinché il regime di immunità venga applicato al fornitore del servizio della società dell'informazione, è necessario che esso tenga un atteggiamento passivo rispetto al contenuto illecito postato dall'utente.[107]

Tuttavia, come si avrà modo di vedere nel successivo paragrafo, bisogna segnalare che il fatto di non aver avuto un ruolo «attivo» non sempre significa mancanza di responsabilità: infatti, il *provider* ha l'obbligo di attivarsi a rimuovere il contenuto o limitarne l'accesso qualora ne venga a conoscenza, anche senza aver svolto un ruolo «attivo»; ciò sarebbe imposto dalla «diligenza professionale tipicamente dovuta», come stabilito dalla Suprema Corte nella prima delle due sentenze in disamina..

Infine, la prima delle due sentenze spiega come gli elementi idonei a verificare «*l'attività*» dell'hosting provider, c.d. "indici di interferenza", siano «a titolo esemplificativo e non necessariamente tutt[i] compresenti: le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare ed

[106]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee*, cit., 2074.
[107]Cfr. Sul tema hosting attivo e passivo, si veda infra Capitolo III 1.

arricchire in modo non passivo la fruizione dei contenuti da parte di utenti determinati».[108]

Tuttavia, secondo alcuni[109] tale principio di diritto soffre di una certa genericità in quanto non spiega quanti e quali degli indici di interferenza succitati debbano essere presenti allo stesso tempo per assegnare all'hosting provider l'attributo «attivo»: ciò finisce per assegnare forse un margine troppo ampio di discrezionalità al giudice di merito nella qualificazione di un *hosting provider* come attivo o meno. contribuendo a migliorare la situazione di incertezza esistente circa la responsabilità del *provider*, ma non di certo a risolverla.

4.2.2. La mera conoscenza del contenuto illecito e la «diligenza professionale tipicamente dovuta».

Oltre ai casi appena visti in cui un *provider* tiene una condotta «attiva», la Corte di Giustizia ha affermato che, anche quando non abbia svolto un ruolo attivo, «il gestore di un mercato online non può tuttavia avvalersi dell'esonero dalla responsabilità [...] qualora sia stato al corrente di fatti o circostanze in base ai quali un operatore diligente avrebbe dovuto constatare l'illiceità delle offerte in vendita di cui trattasi e non abbia prontamente agito conformemente al n. 1, lett. b), del[l'] art. 14».[110]Da ciò si deduce come, diversamente da ciò che avviene in ambito penale, la responsabilità civile del *provider* sorge allorché esso abbia avuto una conoscenza anche non qualificata dell'illiceità del contenuto. Ciò, secondo la Corte può avvenire almeno in due ipotesi: (I) o quando il provider abbia avuto cognizione de «l'esistenza di un'attività o di un'informazione illecite a seguito di un esame effettuato di propria iniziativa», ovvero (II) quando «gli sia notificata l'esistenza di un'attività o di un'informazione siffatte».[111]

Ancora, la Corte di Giustizia, ha affermato che «anche in riferimento al semplice prestatore di un servizio dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio medesimo (c.d. "*hosting* passivo"), va esclusa l'esenzione di responsabilità prevista dall'art. 14 della Direttiva 2000/31 quando lo stesso, dopo aver preso conoscenza, mediante

[108]Cass. Civ., cit., 7708/2019, punto 4.3.
[109]Cfr. DI CIOMMO., *Oltre la direttiva 2000/31/Cee*, cit., 2080.
[110]Cfr. CGUE, 12 luglio 2011, *L'Oréal,* già citata, para. 124.
[111]Cfr. CGUE, 12 luglio 2011, *L'Oréal,* già citata, para. 122.

un'informazione fornita dalla persona lesa o in altro modo, della natura illecita di tali dati o di attività di detti destinatari, abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi».[112]

In conclusione, anche un *provider* che abbia tenuto una condotta neutra e passiva nei confronti della trasmissione o permanenza dei dati illeciti, è tenuto ad attivarsi per la loro rimozione una volta che ne sia venuto a conoscenza per qualsivoglia motivo. È stato così sancito il principio per cui la conoscenza, comunque acquisita (non solo se tramite le autorità competenti o a seguito di esplicita diffida del titolare dei diritti), dell'illiceità dei dati memorizzati fa sorgere la responsabilità civile risarcitoria del prestatore di servizi.

Dal punto di vista domestico, relativamente alla conoscenza dell'illiceità del contenuto generato dall'utente, la quale impone al *provider* di attivarsi al fine di rimuoverlo o limitarne l'accesso, la Suprema Corte si interroga sul significato da attribuire all'articolo 16 comma 1 lett. a del d.lgs. n. 70 del 2003, il quale, al fine della possibile imputazione di responsabilità al prestatore del servizio, richiede che lo stesso sia a conoscenza di fatti che rendano «manifesta» l'illiceità del materiale online: in particolare, la Corte, ritiene che l'*hosting provider* è tenuto a verificar la comunicazione pervenuta e la sua ragionevole fondatezza in base ai criteri della comune esperienza e diligenza professionale tipicamente dovuta.

Se in seguito a tale verifica, l'*hosting provider* dovesse ritenere fondata l'illeceità del materiale generato dall'utente, esso dovrà attivarsi al fine di rimuoverlo o limitarne l'accesso. Ma ciò che di più risulta rilevante, è che la Suprema Corte ha affermato come, anche in mancanza di predetta comunicazione, l'obbligo di attivazione del prestatore del servizio scatterebbe ugualmente nel caso di palese illiceità dei contenuti: come anticipato, ciò sarebbe giustificato dal comune principio per cui ogni consociato è tenuto a comportarsi con la dovuta diligenza.[113]

---

[112]Cfr. CGUE, 23 marzo 2010, Google France, già citata, para. 109.

[113]Cass. Civ., cit., 7708/2019: «L'hosting provider è chiamato quindi a delibare, secondo criteri di comune esperienza, alla stregua della diligenza professionale tipicamente dovuta, la comunicazione pervenuta e la sua ragionevole fondatezza (ovvero, il buon diritto del soggetto che si assume leso, tenuto conto delle norme positive che lo tutelano, come interpretate ad opera della giurisprudenza interna e comunitaria), nonché, in ipotesi di esito positivo della verifica, ad attivarsi rapidamente per eliminare il contenuto segnalato. L'aggettivo vale, in sostanza, a circoscrivere la responsabilità del

Dunque, oggetto di valutazione da parte del giudice ai fini della possibile imputazione della responsabilità, è la condotta che il *provider* tiene in seguito alla conoscenza dell'illiceità dei dati o informazioni generate dagli utenti.

Da ciò risulta chiaro come il legislatore comunitario prima, e nazionale poi, individuano la responsabilità dell'ISP in modo negativo: il suo sorgere è condizionato (I) all'esistenza dell'elemento soggettivo colposo in forma omissiva, quando il *provider* non rimuova o svolga accertamenti o verifiche una volta che sia venuto a conoscenza dell'illecito; oppure (II) all'esistenza dell'elemento soggettivo doloso, quando omette di intervenire pur consapevole dell'antigiuridicità del materiale.[114]

Per concludere, dunque, il tipico scenario risulta essere il seguente: in un primo momento l'utente carica il contenuto illecito su Internet, e in un secondo momento, cioè quando ne prende conoscenza, il prestatore del servizio omette di rimuoverlo.

Il rapporto tra queste due condotte è quello di un concorso sopravvenuto – da parte dell'ISP – nello stesso illecito: all'originaria condotta commissiva dello

prestatore alla fattispecie della colpa grave o del dolo: se l'illiceità deve essere "manifesta", vuol dire che sarebbe possibile riscontrarla senza particolare difficoltà, alla stregua dell'esperienza e della conoscenza tipiche dell'operatore del settore e della diligenza professionale da lui esigibile, così che non averlo fatto integra almeno una grave negligenza dello stesso. Tale interpretazione appare coerente con pronunce della Corte di giustizia dell'Unione Europea, secondo cui, potendo la causa comportare una condanna al pagamento di un risarcimento dei danni, occorre che il giudice esamini se il prestatore di un servizio della società dell'informazione "sia stato al corrente di fatti o di circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità di cui trattasi", in ciò ricomprendendo le norme, "affinché non siano private del loro effetto utile (...) qualsiasi situazione nella quale il prestatore considerato viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze": ove l'esempio che il prestatore "scopre l'esistenza di un'attività o di un'informazione illecite a seguito di un esame effettuato di propria iniziativa, nonché la situazione in cui gli sia notificata l'esistenza di un'attività o di un'informazione siffatte", pur dovendosi considerare i casi in cui "notifiche relative ad attività o informazioni che si asseriscono illecite possono rivelarsi insufficientemente precise e dimostrate", come il giudice nazionale deve valutare (Corte di giustizia UE 12 luglio 2011, C-324/09, L'Orèal c. eBay, punti 120, 121, 122). Del pari, la Corte di giustizia ha escluso l'esenzione da responsabilità, prevista dall'art. 14 della direttiva 2000/31/CE, allorché il prestatore "dopo aver preso conoscenza, mediante un'informazione fornita dalla persona lesa o in altro modo, della natura illecita di tali dati o di attività di detto destinatari abbia omesso di prontamente rimuovere tali dati o disabilitare l'accesso agli stessi" (Corte di giustizia UE 23 marzo 2010, Google c. Louis Vuitton, punti 109, 120): statuendo quindi che la conoscenza, comunque acquisita e non solo proveniente dalle autorità competenti, della illiceità dei dati implica responsabilità. In caso contrario, in presenza di una situazione di "non manifesta" illiceità, nel senso ora indicato, in capo al prestatore del servizio resterà il solo obbligo di informarne le competenti autorità (la cd. notice)».

[114]Cfr. LEANZA, *La responsabilità dell'hosting provider per violazione del diritto d'autore*, in *Danno e responsabilità*, 5, 2019, 691.

user, segue quella omissiva del *provider* (allo stesso modo di come avviene in ambito penale). Dunque, per tutto il periodo antecedente alla conoscenza dell'illecito da parte del *provider*, l'illecito è monosoggettivo: esso è commesso dal solo utente per via del contenuto o materiale contrario alla legge da questo generato su Internet.

