

Andrea Stazi

**I MULTIFORMI APPROCCI
DEI PAESI DELL'ASIA
ESTREMO-ORIENTALE E
DELL'OCEANIA ALLA
RESPONSABILITÀ DEGLI
INTERMEDIARI ONLINE: UNA
PANORAMICA
COMPARATISTICA DA UNA
PROSPETTIVA OCCIDENTALE**

Estratto



Milano • Giuffrè Editore

ANDREA STAZI

I MULTIFORMI APPROCCI DEI PAESI DELL'ASIA ESTREMO-ORIENTALE E DELL'OCEANIA ALLA RESPONSABILITÀ DEGLI INTERMEDIARI ONLINE: UNA PANORAMICA COMPARATISTICA DA UNA PROSPETTIVA OCCIDENTALE

SOMMARIO: I. Introduzione: caratteristiche, economia e policy degli intermediari online. — II. Questioni di policy in gioco. — II.1. Libertà di espressione. — II.2. Innovazione. — II.3. Sorveglianza. — II.4. Le funzioni della regolazione. — III. Approcci regolatori. — III.1. I multiformi approcci dei Paesi dell'Asia estremo orientale e dell'Oceania (da una prospettiva occidentale). — III.2. La responsabilità degli intermediari negli Stati Uniti. — III.3. La responsabilità degli intermediari nell'Unione Europea. — III.4. Le linee guida internazionali. — IV. Modelli di governance. — IV.1. *Legal process*. — IV.2. Regolazione contestuale. — IV.3. Coregolazione. — IV.4. Enforcement. — V. Considerazioni finali. — V.1. Interazioni tra responsabilità degli intermediari, sviluppo, cultura e diritti fondamentali. — V.2. Efficienza economica e considerazioni di policy.

I. INTRODUZIONE: CARATTERISTICHE, ECONOMIA E POLICY DEGLI INTERMEDIARI ONLINE.

Gli intermediari *online* di varie tipologie — inclusi i motori di ricerca, i *social media* o le piattaforme che forniscono applicazioni — svolgono un ruolo estremamente rilevante nell'odierno scenario socio-economico. Dato che le dimensioni e la portata di internet sono cresciute fino a permeare tutti gli aspetti dell'economia e della società, parimenti è cresciuto anche il ruolo degli intermediari *online*, che danno accesso, ospitano, trasmettono o indicizzano il contenuto originato da terze parti o forniscono tramite internet servizi a terzi.

* Il presente lavoro è stato preventivamente sottoposto a referaggio secondo le prassi correnti nella comunità dei giuristi.

Gli intermediari svolgono un'ampia gamma di attività, tra cui quelle di piattaforme pubblicitarie *online*, motori di ricerca, *social media* o fornitori di contenuti creativi, *marketplace*, piattaforme di distribuzione delle applicazioni, fornitori di servizi di comunicazione, fornitori di sistemi di pagamento e piattaforme per l'economia collaborativa.

Le caratteristiche chiave dei loro servizi comprendono l'uso delle tecnologie dell'informazione e della comunicazione per facilitare le interazioni — comprese le transazioni commerciali — tra gli utenti, la raccolta e l'uso dei dati che si basano su queste interazioni e gli effetti di rete che rendono l'utilizzo delle piattaforme con un maggior numero di utenti più utile per gli altri utenti ¹.

La ragione per cui gli intermediari *online* — da piccole bacheche a siti come Google, Baidu, Yandex, YouTube, Facebook, Amazon, Alibaba, eBay, Twitter, Airbnb, Uber, ecc. — sono diventati così importanti e vantaggiosi è che permettono a chiunque, ovunque si trovi, di connettersi istantaneamente con miliardi di persone in tutto il mondo. Prima, chi voleva parlare ad un vasto pubblico doveva avere a disposizione una torre di trasmissione; chi voleva raggiungere i consumatori di tutto il mondo doveva aprire dei punti vendita ovunque. Ora, tutto ciò che serve è un sito *web* e tutti possono connettersi con un pubblico globale ².

Analizzando le questioni relative alla *governance* degli intermediari *online* da più punti di vista e nel contesto di culture e quadri normativi differenti, si creano immediatamente problematiche di base di interoperabilità semantica. Gli intermediari *online* comprendono una vasta gamma di aziende essenziali nel contesto di internet: i fornitori di servizi internet, che forniscono l'accesso a famiglie e imprese; i fornitori di servizi di *hosting*, che affittano lo spazio del *server* del *computer* ad altri; le piattaforme di *social media*, che consentono agli utenti di condividere testi, foto, audio e video; i motori di ricerca, e le più nuove forme di intermediari, come, ad esempio, le società che forniscono passaggi in auto, le piattaforme di noleggio a breve termine, ecc ³.

¹ Si veda, tra gli altri: Commissione europea, Comunicazione "Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa", COM/2016/0288 final, 25 maggio 2016, par. 2, disponibile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52016DC0288>.

² Per un approccio globale alla definizione e all'economia degli intermediari, si vedano: OECD, *The economic and social role of Internet Intermediaries*, April 2010, disponibile al link: <https://www.oecd.org/internet/ieconomy/44949023.pdf>, p. 7 ff.; EDiMA, *Online Intermediaries: Impact on the EU*

Economy, October 2015, disponibile al link: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1466514160026&uri=CELEX:52016DC0288>.

<http://www.europeandigitalmediaassociation.org/pdfs/EDiMA%20-%20Online%20intermediaries%20-%20EU%20Growth%20Engines.pdf>, p. 7 ss., che ha cercato di elaborare una definizione comune e di comprendere ciò che sono gli intermediari di internet e le loro funzioni socio-economiche, i modelli di business ed i mercati.

³ OECD, *The economic and social role of Internet Intermediaries*, cit. p. 9 ss.; A. CHANDER, *Internet Intermediaries as Pla-*

Il termine “intermediario” spesso funge da concetto di riserva in assenza di una definizione chiara. Da un punto di vista giuridico, ad esempio, il fenomeno può essere osservato da varie prospettive, ciascuna delle quali potrebbe condurre all’elaborazione di differenti definizioni. Nei Paesi che hanno elaborato una specifica normativa per regolare il settore dei media, la principale differenza potrebbe essere data dall’impatto del servizio sulla formazione dell’opinione pubblica. Con riferimento alla responsabilità, il focus potrebbe risiedere nel controllo e nella capacità tecnica di eliminare i contenuti ⁴.

Per quanto riguarda la libertà di espressione, gli intermediari svolgono un nuovo tipo di attività e creano uno spazio per gli individui dove esprimere se stessi *online*, funzione che deve essere esaminata a fondo ⁵.

Dal punto di vista economico, la rilevanza che assumono tali servizi sta nel fatto che creano esternalità di rete, ovvero, i benefici derivanti dall’utilizzo del servizio aumentano con la diffusione del servizio stesso; pertanto, la creazione di un numero consistente di utenti è la chiave del successo. Inoltre, tali operatori svolgono spesso la loro attività in mercati a due versanti in cui operano quali intermediari tra due diversi gruppi di agenti, ad esempio, gli utenti e gli inserzionisti o gli acquirenti e i venditori. Quindi, gli intermediari adottano particolari strategie di prezzo e di investimento che potranno coinvolgere entrambi i lati del mercato bilanciando gli interessi dei due lati.

Gli intermediari *online* possono stimolare anche lo sviluppo dell’occupazione e dell’imprenditorialità riducendo gli ostacoli all’avvio e all’operatività delle piccole imprese e creando l’opportunità di compiere delle transazioni economiche c.d. “*long-tail*” che non erano possibili in precedenza, per cui le imprese possono vendere un gran numero di articoli unici, ciascuno dei quali in quantità relativamente piccole.

Così, gli intermediari *online* consentono di far fiorire tra gli individui e le imprese la comunicazione, la creatività e la collaborazione, generando, altresì, innovazione ⁶.

tforms for Expression and Innovation, cit., p. 2; U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, The Berkman Center for internet & Society Research Publication No. 2015-5, February 2015, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566364, p. 1.

⁴ Si veda: F. DI CIOMMO, *Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza Google/Vivi down*, in *Diritto dell’informazione e dell’informatica*, 2010, p. 830.

⁵ Cfr.: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 2-3.