A seguito della conoscenza di tale illecito, da parte del prestatore del servizio, l'illecito in questione diventa plurisoggettivo e sarà caratterizzato da due condotte contrapposte: la prima nel tempo, commissiva, da parte dell'utente; la successiva, omissiva, tenuta dal prestatore del servizio della società dell'informazione .

Tale fattispecie plurisoggettiva sarà quindi regolata, dal punto di vista civilistico, dall'articolo 2055 c.c.,[115] con la conseguenza che l'utente che ha generato il contenuto illecito e il provider, che abbia omesso di rimuoverlo a seguito dell'avvenuta conoscenza, sono responsabili in solido.[116]

[115]Cfr. ALBERTINI, *La responsabilità civile degli ISP per i materiali caricati dagli utenti*, in *Il Caso.it*, 2020, 12.

[116]In materia di diritto d'autore, accenna a tale fattispecie di responsabilità l'Avvocato Generale Szpunar in *Ziggo v. The Pirate Bay*, para. 64-68: «64. Orbene, il caso previsto dall'articolo 8, paragrafo 3, della direttiva 2001/29 presuppone la sussistenza di un nesso tra l'oggetto del provvedimento inibitorio e la violazione dei diritti d'autore. Una misura di blocco di un sito Internet implica che sia stata accertata la responsabilità dell'operatore del suddetto sito per aver violato i diritti d'autore mediante i servizi dell'intermediario nei confronti del quale è diretto il provvedimento inibitorio. In tal caso detto operatore ha la qualità di terzo che viola i diritti d'autore ai sensi dell'articolo 8, paragrafo 3, della direttiva 2001/29. 65. Se l'operatore in questione non pone in essere l'atto oggetto del monopolio dell'autore (ad esempio la comunicazione al pubblico), tale violazione può unicamente essere indiretta. Tenuto conto del fatto che la responsabilità per tale tipo di violazioni non è armonizzata nell'ambito del diritto dell'Unione, essa deve essere espressamente prevista nel diritto nazionale. Spetta ai giudici nazionali verificare se una siffatta responsabilità sussista nel loro diritto interno. 66. Qualora sia possibile accertare una responsabilità siffatta in capo all'operatore di un sito di indicizzazione in una rete peer-to-peer in cui sono condivise opere protette senza l'autorizzazione dei titolari dei diritti d'autore, si deve ritenere che tale operatore utilizzi i servizi dei fornitori di accesso ad Internet, i cui clienti condividono i file in tale rete, in modo analogo al soggetto che, di per sé, viola direttamente i diritti d'autore. 67. Tale constatazione non è messa in discussione dal fatto che un sito come TPB possa rientrare nella categoria dei prestatori di servizi di hosting la cui responsabilità per le informazioni memorizzate è, in linea di principio, esclusa ai sensi dell'articolo 14, paragrafo 1, della direttiva 2000/31. Tale immunità è un effetto soggetto a condizione. Essa è concessa unicamente se il prestatore non era al corrente dell'illiceità delle informazioni memorizzate o dell'attività svolta con tali informazioni e a condizione che, non appena al corrente di tale illiceità, esso agisca immediatamente per rimuovere le informazioni in questione o per disabilitarne l'accesso. 68. Se il prestatore intermediario non soddisfa tali condizioni, ossia se era al corrente dell'illiceità delle informazioni memorizzate ma non ha agito al fine di rimuoverle o di disabilitarne l'accesso, esso può essere considerato indirettamente responsabile di tali informazioni».

Un primo punto controverso, nell'applicazione del già menzionato articolo, risiede nel tenore letterale e nelle interpretazioni fino ad oggi succedutesi dello stesso: l'articolo 2055 c.c. è stato sovente applicato a condotte contestuali: ciononostante, non è mancato chi, in dottrina,[117] ritiene di estenderne l'ambito applicativo anche al caso in cui la condotta imputabile di un soggetto, il *provider*, è successiva a quella dell'altro, l'utente.

Un secondo punto potenzialmente controverso in applicazione dell'articolo 2055 c.c. potrebbe risiedere nell'elemento soggettivo: ci si è chiesto, cioè, se sia richiesta la consapevolezza di compartecipare alla produzione di un danno ingiusto. Tuttavia, tale dubbio perde di rilevanza in tale situazione, in quanto, il prestatore del servizio, dal momento in cui sorge il suo dovere di attivarsi per la rimozione del contenuto illecito, ha sicuramente avuto conoscenza dell'illiceità.

Chiarito ciò, nel prossimo paragrafo ci si occuperà di capire quale tipologia di responsabilità imputare al *provider*, qualora ricorrano i presupposti su esaminati.

4.2.3. La responsabilità civile del provider: tutela aquiliana o contrattuale per i danneggiati?

Dopo aver chiarito come, dal punto di vista civilistico, il prestatore di servizi della società dell'informazione possa incorrere in un tipo di responsabilità omissiva, consistente nel non aver rimosso il (o limitato l'accesso al) contenuto illecito o qualora a seguito della mera conoscenza dell'illecito ovvero quando – senza aver ricevuto nessun tipo di segnalazione – avrebbe dovuto accorgersi della manifesta illiceità del contenuto per via della diligenza professionale tipicamente dovuta, resta infine da chiedersi se la responsabilità civile imputabile agli *Internet Service Providers* derivi da una responsabilità contrattuale *ex* articoli 1218 ss. c.c. oppure una responsabilità aquiliana *ex* articolo 2043 ss. c.c., con le relative differenze di disciplina che ne derivano.[118]

[117] Così ALBERTINI, *La responsabilità civile degli* ISP., cit., 14.

[118] «Le principali differenze, scolasticamente ripetute, riguardano: i) limitazione della responsabilità contrattuale ai danni prevedibili, tranne che ricorra dolo, art. 1225, non richiamato dagli artt. 2043 ss.; ii) il termine prescrizionale, decennale per la responsabilità civile e quinquennale per la responsabilità aquiliana, art. 2947 cc; iii) la messa in mora, non necessaria quando si tratta di fatto illecito, art. 1219 c. 2 cc. La differenza non riguarda invece il giudizio di colpa/negligenza, la quale è sempre costituito dalla violazione della normale diligenza». Così, ALBERTINI, *La responsabilità civile degli* ISP., cit., 29.

Relativamente a tale quesito, si dà per scontato che, così come la responsabilità dello *user*, anche quella del *provider* sia una responsabilità di tipo aquiliano *ex* articolo 2043 c.c., in combinato disposto con le norme che tutelano i diritti, di volta in volta, violati dagli *user generated contents*. La giurisprudenza da ultimo si è espressa in tal senso.[119]

Tuttavia, c'è chi non esclude che la responsabilità del *provider* sia di tipo contrattuale[120]: la differenza tra responsabilità aquiliana o contrattuale si basa sulla esistenza o meno di un previo rapporto tra le parti (in questo caso tra *provider* e soggetto leso), tale per cui la condotta oggetto di censura costituisca o meno inadempimento rispetto ad un obbligo sorto da quel rapporto.

Ecco allora che chi ritiene che la responsabilità del *provider* sia una responsabilità di tipo contrattuale, ritiene che un rapporto tra le parti – *provider* e titolare dei diritti lesi – esista: secondo costoro, l'obbligo di rimozione del contenuto illecito a carico del *provider*– che scatta, lo si ripete, quando il *provider* abbia avuto conoscenza dell'illiceità o quando l'illiceità sia manifesta–, mira ad evitare la lesione della sfera giuridica di un soggetto ben determinato (*i.e.*, il soggetto leso che normalmente è anche autore della diffida).

Il dovere di rimuovere il materiale dannoso dalla rete, quindi, non è più a favore della collettività, come sarebbe se sul *provider* gravasse un generale dovere di sorveglianza (cosa esclusa dall'articolo 15 della Direttiva e 17 del d.lgs. n. 70 del 2003, nonché dal DSA, come già affermato), ma è un dovere che tutela in modo specifico la situazione giuridica soggettiva di un soggetto determinato.

Tale dovere crea dunque un rapporto ben individuato tra *Internet Service Provider* e soggetto leso: la conseguenza che ne segue è quella per cui omettere di rimuovere il contenuto dannoso a favore del soggetto leso, rende quest'ultimo creditore della prestazione di rimozione nei confronti del debitore di tale prestazione, il *provider*.

In senso contrario, i sostenitori dell'applicazione degli articoli 2043 ss. c.c., affermano come le disposizioni normative comunitarie e nazionali, rispettivamente della Direttiva e del d.lgs. n. 70 del 2003, limitandosi ad individuare una

[119]Trib. Roma, 10 gennaio 2019, n. 693, in *Danno e responsabilità*, 5, 2019, 671 s.
[120]ALBERTINI, *La responsabilità civile degli* ISP., cit., 16 s.

responsabilità in senso negativo e non positivo, non assegnano al *provider* un obbligo di agire, bensì un onere: in altre parole, ritengono che se il *provider*, dopo averne preso conoscenza, non procede alla rimozione del materiale illecito, egli tuttavia non avrebbe un obbligo in senso tecnico di agire in tal senso.[121]

Tuttavia, e a loro volta, i sostenitori dell'imputazione di una responsabilità contrattuale, chiariscono come il dovere di solidarietà, tipico di ogni rapporto sociale, genera nel *provider* un obbligo di diligenza professionale tale per cui, esso, nello svolgimento della proprietà attività di fornitura di servizi di Internet, deve sforzarsi per evitare che ai terzi con cui viene a contatto venga causato un danno.

Tutto risiede in come si costruisce il dovere di rimozione del contenuto illecito da parte del *provider*: se come dovere giuridico *erga omnes* o come dovere specifico nei confronti del solo soggetto leso. In questa seconda ipotesi, si dovrebbe optare per imputare all'*ISP* una responsabilità di tipo contrattuale a discapito di quella aquiliana con tutte le differenze di disciplina che ne derivano.

4.3. La responsabilità dell'Internet Service Provider: profili comparatistici.

Concluso così il tema della responsabilità «domestica» delle piattaforme digitali, d'ora innanzi la dissertazione offrirà degli spunti comparatistici con ordinamenti anglosassoni e sotto il profilo civile, e sotto il profilo penale.

4.3.1 Profili civilistici.

Essendo Internet il fenomeno globale per antonomasia, risulta evidente come l'Europa non sia stata la sola, ma soprattutto la prima, a dotarsi di una regolamentazione sulla responsabilità degli *Internet Service Providers*. Infatti, protagonista in tal senso, prima ancora del legislatore comunitario con l'emanazione della Direttiva *E-commerce* del 2000, è stato il legislatore statunitense, nel 1996, prima, con l'emanazione del *Communication Decency Act* («CDA»), [122] e nel 1998, poi, con l'emanazione del *Digital Millenium Copyright Act* («DMCA»).[123] Si procederà introducendo brevemente il primo, per poi soffermarsi in maniera più approfondita sul secondo.

[121]Cfr. ALBERTINI, *La responsabilità civile degli* ISP., cit., 17 s.
[122]Communication Decency Act, 47 U.S.C., § 230, 1996.
[123]Digital Millennium Copyright Act, 17 U.S.C. (n. 47).

Il CDA si concentra sui contenuti illegali online ad un livello generale: la sezione 230 stabilisce come un *service provider* sia assolutamente immune, in maniera incondizionata (salve limitatissime eccezioni),[124] da qualsiasi tipo di responsabilità per i contenuti generati dagli utenti; allo stesso tempo, la medesima sezione protegge gli ISP anche nel caso in cui questi decidano di rimuovere contenuti tutt'altro che illeciti. Ciò allo scopo di (I) supportare lo sviluppo dell'Internet inteso come ecosistema e la libertà di espressione protetta dal primo Emendamento[125], limitando rischi e responsabilità per tutti quei *providers* che si pongono come intermediari, e (II) lasciare libertà assoluta ai *providers* stessi circa l'applicazione di meccanismi che possano fronteggiare contenuti potenzialmente illeciti. Tale sezione, data la specifica e separate previsione per il *copyright*, sembra applicarsi alle altre due *species* della proprietà intellettuale: i marchi (c.d. *trademarks*) e i brevetti (c.d. *patents*).

Ciò risulta vero per qualsiasi contenuto illecito generato dagli *user* su Internet, eccetto il caso in cui tale contenuto o materiale violi il *copyright*: infatti per ciò che riguarda materiale protetto da copyright, il DCMA, sezione 512,[126] contiene una disciplina diversa rispetto a quella contenuta dal CDA, sezione 230, pur prevedendo sempre un *safe harbour* a favore degli ISP.

In particolare, in materia di *copyright*, al fine di godere dell'esenzione da responsabilità, un *online service provider* («OSP») (I) non deve avere «effettiva conoscenza» che il materiale sul sistema sia *infringing*, i.e. in violazione delle norme sul *copyright*, oppure (II) non deve avere consapevolezza «di fatti o circostanze da cui risulti un'attività di violazione».[127]

---

[124]Ci si riferisce al caso in cui la piattaforma concorre alla creazione o diffusione del contenuto illecito. In Huon v.Denton, 841 F.3d 733 (7th Cir. 2016), la corte ha ritenuto che Gawker stesso fosse un «fornitore di contenuti informativi, nella misura in cui Gawker: (1) incoraggiava e invitava gli utenti a diffamare Huon, selezionando ed esortando i commentatori più inclini alla diffamazione a «postare più commenti e continuare a intensificare il dialogo»; (2) modificava, modellava e coreografava il contenuto dei commenti che riceveva; (3) selezionava per la pubblicazione ogni commento che appariva sotto l'articolo di Jezebel; e (4) assumeva individui che erano autori di almeno alcuni dei commenti stessi». Nello stesso senso Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

[125]Negli Stati Uniti la libertà di parola è fortemente tutelata dal Primo Emendamento. Ciò comporta una pressione sulle piattaforme affinché lascino i contenuti pubblicati piuttosto che rimuoverli, soprattutto nel contesto del discorso/dibattito politico.

[126]17 U.S.C. (n. 47) § 512.

[127]17 U.S.C. (n. 47) § 512 (c).

Essendo le due condizioni appena viste poste in modo alternativo, l'assenza di una delle due rende inapplicabile l'applicazione dell'esenzione. Nel momento in cui il *provider* ottiene tale conoscenza o consapevolezza, esso deve «agire tempestivamente per rimuovere o disabilitare l'accesso al materiale».[128]
Inoltre, il *service provider* non deve «ricevere un beneficio finanziario direttamente attribuibile all'attività di violazione, nel caso in cui il fornitore di servizi abbia il diritto e la capacità di controllare tale attività». Sebbene a prima vista le disposizioni DMCA sembrino simili alla *E-commerce Directive*, vi sono in realtà alcune differenze fondamentali.

In primo luogo, a differenza della Direttiva, il *safe harbour* del DMCA non contiene nessun riferimento iniziale di hosting «attivo/passivo», ma è interamente incentrato sulla conoscenza del *provider*. Gli aspetti aggiuntivi del «beneficio finanziario» e del «diritto e capacità di controllo» non sono equivalenti all'analisi «dell'attività» o meno di un *provider* nell'ambito Direttiva europea.

La giurisprudenza statunitense suggerisce che l'imputazione di responsabilità è più ristretta rispetto alla normativa europea e interpretazione della Corte di Giustizia.

Il «diritto e la capacità di controllo» richiedono «qualcosa di più della capacità di rimuovere o bloccare l'accesso al materiale pubblicato sul sito web di un fornitore di servizi» ed è rilevante solo in relazione all'attività di violazione del *copyright*, piuttosto che in generale.[129]

---

[128]17 U.S.C. (n. 47) § 512 (c)(1)(B).

[129]Viacom Int'l, Inc. v YouTube Inc. 676 F.3d 19, 34–38 (2d Cir 2012), para. 71: «In any event, the foregoing tension elsewhere described as a 'predicament'[11] and a 'catch22' [12]—is sufficient to establish that the control provision 'dictates' [676 F.3d 38] a departure from the common law vicarious liability standard[...]. Accordingly, we conclude that the 'right and ability to control' infringing activity under § 512(c)(1)(B) 'requires something more than the ability to remove or block access to materials posted on a service provider's website.' [...] The remaining—and more difficult—question is how to define the 'something more' that is required».
La stessa corte si domanda come definire quel «qualcosa di più»: «To date, only one court has found that a service provider had the right and ability to control infringing activity under § 512(c)(1)(B).[13] In Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146 (C.D.Cal.2002), the court found control where the service provider instituted a monitoring program by which user websites received 'detailed instructions regard[ing] issues of layout, appearance, and content.' [...] The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions. [...] Similarly, inducement of copyright infringement under Metro–Goldwyn–Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005), which 'premises liability on purposeful, culpable expression and conduct,' [...] might also rise to the level of control under § 512(c)(1)(B). Both of these examples involve a service provider exerting substantial influence on the activities of users, without necessarily—or even

Il «beneficio finanziario» deve essere «direttamente attribuibile all'attività di violazione», il che significa che «costituisce un'attrazione per gli abbonati, non solo un beneficio aggiunto».[130]

In altre parole, l'esclusione dall'ammissibilità del *safe harbour* si concentra su servizi come *The Pirate Bay* e non, ad esempio, sulle piattaforme che si occupano dei contenuti degli utenti. Ad esempio, nella causa *Viacom Int'l, Inc. v. YouTube, Inc*. il giudice ha ritenuto che gli sforzi di YouTube per far rispettare le proprie regole sui contenuti non raggiungessero il livello di partecipazione all'attività di violazione tale da escludere l'esenzione.[131]

A livello comunitario, al contrario, il coinvolgimento e le azioni della piattaforma in relazione ai contenuti degli utenti sono rilevanti più ad un livello generale, anziché più concentrate su attività dedicate e che incoraggiano la violazione. Infatti, i casi succitati hanno dimostrato come ciò che in Europa avrebbe reso i *providers* «attivi» – e dunque passibili di responsabilità in quanto le esenzioni non si sarebbero applicati – negli Stati Uniti non rileva: ciò che conta oltreoceano è la sola conoscenza effettiva dell'illiceità dei contenuti.

In secondo luogo, il DMCA stabilisce anche un formato prescritto per le comunicazioni (c.d. "*notice and take-down procedure*"), grazie al quale al titolare dei diritti di *copyright* è garantito un controllo reale sui diritti sottostanti in questione, a differenza della Direttiva europea. Se un *provider* riceve una notifica avente ad oggetto la violazione del *copyright*, il *provider*, se tale notifica risulta fondata, deve «rapidamente» rimuovere o disabilitare l'accesso a tale materiale.[132]

In Europa non esiste – o meglio non esisteva – un meccanismo di segnalazione prestabilito; spettava agli Stati membri decidere se richiedere determinate formalità. Tuttavia, tale problematica sarà superata dal Regolamento DSA, che prevede – come visto – agli articoli 16-17, 20-21 un dettagliato meccanismo di segnalazione che verrà implementato dagli stessi gestori delle

---

frequently—acquiring knowledge of specific infringing activity». Così, Viacom Int'l, Inc. v YouTube Inc. 676 F.3d 19, 34–38 (2d Cir 2012), para. 72.

[130]Cfr. Perfect 10, Inc. v CCBill LLC 488 F.3d 1072, 1117–18 (9th Cir 2004).

[131]Viacom Int'l, Inc. v YouTube, Inc. 940 F. Supp. 2d 110, 121 (SDNY 2013): «YouTube's decisions to restrict its monitoring efforts to certain groups of infringing clips, like its decisions "to restrict access to its proprietary search mechanisms," do not exclude it from the safe harbor, regardless of their motivation».

[132] 17 U.S.C. (n. 47) § 512 (c)(1)(C).

piattaforme digitali (ed in particolare dai «servizi intermediario» a cui si applicano solo gli articoli 16 e 17, e dalle «piattaforme online» cui si applicano anche gli articoli 20 e 21).