⁶ Si veda, tra gli altri: Commissione europea, Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy, May 2016 disponibile al link: <https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-intermediaries>, p. 6 ss., in

Dal punto di vista regolatorio, gli intermediari *online* sono al centro di dibattiti intensi e spesso controversi⁷. Naturalmente, poi, come con qualsiasi tecnologia, alcune persone la usano impropriamente. Per sua natura, la tecnologia può creare nuove sfide e complessità e gli intermediari *online* sono diventati un punto fondamentale per la regolazione di internet a livello globale. Visto che aiutano le imprese, le organizzazioni e gli individui a connettersi in tutto il mondo coinvolgendo più ambiti della loro vita, vengono considerati come degli arbitri cruciali in grado di stabilire ciò che è permesso o non è permesso in una determinata società. I governi ritengono che gli intermediari *online* siano dei punti nevralgici sui quali esercitare il controllo, essendo molto più facile lo svolgimento di questo compito rispetto a quello di regolare direttamente gli individui che usano internet. Pertanto i governi spesso richiedono agli intermediari di censurare le informazioni in modo che non siano distribuite tra i loro cittadini,

cui, mentre non vi era il consenso su una possibile definizione giuridica delle piattaforme online, la maggior parte degli intervistati concordava sul fatto che vi siano significativi benefici derivanti dalle piattaforme stesse, in quanto guidano l'innovazione, facilitano le interazioni sociali e sono potenti motori di crescita; H. LEE-MAKIYAMA, R. GEORGIEVA, *The Economic Impact of Online Intermediaries*, in M. TADDEO, L. FLORIDI, *The Responsibilities of Online Service Providers*, Springer, 2017, p. 325 ss.; B. MARTENS, *An Economic Policy Perspective on Online Platforms*, European Commission Joint Research Centre - Institute for Prospective Technological Studies, *Digital Economy Working Paper* 2016/05, disponibile al link: <https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf>, p. 8 ss.; EDiMA, *Online Intermediaries: Impact on the EU Economy*, October 2015, cit., p. 8 ss.; OECD, *The economic and social role of Internet Intermediaries*, cit., p. 15 ss.

⁷ Si vedano, tra gli altri: A. SPAGNOLO, *Bilanciamento tra diritto d'autore, libertà d'impresa e libertà fondamentali nella giurisprudenza recente della Corte di Giustizia*, in *Giurisprudenza di merito*, 2013, p. 125; M. BELLIA, G.A.M. BELLOMO, M. MAZZONCINI, *La responsabilità civile dell'Internet Service Provider per violazioni del diritto d'autore*, in *Diritto industriale*, 2012, p. 346; M. COLANGELO, *Internet e sistemi di filtraggio tra enforcement del diritto d'autore e tutela dei diritti fondamentali: un commento ai casi Scarlet e Netlog*, in *La nuova giurisprudenza civile commentata*, 2012, p. 580; A. MONTA-

NARI, *Prime impressioni sul SABAM c. Netlog NV: gli Internet Service Provider e la tutela del diritto d'autore online*, in *Diritto del commercio internazionale*, 2012, p. 1075; E. TOSI, *Tutela dei contenuti digitali in internet e responsabilità civili degli internet service provider*, 2013, disponibile al link: http://www.elusit.it/whitepapers/resp_isp_2013.pdf; R. JULIÀ-BARCELÒ, K. J. KOLEMAN, *Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough!*, in *Computer Law & Security Report*, 2000, p. 231; A. MUSSO, *La proprietà intellettuale nel futuro della responsabilità sulla rete: un regime speciale?*, in *Diritto dell'informazione e dell'informatica*, 2010, p. 795. Più in generale si veda P.S. MENELL, *Envisioning Copyright Law's Digital Future*, in *New York Law School Law Review*, Vol. 46, 2002-2003, p. 63; L. BELLÌ, N. ZINGALES (a cura di), *Platforms regulations: how platforms are regulated and how they regulate us*, Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility - Geneva, December 2017, FGV Direito Rio, disponibile al link: <http://bibliotecadigital.fgv.br/dspace/handle/10438/19402>; Commissione europea, *Full report on the results of the public consultation on the Regulatory environment for Platforms, Online Intermediaries and the Collaborative Economy*, cit., e la seguente Comunicazione "Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa", cit.; G.B. DINWOODIE, *A Comparative Analysis of the Secondary Liability of Online Service Providers*, in G.B. DINWOODIE (a cura di), *Secondary Liability of Internet Service Providers* Springer, 2017, disponibile al link: <https://ssrn.com/abstract=2997891>.

ovvero utilizzano gli stessi per ottenere alcune delle informazioni che raccolgono dai loro utenti ⁸.