Dunque, risulta chiaro da queste premesse come la disciplina regolante l'attività dell'ISP, nel CDA e DMCA statunitensi, offrano una protezione maggiore ai prestatori di servizi della società dell'informazione rispetto a quanto abbia fatto la Direttiva E-commerce e quanto faccia il nuovo Regolamento (UE) 2022/2065:[133] l'assenza di una qualsiasi rilevanza in ordine all'attività o passività del *provider*, fa sì che tutta l'analisi si concentri sulla effettiva conoscenza o consapevolezza dell'illegalità del materiale generato dagli utenti.

Proprio su tale «conoscenza» vale la pena soffermarsi: in Europa deve esserci una qualche indicazione di illegalità del contenuto per generare una conoscenza effettiva e privare la piattaforma del *safe harbour*, ma la conoscenza può essere imputata alla piattaforma se un giudice ritiene che un «operatore economico diligente» avrebbe identificato l'illegalità in questione.[134]

Negli Stati Uniti, i querelanti devono dimostrare che il prestatore era specificamente a conoscenza della violazione, uno standard, dunque, più elevato. Nel caso di LiveJournal[135], la domanda chiave (c.d. "*issue*") era se fosse «ovvio per una persona ragionevole» che il contenuto del caso di specie costituisse una violazione del *copyright*. In confronto, un «operatore economico diligente» avrebbe sicuramente maggiori probabilità di identificare l'illegalità o la violazione rispetto a una «persona ragionevole comune» (che non sia un esperto di *copyright*). Anche qui, dunque, lo standard statunitense sembra dunque favorire i servizi intermediario.

Un'ulteriore rilevante differenza è che, per quanto riguarda il diritto d'autore, gli Stati Uniti dispongono di una difesa più ampia contro le violazioni del diritto d'autore (ad esempio, il c.d. "*fair use*")[136] rispetto al *fair dealing* e ad altre

[133]Cfr. ALLGROVE, GROOM, *Enforcement in a digital context: intermediary liability*. "Research Handbook on Intellectual Property and Digital Technologies", edited by Tanya Aplin, Edward Elgar Publishing Ltd., 2019, 516 s.
[134]CGUE, 12 luglio 2011, *L'Oréal, già citata*, para. 120.
[135]Mavrix Photographs, LLC v LiveJournal, Inc. 853 F.3d 1020, 1033 (9th Cir 2017).
[136]17 U.S.C. § 107: «Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the

difese ristrette e specifiche che esistono nel Regno Unito e nell'Unione europea. Ciò potrebbe significare che negli Stati Uniti è più probabile che alcune opere generate dall'utente che coinvolgono determinati diritti protetti si qualifichino come *fair use*, e dunque non costituenti *infringement*, con la naturale conseguenza che non esisterà una *secondary liability*[137] per il *provider*.[138]

4.3.2. Profili penalistici.

Così come avviene in ambito civilistico, anche in ambito penalistico il *target* delle sanzioni per violazioni dei diritti di proprietà intellettuale avvenute online – come già visto in ambito domestico – risulta essere, oltre ovviamente l'utente che genera il contenuto illecito, anche *l'Internet Service Provider*.

Da qui in poi si analizzerà dunque la responsabilità penale dell'ISP nei principali paesi di *common law*, con riferimento soprattutto al *copyright*.

I reati in materia di proprietà intellettuale sono stati elaborati tra la fine del diciannovesimo e la prima metà del ventesimo secolo per fronteggiare le condotte di pirateria e contraffazione.[139]

Tali fattispecie criminose riguardavano, e riguardano, soprattutto gli operatori commerciali che importano e vendono prodotti in violazione delle norme sul *copyright* e le persone che distribuiscono materiale in modo illecito in misura tale da arrecare pregiudizio al titolare del *copyright*.

La previsione di norme incriminatrici che punivano condotte di diffusione su larga scala di contenuti protetti da *copyright* era meno necessaria, soprattutto

---

factors to be considered shall include— (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors».

[137]Con il termine «s*econdary liability*» s'intende la responsabilità di chi non è autore diretto della violazione ma che abbia in qualche modo assistito, incoraggiato, controllato, beneficiato o partecipato in altro modo alla condotta di violazione diretta commessa da un altro soggetto. Così, FROMER, SPRIGMAN, *Copyright Law*, cit., 507.

[138]ALLGROVE, GROOM, *Enforcement in a digital context: intermediary liability*. "Research Handbook on Intellectual Property and Digital Technologies", edited by Tanya Aplin, Edward Elgar Publishing Ltd., 2019, 518.

[139]WEATHERALL, *Criminal Sanctions as a Tool Against Online Infringement: National Law, International Treaties, Transnational Cooperation (August 17, 2018)*, in "Research Handbook on Intellectual Property and Digital Technologies", edited by Tanya Aplin, Edward Elgar Publishing Ltd., 2019, Forthcoming, Sydney Law School Research Paper No. 18/49.

perché la tecnologia di trasmissione non era poi così tanto sviluppata. Ma la rivoluzione digitale apportata da Internet ha aumentato le violazioni, ormai commesse su scala globale.

Per tali motivi, la risposta dei legislatori nelle varie giurisdizioni è stata diversa: gli Stati Uniti si sono mossi relativamente presto, nel 1997, estendendo la responsabilità penale per violazione del *copyright* anche alle attività non commerciali – e più in particolare, sia alle violazioni che superano un certo valore al dettaglio, sia in caso di guadagno finanziario privato, compreso il caso in cui l'autore della violazione si aspetti di ricevere in cambio qualcosa di valore, che può includere altre opere protette da *copyright*.[140] Tale ultima estensione è stata pensata per essere applicata, ad esempio, ai trasgressori online che si scambiano *file* come software decriptati.[141]

Anche l'Australia ha semplicemente esteso i suoi reati esistenti al nuovo *cyber-environment*: ha modificato la sua definizione di *infringing* «*articles*» («articoli», che violano il *copyright*) al fine di includere gli *electronic files* (file elettronici)[142], coprendo così in modo inequivocabile l'attività online, compresa quella non commerciale ma di portata sufficiente a pregiudicare i diritti del titolare del *copyright*.[143]

Tale emendamento ha anche assicurato pene massime uguali sia per violazioni offline che online. Successivamente, nel 2006 l'Australia è andata oltre: il legislatore australiano ha infatti applicato la sua politica generale in materia di

---

[140]17 U.S.C. 506 (a)(1)(B) and (C), introdotto dal *No Electronic Theft Act* 1997 (US). 17 U.S.C. 506 (a)(1)(C) rende reato la distribuzione, durante un periodo di 180 giorni, di una o più copie di una o più opere protette dal diritto d'autore per un valore totale al dettaglio superiore a 1.000 dollari. L'emendamento è stato motivato dal caso US v LaMacchia 871 F Supp 535 (D Mass 1994). Brevemente, David LaMacchia, studente del Massachussets Institute of Technology (MIT), aveva realizzato una app di file-sharing che consentiva agli studenti dello stesso ateneo di effettuare il download gratuito di software didattici e libri di testo. Tuttavia, le fattispecie di *criminal copyright infringment* vigenti fino ad allora non erano applicabili all'imputato in quanto mancava la commercialità attività realizzate e l'assenza d'ogni profitto per l'autore del dispositivo telematico.

[141]Si veda ad esempio, Griffiths v US [2005] FCAFC 34, (2005) 143 FCR 182. Nel caso Griffiths, l'accesso a un sito web protetto era stato garantito da una persona che forniva file protetti da copyright. Secondo la legge statunitense, ed in particolare il 17 U.S.C. 506 (a)(1)(A), si trattava di una violazione «a scopo di lucro privato» in quanto, pur non essendo previsto alcun pagamento in denaro, gli individui hanno «barattato» file e competenze per consentire a tutti loro di accedere a un numero significativo di opere protette da copyright.

[142]Copyright Act 1968 (Cth), sec. 132AA: «article includes a reproduction or copy of a work or other subject-matter, being a reproduction or copy in electronic form». Tale definizione è stata introdotta dal Copyright Amendment (Digital Agenda) Act 2000 (Cth).

[143]WEATHERALL, *Criminal Sanctions*, cit., 534.

diritto penale, che prevede reati a più livelli – in cui le pene più elevate si applicano solo alla condotta intenzionali –, anche al *copyright*. La conseguenza è che dunque in Australia è possibile commettere un reato in materia di *copyright* anche con colpa (sono addirittura previsti anche casi di responsabilità oggettiva come si vedrà in seguito).[144] Questo approccio - importato dal diritto penale generale al *copyright* - si discosta radicalmente dai reati in materia di *copyright* in giurisdizioni analoghe, che tendono a criminalizzare solo le violazioni dolose o intenzionali – c.d. "*intentional infringement*"– (o, negli Stati Uniti, c.d. "*wilful misconduct*").[145] L'Australia ha inoltre introdotto un reato di ampia portata che vieta quella condotta risultante in violazioni su scala commerciale che hanno un sostanziale impatto pregiudizievole sul titolare del *copyright*, laddove il trasgressore intenda, o sia negligente rispetto a tali risultati.[146] Il reato si sovrappone stranamente a quello di distribuzione[147], ma sembra anche adatto a catturare persone che intenzionalmente o negligentemente forniscono la tecnologia che consente una violazione diffusa.

Il Regno Unito è stato più cauto. Nel 2003, il Regno Unito ha criminalizzato le comunicazioni al pubblico che violano il *copyright*, comprese le comunicazioni commerciali di portata sufficiente a pregiudicare il titolare del *copyright*.[148]

---

[144]Si veda ad esempio il Copyright Act 1968 (Cth), sec. 132 AC (3)(d), rubricato «summary offence»: «(3) A person commits an offence if: (a) the person engages in conduct; and (b) the conduct results in one or more infringements of the copyright in a work or other subject-matter; and (c) the infringement or infringements have a substantial prejudicial impact on the owner of the copyright and the person is negligent as to that fact; and (d) the infringement or infringements occur on a commercial scale and the person is negligent as to that fact».

[145]Un *intentional infringement* è quella che un dipendente commette di proposito, non per negligenza. Non è necessario che il dipendente sappia che l'azione è illegale, è sufficiente che si provi che il dipendente voleva tenere quella condotta. Una *wilful infringement* è diversa; si tratta di un'azione che un dipendente commette di proposito con la consapevolezza che l'atto è proibito. Se non ci sono prove che il dipendente sapesse che l'azione era vietata, la cattiva condotta non è *wilful*, ma può essere *intentional*.

[146]Copyright Act 1968 (Cth) sec. 132AC (1). Il dolo rende il reato perseguibile d'ufficio; la negligenza lo rende un reato sommario con una pena inferiore. La definizione degli stati mentali applicabili ai reati australiani in materia di copyright non si trovano nel Copyright Act, ma sono indicati nel Criminal Code Act 1995 (Cth) Division 5.

[147]Presumibilmente, se grave, la distribuzione di file elettronici che arreca pregiudizio al titolare del copyright (disciplinata dalla sec. 132AD) potrebbe anche essere considerata come una condotta che comporta violazioni su scala commerciale che causano un pregiudizio sostanziale (disciplinata dalla sec. 132AC), con la conseguenza che il reato minore resterebbe assorbito da quello più grave.

[148]Si veda Copyright, Designs and Patents Act 1988 (UK) sec. 107(2A): «A person ("P") who infringes copyright in a work by communicating the work to the public commits an offence if P: (a) knows or has reason to believe that P is infringing copyright in the work, and (b) either— (i) intends to make a gain for P or another person, or (ii) knows or has reason to believe that communicating the work to the public will cause loss to the owner of the copyright, or will expose the owner of the copyright to a risk of loss».

Inizialmente questo reato prevedeva una pena massima inferiore rispetto ad altri reati in materia di *copyright* (2 anni rispetto ai 10 anni previsti per gli altri reati). Nel 2017, dunque, il governo si è mosso per eliminare l'ingiustificabile differenza tra le pene, sulla base del fatto che la violazione online è altrettanto dannosa che quella offline. In questo modo, tuttavia, il governo ha risposto alle preoccupazioni circa l'eccessiva ampiezza della fattispecie e ha riformulato il reato in modo da richiedere l'elemento soggettivo del dolo: è necessario che il trasgressore abbia l'intenzione di guadagnare denaro o sappia che la comunicazione può causare una perdita monetaria al titolare del *copyright*.[149]

In Australia esistono vari livelli di reati (doloso, colposo o responsabilità oggettiva, c.d., rispettivamente, *indictable offence*, *summary offence*, *strict liability*) per il possesso di un articolo pirata (compresi i file elettronici) con l'intenzione di distribuirlo in misura tale da arrecare pregiudizio al titolare del *copyright*, o per il possesso di tale articolo contraffatto nel corso dell'attività di distribuzione.[150]

---

[149]Copyright, Designs and Patents Act 1988 (UK) sec. 107(2A)–(2B), sec. 107(4A)(b).

[150]Copyright Act 1968 (Cth) sec. 132AJ, rubricato «Possessing infringing copy for commerce» e diviso in *indictable offense, summary offense or strict liability*: «A. Indictable offence: "(1) A person commits an offence if: (a) the person possesses an article, with the intention of doing any of the following with the article: (i) selling it; (ii) letting it for hire; (iii) by way of trade offering or exposing it for sale or hire; (iv) offering or exposing it for sale or hire to obtain a commercial advantage or profit; (v) distributing it for trade; (vi) distributing it to obtain a commercial advantage or profit; (vii) distributing it to an extent that will affect prejudicially the owner of the copyright in the work or other subject-matter of which the article is an infringing copy; (viii) by way of trade exhibiting it in public; (ix) exhibiting it in public to obtain a commercial advantage or profit; and (b) the article is an infringing copy of a work or other subject-matter; and (c) copyright subsists in the work or other subject-matter at the time of the possession. (2) An offence against subsection (1) is punishable on conviction by a fine of not more than 550 penalty units or imprisonment for not more than 5 years, or both." 2. Summary offence: (3) A person commits an offence if: (a) the person possesses an article, with the intention of doing any of the following with the article: (i) selling it; (ii) letting it for hire; (iii) by way of trade offering or exposing it for sale or hire; (iv) offering or exposing it for sale or hire to obtain a commercial advantage or profit; (v) distributing it for trade; (vi) distributing it to obtain a commercial advantage or profit; (vii) distributing it to an extent that will affect prejudicially the owner of the copyright in the work or other subject-matter of which the article is an infringing copy; (viii) by way of trade exhibiting it in public; (ix) exhibiting it in public to obtain a commercial advantage or profit; and (b) the article is an infringing copy of a work or other subject-matter and the person is negligent as to that fact; and (c) copyright subsists in the work or other subject-matter at the time of the possession and the person is negligent as to that fact.
Penalty: 120 penalty units or imprisonment for 2 years, or both. (4) An offence against subsection (3) is a summary offence, despite section 4G of the Crimes Act 1914." 3. Strict liability: "(5) A person commits an offence if: (a) the person possesses an article in preparation for, or in the course of, doing any of the following with the article: (i) selling it; (ii) letting it for hire; (iii) by way of trade offering or exposing it for sale or hire; (iv) offering or exposing it for sale or hire to obtain a commercial advantage or profit; (v) distributing it for trade; (vi) distributing it to obtain a commercial advantage or profit; (vii) distributing it to an extent that will affect prejudicially the owner of the copyright in the work or other subject-matter of which the article is an infringing copy; (viii) by way of trade exhibiting it in public; (ix) exhibiting it in public to obtain a commercial

La Nuova Zelanda e il Regno Unito, invece, considerano reato solo il possesso di un articolo pirata nel corso di un'attività commerciale al fine di commettere un atto illecito.[151] Nel Regno Unito, l'autore del reato è responsabile se sa o ha motivo di credere che l'articolo è una copia pirata; in Nuova Zelanda è richiesta la conoscenza.

In Australia, inoltre, è un reato possedere anche un dispositivo capace di realizzare una copia pirata di materiale protetto, sia a titolo di dolo che di colpa.[152]

In Nuova Zelanda e nel Regno Unito il legislatore è stato più accorto: una persona commette reato se possiede un dispositivo specificamente progettato o adattato per la creazione di copie di una particolare opera protetta da *copyright* sapendo che l'oggetto verrà utilizzato per creare copie illegali per la vendita o il noleggio o per l'uso di tali copie nel corso di un'attività commerciale.[153]

Dunque, nel Regno Unito e in Nuova Zelanda solo pochi dispositivi generici utilizzati per accedere a materiale online potrebbero porre problemi ai sensi di questa norma, a differenza di quanto potrebbe avvenire in Australia, data l'ampiezza della fattispecie che comprende, come visto, anche condotte colpose.[154]

---

advantage or profit; and (b) the article is an infringing copy of a work or other subject-matter; and (c) copyright subsists in the work or other subject-matter at the time of the possession.
Penalty: 60 penalty units. (6) Subsection (5) is an offence of strict liability».

[151]Copyright, Designs and Patents Act 1988 (UK) sec. 107(1)(c): «(1) A person commits an offence who, without the licence of the copyright owner: (c)possesses in the course of a business with a view to committing any act infringing the copyright […]»; Copyright Act 1994 (NZ) sec. 131(1)(c): « 1. Every person commits an offence against this section who, other than pursuant to a copyright licence, […] (c) possesses in the course of a business with a view to committing any act infringing the copyright».

[152]Copyright Act 1968 (Cth) sec. 132AL (2): «(2) A person commits an offence if: (a) the person possesses a device, intending it to be used for making an infringing copy of a work or other subject-matter; and (b) copyright subsists in the work or other subject-matter at the time of the possession». Per essere responsabile, la persona può anche essere incurante dell'esistenza del *copyright* sull'articolo al momento del possesso: Criminal Code 1995 (Cth) s 5.6(2).

[153]Copyright Act 1994 (NZ) sec. 131(2): « Every person commits an offence against this section who (a) makes an object specifically designed or adapted for making copies of a particular copyright work; or (b) has such an object in that person's possession, knowing that the object is to be used to make infringing copies for sale or hire or for use in the course of a business»; Copyright, Designs and Patents Act 1988 (UK) sec. 107(2): «(2) A person commits an offence who: (a)makes an article specifically designed or adapted for making copies of a particular copyright work, or (b)has such an article in his possession, knowing or having reason to believe that it is to be used to make infringing copies for sale or hire or for use in the course of a business». Il legislatore britannico, come al solito, estende la responsabilità, al di là delle persone che «sanno», anche alle persone che «hanno ragione di credere».

[154]Interpretando la fattispecie nella sua forma più ampia, banalmente, anche il possesso di uno s*martphone* potrebbe risultare reato.

All'ampliamento della portata della responsabilità penale per violazione del *copyright* nei sistemi nazionali, è corrisposto una crescita del numero di obblighi creati da importanti trattati internazionali.[155]

Per ciò che attiene all'*enforcement* contro gli ISP, bisogna sottolineare come ad oggi le azioni promosse dai soggetti lesi abbiano avuto carattere preminentemente civilistico piuttosto che penalistico: ciononostante, nella maggior parte dei paesi di *common law* in disamina, una responsabilità penale secondaria o accessoria può sorgere per questi reati in base al diritto penale generale (statutario o di common law), indipendentemente dalla fonte legislativa del reato principale.[156]

Le principali tipologie di responsabilità penale secondaria o accessoria degli *Internet Service Providers* che potrebbero essere rilevanti nel contesto dell'*online infringement* includono la *complicity*, l'*incitement* e la *conspiracy*.

La distinzione tra responsabilità per «*aiding and abetting*» (*i.e.*, aiutare o favorire) nella commissione di un crimine e responsabilità primaria, per stabilire la responsabilità penale dei prestatori di servizi di *file-sharing*, è stata illustrata dai procedimenti penali in Svezia nel 2009 contro The Pirate Bay e in Finlandia nel 2010 contro Finreactor.[157]

Nel caso *The Pirate Bay*, le persone coinvolte nella gestione del sito web sono state ritenute responsabili di «*aiding and abetting*» per le violazioni del *copyright* commesse dagli utenti.[158]

Nel caso di Finreactor, la violazione del *copyright* è stata, come previsto dalla legge finlandese, direttamente imputabile alle persone che gestivano il servizio, in quanto è stato accertato che questi avevano collaborato con gli utenti in modo attivo.[159] Ciò è stato in parte dovuto alla decisione del tribunale di considerare l'apparato di *file-sharing* nel suo complesso e alla constatazione che gli operatori erano a conoscenza delle violazioni, nonostante non avessero effettivamente e direttamente intrapreso le azioni in violazione del copyright.

---

[155]Per un approfondimento si veda WEATHERALL, *Criminal Sanctions*, cit., 536.
[156] Si vedano Criminal Code Act (Australia); Serious Crime Act 2007 (UK); Crimes Act 1961 (NZ) sec 66.
[157]WEATHERALL, *Criminal Sanctions*, cit., 540 s.
[158]WEATHERALL, *Criminal Sanctions*, cit., 540 s.
[159]WEATHERALL, *Criminal Sanctions*, cit., 540 s.

Tuttavia, entrambi i casi sono stati criticati per aver eccessivamente esteso i principi giuridici preesistenti.[160]

Precedentemente si è accennato al fatto che le principali tipologie di responsabilità penale c.d. "secondaria" o "accessoria", che avrebbero potuto assumere rilevanza nel contesto dell'*online infringement* da parte dei *providers*, riguardano la *complicity*, l'*incitement* e la *conspiracy*.

4.3.2.1. Complicity.

In Australia,[161] Regno Unito[162] e Nuova Zelanda,[163] una persona commette reato se tiene condotte assistenziali la commissione di un crimine. Nonostante ci siano, all'interno di questi tre paesi, delle differenze giurisdizionali, la *ratio* principale per una responsabilità per *complicity* è da rinvenirsi nel fatto che la persona è in qualche modo «*linked in purpose*» con la persona che commette effettivamente il crimine,[164] e la sua condotta assistenziale renda più probabile la commissione del reato.[165]

Il comportamento che integra la fattispecie di *complicity* può manifestarsi attraverso delle condotte di *aid*, *abet*, *counsel* or *procure* la commissione del crimine. Ognuna di queste condotte ha un significato diverso: (I) «*aid*» consiste nell'assistere il reo principale;[166] (II) «*abet*» significa incoraggiare l'autore del reato principale al momento del reato[167]; e infine la condotta che (III) «*counsels*» e (IV) «*procures*» non deve necessariamente essere associata a un reato. Ad esempio, si dice che una persona ha «*counselled*» se ha esortato la commissione del reato, e «*procured*» il reato se ha usato mezzi come, ad esempio, il pagamento di una somma di denaro, per realizzarlo.

Si consideri, ad esempio, una persona che fornisce *software peer-to-peer*.[168] Tale software facilita la violazione del *copyright online* e renderlo disponibile al pubblico potrebbe essere considerato un «*aid*» alla violazione. Se qualcuno che

[160]WEATHERALL, *Criminal Sanctions*, cit., 540 s.
[161]Criminal Code Act 1995 (Cth) sec. 11.2(1).
[162]Crimes Act 1961 (NZ) sec. 66(1)(b)–(d).
[163]Serious Crime Act 2007 (UK) sec. 44–46.
[164]WEATHERALL, *Criminal Sanctions*, cit., 541.
[165]WEATHERALL, *Criminal Sanctions*, cit., 541
[166]WEATHERALL, *Criminal Sanctions*, cit., 541
[167]WEATHERALL, *Criminal Sanctions*, cit., 541
[168]WEATHERALL, *Criminal Sanctions*, cit., 541

utilizza il software tenesse una condotta che si traduce in una violazione del *copyright* su scala commerciale che causa un danno sostanziale al suo titolare, ciò potrebbe rendere il distributore del *software* P2P responsabile per *complicity* in casi eccezionali. Se la rete creata dal software facilita il *download* di materiale protetto dal *copyright*, caricato da un particolare utente che viola la sezione 132AC dell'Australia Copyright Act 1968 (Cth),[169] è chiaro infatti che il fornitore di software P2P ha fornito parte dei mezzi per effettuare la distribuzione su scala commerciale. [170]

L'elemento soggettivo sarebbe probabilmente fondamentale per distinguere i *providers* innocenti da quelli colpevoli. La responsabilità, infatti, sorge solo se si può dimostrare che il *provider* ha agito con dolo.[171] È probabile che sia richiesto un dolo specifico («*intended*»), piuttosto che una generica consapevolezza del rischio. Nella maggior parte dei casi il software può essere utilizzato anche per scopi legittimi e il distributore può avere l'intenzione di farne solo un uso legittimo, e potrebbe dimostrarlo tramite *disclaimers* (*i.e.*, esonero da responsabilità).[172] Il dolo specifico potrebbe essere dimostrato, ad esempio, da e-mail interne incaute.[173]

4.3.2.2. Incitement.

L'«*incitement*» (istigazione) riguarda la situazione in cui un soggetto sollecita la commissione di un reato.[174] Varie corti hanno interpretato il concetto

[169] V. nota 139.

[170]Un esempio in cui una persona ha fornito assistenza alla violazione del copyright di un'altra persona, si riscontra in Griffiths v US già citato. Griffiths fu considerate colpevole per aver assistito la violazione del *copyright* per aver dato ad uno *user* una password di un sito web che gli ha concesso di scaricare 1,899 file protetti da copyright.

[171]In base al Criminal Code Act 1995 (Cth) sec. 11.2(3), in Australia una persona deve avere l'intenzione che la sua condotta *aid, abet, counsel or procure* un reato del tipo di quello commesso, ed essere *reckless* riguardo alla commissione del reato che l'altra persona ha di fatto commesso.

[172]Tuttavia, non sempre i *disclaimers* sono stati ritenuti sufficienti dalle corti per esonerarsi dalla responsabilità: si veda, ad esempio, Cooper v Universal Music Australia Pty Ltd [2006] FCAFC 187, (2006) 156 FCR 380.

[173]Tali e-mail interne incaute sono state un fattore chiave nel *Kim Dotcom litigation*: si veda Ortmann v The United States of America [2017] NZHC 189.

[174]Ad esempio, Criminal Code Act 1995 (Cth) s 11.4(1). Allo stesso modo, in Nuova Zelanda "*è partecipe e colpevole di un reato chi incita [...] qualsiasi persona a commettere il reato*": Crimes Act 1961 (NZ) s 66(1)(d). Il regime di responsabilità secondaria del Regno Unito ai sensi del Serious Crime Act 2007 (sez. 44-46) racchiude l'istigazione attraverso l'uso del termine «*encourage*» e abolisce il reato di istigazione di common law (s 59). Ad esempio, l'articolo 44(1) della legge britannica stabilisce che «una persona commette un reato se compie un atto in grado di incoraggiare […] la commissione di un reato e intende incoraggiare […] la sua commissione».

nel senso di «eccitare; stimolare; sollecitare o spronare; animare»,[175] diretto «a una persona particolare o in generale».

La gamma di comportamenti che possono essere considerati «istigazione» è ampia. Una persona può essere ritenuta colpevole di istigazione «anche se la persona istigata non fa nulla nel perseguire lo scopo criminale, a condizione che quest'ultima persona abbia sentito e compreso le parole di incitamento»;[176] infatti, si può essere responsabili per il tentativo di istigazione anche quando l'incitamento non venga recepito dalla persona a cui è rivolto.[177]

Con un campo di applicazione così ampio, l'istigazione è potenzialmente in grado di rendere responsabili le persone che presumono che le loro parole o azioni siano meno colpevoli perché non conoscono il loro pubblico o stanno semplicemente lanciando esortazioni generali al mondo in generale, anche online soprattutto in ambito civile.

Non è difficile pensare, infatti, a esempi di controversie civili in materia di *copyright* che potrebbero rientrare in questo paradigma. Si pensi, ad esempio, alla condotta dei fornitori di Kazaa, un software e sistema di condivisione di file P2P ampiamente utilizzato nei primi anni 2000 per violare il copyright su *sound recordings* commerciali. [178]

Nella causa civile australiana *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* per violazione del *copyright*, il giudice ha ritenuto che vi fossero «prove di atti positivi da parte di Sharman che avrebbero avuto l'effetto di incoraggiare la violazione del copyright» tra cui «esortazioni agli utenti a utilizzare questo strumento e a condividere i loro file» e «promozione del movimento 'Join the Revolution', che si basa sulla condivisione di file, in particolare di musica, e che disprezza l'atteggiamento delle case discografiche e cinematografiche in relazione alle loro opere protette da copyright».[179]

[175] WEATHERALL, *Criminal Sanctions*, cit., 543.
[176] WEATHERALL, *Criminal Sanctions*, cit., 543.
[177] WEATHERALL, *Criminal Sanctions*, cit., 543.
[178] Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2005] FCA 1242, (2005) 222 FCR 465. Si veda anche Metro-Goldwyn-Mayer Studios In v Grokster Ltd 545 US 913 (2005).
[179] Universal Music Australia Pty Ltd v Sharman License Holdings Ltd, già citato.

4.3.2.3. Consiparcy.

L'accusa di *conspiracy* impone la responsabilità per aver concordato di commettere un crimine, indipendentemente dal fatto che il crimine venga poi commesso, e indipendentemente dal fatto che si possa dimostrare che l'imputato (di responsabilità secondaria) abbia partecipato effettivamente alla commissione del reato.[180] La caratteristica chiave della *conspiracy* è «l'intenzione condivisa di commettere un crimine in base ad un accordo»[181] tra almeno due persone.

Il concetto di «accordo» è sufficientemente ampio da coprire le relazioni che si instaurano anche online. Un accordo che costituisce una *conspiracy* può essere dimostrato attraverso atti o parole e può essere espresso o tacito, formale o informale; e un cospiratore può «stipulare un accordo con una o più persone senza sapere quante persone hanno precedentemente stipulato l'accordo o l'identità di queste altre persone».[182]

Non è previsto l'obbligo di identificare, né tantomeno di perseguire, contemporaneamente tutte le parti. Ciò è potenzialmente utile nell'ambiente online, dove non vi è sempre la possibilità di identificare tutte le persone coinvolte, né tanto meno di incriminarle. Ad esempio, nel 2012 le autorità statunitensi hanno denunciato per *conspiracy* finalizzata alla violazione del *copyright* Kim Dotcom e varie altre persone coinvolte in Megaupload, un popolare sito *web* di *file hosting*. Le autorità statunitensi hanno sostenuto che Kim Dotcom, in qualità di fondatore, maggiore azionista ed ex amministratore delegato, supervisionando il sito web e creando incentivi finanziari per gli utenti che caricavano file particolarmente popolari (per lo più in violazione di materiale protetto), ha cospirato con gli utenti del sito - un gruppo numeroso, mutevole e parzialmente anonimo - per violare il *copyright* allo scopo di ottenere un vantaggio commerciale e un guadagno finanziario privato.[183]

Uno dei più grandi dibattiti in corso sulla proprietà intellettuale in generale, e sul *copyright* in particolare, nel contesto online, come ampiamente visto nel corso

---

[180]WEATHERALL, *Criminal Sanctions*, cit., 544.
[181]Criminal Code Act 1995 (Cth) sec. 11.5(2)(b): *"(2) For the person to be guilty:*
(b) the person and at least one other party to the agreement must have intended that an offence would be committed pursuant to the agreement."
[182]WEATHERALL, *Criminal Sanctions*, cit., 544.
[183]Ortmann v The United States of America, già citato.; upheld in Ortmann v United States of America [2018] NZCA 233.

del presente elaborato, è stato quello di stabilire quando sia opportuno rendere i *providers* responsabili delle violazione che si verifica sulle loro piattaforme e attraverso le loro reti, e quando il desiderio di promuovere l'innovazione, la disponibilità e l'accessibilità della tecnologia digitale, la libertà di parola e la libertà d'impresa impongono, invece, di proteggerli dal pericolo di sanzioni, *a fortiori* se penali.

Il fatto che lo sviluppo tecnologico non sembri rallentare, anzi, stia crescendo di anno in anno è probabilmente dovuto a una combinazione di fattori: (I) i bassi livelli di consapevolezza della portata della responsabilità secondaria e della possibilità di subire un'azione penale da un lato, a causa delle difficoltà nel provare i reati e in particolare il dolo secondo lo standard richiesto (oltre il ragionevole dubbio), e (II) la complessità e il costo di tali casi, dall'altra.[184] Tuttavia, non sono mancati casi, diametralmente opposti, in cui addirittura si è proceduto all'estradizione a seguito di condanna per *conspiracy* finalizzata alla violazione di *copyright*: si tratta dei casi Richard O'Dwyer[185] e Hew Griffiths.[186]

Le violazioni del *copyright* che avvengono online attraversano quasi sempre i confini statali, ponendo sfide avvincenti a un'efficace applicazione globale della proprietà intellettuale. In teoria, il diritto penale è territoriale: la punizione penale extraterritoriale mina l'ordine giuridico internazionale che divide il mondo in Stati, i quali hanno il diritto esclusivo di regolare, secondo i propri principi generali, la condotta all'interno dei propri confini.

Lungi dal limitare la responsabilità penale, la natura globale dell'attività online rende potenzialmente più facile per gli Stati rivendicare la giurisdizione per perseguire il reato sulla base del fatto che– magari solo una parte– della condotta che costituisce il reato, si è verificato nel loro territorio.

I meccanismi di cooperazione penale transnazionale possono portare l'autore del reato – reato compiuto all'estero – alla portata delle forze dell'ordine nazionali. In questo modo, una gamma più ampia di individui - anche quelli che

[184]WEATHERALL, *Criminal Sanctions*, cit., 544 s.
[185]In the Westminster Magistrates' Court, The Government of the United States of America v Richard O'Dwyer (2012).
[186]Griffiths v US, già citato.

rimangono interamente all'interno dei confini di un paese - può esporsi al rischio di essere perseguiti all'estero.

È proprio ciò che è avvenuto con i casi succitati: nel 2015, il residente Australiano Hew Griffiths è stato incriminato in Virginia for *committing, aiding and abetting and conspiring* una violazione del copyright.[187] Griffiths faceva parte di DrinkorDie ("DOD"), un gruppo di individui che utilizzava un *server*, situato in Virginia, protetto da *password*, per riprodurre e distribuire ai membri software commerciali, giochi, film e musica (in particolare quelli non ancora commercializzati) senza l'autorizzazione dei proprietari del *copyright*. Il tribunale australiano non ha avuto difficoltà a definire la condotta in questione come avvenuta fisicamente negli Stati Uniti, nonostante lo stesso Griffiths si trovasse in Australia in ogni momento. Griffiths è stato estradato e ha scontato 15 mesi in un carcere statunitense.

Nel 2007 gli Stati Uniti hanno chiesto l'estradizione di Richard O'Dwyer, uno studente britannico che aveva creato il sito web TVShack, che rimandava a programmi e film disponibili gratuitamente online. Richard O'Dwyer è stato ritenuto idoneo per l'estradizione, ma ha raggiunto un accordo di rinvio dell'azione penale, ha pagato una multa ed è rimasto nel Regno Unito.

Nel 2012, gli Stati Uniti hanno carcato di estradare Kim Dotcom e altre persone dalla Nuova Zelanda per affrontare le accuse relative a Megaupload, un sito di *cyberlocker* gestito da circa 1000 server che archiviavano e rendevano disponibili circa 25 petabyte di file presumibilmente in violazione del *copyright*. Si stima che al suo apice Megaupload generasse il 4% del traffico Internet globale, con 50 milioni di visite giornaliere. Il giudice statunitense ha incriminato Dotcom e altre persone coinvolte nell'attività per una serie di reati, tra cui la violazione del *copyright*, *aiding and abetting and conspiracy* finalizzata alla violazione del copyright, oltre a reati di diritto generale come *conspiracy* finalizzata al racket e al riciclaggio di denaro e, infine, la frode telematica. Tuttavia, nel momento in cui si

[187]Griffiths è stato accusato di criminal copyright infringement. Secondo la legge statunitense, una persona che aiuta e favorisce la commissione di un reato è punibile come un *principal*. 18 USC §2 (a): «(a)Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal».

scrive, non si hanno ancora notizie circa l'estradizione dell'imprenditore statunitense, che al momento continua a risiedere in Nuova Zelanda.

CONCLUSIONE.

Alla luce di quanto affermato sinora, è possibile trarre le seguenti conclusioni. In particolare, come anticipato nell'introduzione alla dissertazione, scopo del presente elaborato era quello di trovare delle risposte ad una serie di domande attinenti alla responsabilità delle piattaforme digitali: nello specifico, ci si è chiesti se una piattaforma di tal tipo potesse essere ritenuta responsabile per i fatti illeciti commessi dall'utente tramite i propri servizi; fatti illeciti, inerenti alla violazione dei diritti di proprietà intellettuale.

Ebbene, si è avuto modo di vedere come, col ricorrere di determinate condizioni, alla piattaforma digitale, così come definita nella premessa del Capitolo II, possa imputarsi una responsabilità, sia penale che civile.

Ovviamente, coerentemente con il principio di *extrema ratio* della sanzione penale, le condizioni in presenza delle quali sorge una responsabilità di tal genere sono assai più rigorose di quelle invece previste per il sorgere di una responsabilità civile. In particolare, se per l'imputabilità di una responsabilità civile è sufficiente che il *provider* tenga una condotta «attiva» o, in alternativa, che abbia una «mera» conoscenza del materiale illecito dovuta anche ad una comunicazione non qualificato, al contrario, per l'imputabilità di una responsabilità penale non è sufficiente la «mera» conoscenza del materiale illecito ma è necessario che tale conoscenza derivi da una comunicazione «qualificata», cioè da un soggetto dotato di autorità.

Chiarito ciò, si è poi passati ad indagare la natura delle due responsabilità: nello specifico, riguardo alla responsabilità penale, il dubbio verteva sull'applicazione della responsabilità per omesso impedimento *ex* articolo 40 co. 2 c.p., o, in alternativa, della responsabilità concorsuale omissiva nel reato commissivo dell'utente *ex* combinato disposto degli articoli 40 co. 2 e 100 c.p; con riferimento alla responsabilità civile, invece, il dubbio ricadeva sull'applicazione della responsabilità contrattuale *ex* articolo 1218 c.c. o, alternativamente, delle responsabilità extracontrattuale *ex* articolo 2043 c.c.

Ebbene, con riferimento alla responsabilità penale, si è sostenuta l'adozione della seconda alternativa, in quanto è stato dimostrato come in capo alla piattaforma

digitale non siano configurabili né obblighi giuridici di impedire l'evento – per espressa previsione normativa che non obbliga le piattaforme a «vigilare» sui contenuti pubblicati dagli utenti –, né posizioni di garanzia e di controllo – in quanto l'utente non ha peculiarità che lo rendono di per sé pericoloso ed, inoltre, il *provider* non ha alcun legame sostanziale con la fonte pericolosa, cioè l'utente –, e di protezione – non sembra infatti configurabile come bene giuridico da proteggere una "rete sana", rispetto al quale il *provider* assume una posizione di protezione da ogni fonte di pericolo. Posizione di garanzia che sorgerebbe, al contrario, nel momento in cui la piattaforma digitale riceve una comunicazione «qualificata» riguardo la potenziale esistenza di un contenuto illecito: infatti, sembrerebbe che a seguito di tale comunicazione si venga a creare quel legame sostanziale tra piattaforma e fonte pericolosa (non già l'utente potenziale *reo*, bensì la rete, che dopo la memorizzazione del contenuto illecito diviene «pericolosa»)[1] che contraddistingue le posizioni di garanzia, e crea in questo caso obblighi di controllo in capo al gestore della piattaforma. Si parla in tal caso di concorso mediante omissione nel reato commissivo compiuto da altri ex combinato disposto degli articoli 40 co. 2 c.p. e 110 c.p.

Riguardo alla responsabilità civile, il presente elaborato, ha illustrato le motivazioni per cui alcuni sostengono che alla piattaforma digitale vada imputata una responsabilità aquiliana ex articolo 2043 c.c. mentre altri ritengono ad essa imputabile una responsabilità contrattuale ex articolo 1218 c.c.: questi ultimi, in particolare, ritengono che esista un rapporto tra le parti – *provider* e titolare dei diritti lesi –, tale per cui l'obbligo di rimozione del contenuto illecito a carico del *provider* eviterebbe la lesione della sfera giuridica di un soggetto ben determinato (*i.e.*, il soggetto leso che normalmente è anche autore della diffida). Al contrario, i sostenitori dell'applicazione dell'articolo 1218 c.c. ritengono che le disposizioni

[1]Cfr. BARTOLI, *Brevi considerazioni sulla responsabilità penale*, cit., 606. Nello stesso senso anche TERRACINA, *La tutela penale del diritto d'autore*, cit., 185: «Deve, infine, tenersi in considerazione il fatto che, come già accennato, nel nostro ordinamento penale la responsabilità ai sensi del capoverso dell'art. 40 c.p. appare ammissibile solamente in relazione alla protezione di diritti fondamentali quali la vita o l'incolumità fisica e non certo per interessi di carattere patrimoniale quali quelli tutelati dalla LDA. Diverso potrebbe apparire il discorso nell'ipotesi in cui, una volta individuata l'attività illecita posta in essere attraverso *Internet* venga invitato il *provider* a provvedere con i mezzi tecnici a sua disposizione a rimuoverla dalla Rete. In questo caso, infatti, potrebbe configurarsi una sorta di 'messa in mora' del *provider* alla quale, in una prospettiva *de iure condendo*, potrebbe ricollegarsi una qualche responsabilità penale».

normative limitandosi ad individuare una responsabilità in senso negativo assegnerebbero al *provider* un onere di agire, non già un obbligo: in altre parole, ritengono che se il *provider*, dopo averne preso conoscenza, non procede alla rimozione del materiale illecito, egli tuttavia non avrebbe un obbligo in senso tecnico di agire in tal senso.

Tutto dipende da come si costruisce il dovere di rimozione del contenuto illecito da parte del *provider*: se come dovere giuridico *erga omnes* o come dovere specifico nei confronti del solo soggetto leso. In questa seconda ipotesi, si dovrebbe optare per imputare all'*ISP* una responsabilità di tipo contrattuale a discapito di quella aquiliana con tutte le differenze di disciplina che ne derivano.

BIBLIOGRAFIA

ALBERTINI, *La responsabilità civile degli ISP per i materiali caricati dagli utenti*, in *Il Caso.it*, 2020.

ALLGROVE, GROOM, *Enforcement in a digital context: intermediary liability*. "Research Handbook on Intellectual Property and Digital Technologies", edited by Tanya Aplin, Edward Elgar Publishing Ltd., 2019.

ALMBORG, *Counterfeiting and Piracy, From a right holders perspective*.

AMENDOLARA, *Knocking Out Knock-Offs: Effectuating the Criminalization of Trafficking in Counterfeit Goods*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 15, 3, 2005.

BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider*, in Diritto penale e processo, vol. 19, 5, 2013, 600.

BELLAN, *Per una reasonable liability: critiche alla responsabilità oggettiva degli internet service provider e tutela dei diritti*, in *Il diritto industriale*, 3, 2012, 243.

CAMPOBASSO, *Diritto commerciale 1: diritto dell'impresa*, 7ª ed, Milano, 2017.

CASABURI, *Nomi a dominio Internet e tutela della proprietà industriale*, in *Giurisprudenza di merito*, 5, 2008, 1492.

CINGARI, *Misure punitive per il rilancio della competitività: tra repressione dell'incauto acquisto di prodotti «taroccati» e tutela del made in Italy*, in *Diritto Penale e processo*, 11, 2005, 1337.

DE STEEL, LAROUCHE, *An Integrated Regulatory Framework for Digital Networks and Services. A CERRE Policy Report*, 2016.

DI AGOSTA, *Il caso "Pirate Bay" arriva alla Cedu: spunti per una riflessione sulla responsabilità degli "internet service provider", tra libertà d'espressione e reati in materia di "copyright!*, Nota a Corte eur. Dir. Uomo sez. V 13 marzo 2013 (Neij e Sunde Kolmisoppi c. Svezia), in *Cassazione penale*, 10, 2013, 3375.

DI CIOMMO., *Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei providers di Internet nell'incerta giurisprudenza europea*, in *Il Foro Italiano*, 6, 2019, 2072.

DI TODARO, *Il caso "The Pirate Bay" tra libertà di espressione e diritto d'autore*, Nota a Corte eur. Dir. Uomo sez. V 19 febbraio 2013 (Fredrik Neij e Peter Sunde Kolmisoppi c. Svezia), in *Giurisprudenza costituzionale*, 6, 2014, 4786.

FALLENBÖCK, *On the Technical Protection of Copyright: The Digital Millennium Copyright Act, the European Community Copyright Directive and Their Anticircumvention Provisions*, in *International Journal of Communications Law and Policy*, 2003.

FLOR, *Autore (Diritto di) (diritto penale)*, in Enciclopedia del Diritto- Annali X-2017, 111.

FROMER, SPRIGMAN, *Copyright Law: Cases and Materials*, 2022.

GALLI, *I domain name nella giurisprudenza. L'analisi dei problemi. Il testo di 78 provvedimenti italiani dal 1996 al 2001. Il repertorio sistematico delle massime*, Milano, 2001.

GATTA, *La disciplina della contraffazione del marchio d'impresa nel codice penale (artt. 473 e 474): tutela del consumatore e/o del produttore?*, in *Diritto penale contemporaneo*, 2012.

GIUNTA, *Lineamenti di diritto penale dell'economia*, 2ª ed., Giappichelli, Torino, 2004.

INGRASSIA, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?, Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*. In: (a cura di): LUPÁRIA, Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale, Milano, 2012.

JENSEN, *The More Things Change, the More They Stay the Same: Copyright, Digital Technology, and Social Norms*, in *Stanford Law Review*, vol. 56, 2003, 2.

LEANZA, *La responsabilità dell'hosting provider per violazione del diritto d'autore*, in *Danno e responsabilità*, 5, 2019, 671.

MANCA, *La tutela penale della proprietà industriale e della struttura produttiva italiana. Prospettive e ripercussioni della legge 23 luglio 2009*, n. 99, Padova, 2009.

MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale: parte generale*, 9ª ed., Milano, 2020.

MERLA, *Diffusione abusiva di opere in internet e sequestro preventivo del sito web: il caso "The Pirate Bay"*, Nota a Cass. sez. III pen. 23 dicembre 2009, n. 49437, in *Il Diritto dell'informazione e dell'informatica*, 3, 2010, 448.

OMODEI, *La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione*, in *Diritto penale contemporaneo*, 2019, 112.

PARODI, *Profili di tutela penale dei domini su internet*, in *Diritto penale e processo*, 4, 2001, 505.

PISANI, *I reati contro la fede pubblica*. In: (a cura di): FIORELLA, Questioni fondamentali della parte speciale del diritto penale Torino, 2012.

RIVERDITI, *La tutela penalistica della proprietà intellettuale*, in *Diritto ed economia dell'impresa*, 1, 2016, 66.

SARTOR, LOREGGIA, *The Impact of Algorithms for Online Content Filtering or Moderation*, Policy Department for Citizens' Rights and Constitutional Affairs, 2020.

SCALZINI, *Hyperlinking e violazione del diritto d'autore nell'evoluzione giurisprudenziale europea*, in *Analisi giuridica dell'economia*, 2, 2017, 639.

STUART, *The Criminalization of Trade Secret Theft: The Economic Espionage Act of 1996*, in *ILSA Journal of International & Comparative Law*, Vol. 4, 1998.

SVENSSON, LARSON, *Social Norms and Intellectual Property, Online norms and European Legal Development*, in *Research Report in Sociology of Law*, Vol. 1, 2009.

TERRACINA, *La tutela penale del diritto d'autore e dei diritti connessi*, Torino, 2006.

VAN HOBOKEN, KELLER, *Design Principles for Intermediary Liability Laws*, 2019.

WEATHERALL, *Criminal Sanctions as a Tool Against Online Infringement: National Law, International Treaties, Transnational Cooperation (August 17, 2018)*, in "Research Handbook on Intellectual Property and Digital Technologies", edited by Tanya Aplin, Edward Elgar Publishing Ltd., 2019, Forthcoming, Sydney Law School Research Paper No. 18/49.

YEH, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Congressional research service, 2014.

INDICE GIURISPRUDENZA

Cass. pen., Sez. II, 5 febbraio 2014, n. 5687.
Cass. pen., Sez. VI, 29 aprile 2015, n. 18015.
Cass. Pen., Sez. III, 26 gennaio 2016, n. 23365.
Cass. pen., Sez. V, 14 luglio 2016, n. 54946.
Huon v.Denton, 841 F.3d 733 (7th Cir. 2016).
Cass. pen., Sez. V, 28 luglio 2017, n. 37957.
Mavrix Photographs, LLC v LiveJournal, Inc. 853 F.3d 1020, 1033 (9th Cir 2017).
Ortmann v The United States of America [2017] NZHC 189.
Cass. pen., Sez. V, 19 luglio 2018, n. 33900.
Ortmann v United States of America [2018] NZCA 233.
Trib. di Roma, 10 gennaio 2019, n. 693.
Cass. Civ., Sez. I, 19 marzo 2019, n.7708.
Cass. Civ., Sez. I, 19 marzo 2019, n.7709.
Cass. Pen., Sez. II, 2 ottobre 2019, n.40324.
Cass. Pen. Sez. II, 1 giugno 2020, n.16568.
Cass. pen., Sez. V, 3 settembre 2020, n. 25036.
Cass. pen., Sez. V, 15 giugno 2022, n. 23364.