Tuttavia, l'imposizione del ruolo di censore e di polizia per l'era dell'informazione mina le capacità di *empowerment* dell'individuo che gli intermediari *online* possono avere ⁹. Rendere gli intermediari responsabili per le informazioni scambiate sulle loro piattaforme può condurre gli stessi a bloccare anche i contenuti leciti, per timore che possano trovarsi ad affrontare delle richieste di risarcimento danni. Fare in modo che gli intermediari *online* svolgano attività censoria o di polizia può indurre le persone ad autocensurarsi, per evitare di attirare l'attenzione indesiderata delle autorità o degli intermediari. Gli obblighi di monitoraggio dei contenuti per timore di incorrere in responsabilità non solo pregiudicano la libertà di espressione, ma scoraggiano anche l'innovazione ¹⁰.

Tuttavia, recentemente il dibattito sull'argomento è molto acceso e molteplici sono le iniziative a livello politico e della dottrina, che continua a studiarne le varie implicazioni, tra cui, in particolare, quelle etiche, che si concentrano sull'influenza significativa degli intermediari *online* sull'ambiente informativo, sulle interazioni degli utenti al suo interno e sulle responsabilità successive che tale influenza comporterebbe ¹¹.

In un simile contesto, si deve, inoltre, considerare che spesso la

⁸ Nel 2014 l'UNESCO ha pubblicato un rapporto sugli intermediari di internet in relazione ai diritti digitali nel mondo, in cui ha rilevato come le operazioni degli intermediari di internet siano fortemente influenzate dagli ambienti giuridici e politici degli Stati. Si veda: R. MACKINNON, E. HICKOK, A. BAR and H. LIM, *Fostering Freedom Online: The Role of Internet Intermediaries*, United Nations Educational, Scientific and Cultural Organization Report, 2014, disponibile al link: <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>, p. 10 ss.

⁹ Si veda S. MAGLI, M.S. SPOLIDORO, *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Diritto dell'Informazione e dell'Informatica*, 1997, p. 61.

¹⁰ A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, Global Commission on internet Governance, Paper Series No. 42 - November 2016, disponibile al link: <https://www.cigionline.org/publications/internet-intermediaries-platforms-expression-and-innovation>, p. 1. Cfr. anche: G. CASSANO e A. CONTALDO, *La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza*, in *Corriere giuridico*, n. 9/2009, p. 1206. Parte della dottrina italiana

ha sostenuto, poi, che la situazione di responsabilità dell'ISP sia di colpa per omesso controllo — ex art. 2049 c.c., responsabilità del padrone o committente — che avviene “tutte le volte che l'ISP non impedisce l'evento illecito, poiché non controlla la liceità dei contenuti immessi dall'esterno sul server da lui gestito. Questa figura sarebbe assimilabile a quella ricavabile dall'art. 57 c.p.(responsabilità del direttore o vicedirettore responsabile di uno stampato periodico). In tal senso: R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione*, Cedam, 2002, p. 321.

¹¹ Si veda: M. TADDEO, L. FLORIDI, *The Responsibilities of Online Service Providers*, cit., p. 1 ss.; B.G. JOHNSON, *Speech, Harm, and the Duties of Digital Intermediaries: Conceptualizing Platform Ethics*, in *Journal of Media Ethics*, 2017, Vol. 32, No. 1, p. 16 ss. Si veda anche: M. GAMBINI, *Colpa e responsabilità nella fornitura di servizi internet*, in CLARIZIA, *I contratti informatici*, a cura di CLARIZIA, in *Trattato dei contratti*, diretto da P. Rescigno ed E. Gabrielli, Vol. VI, Utet, 2007, p. 559. Per un approfondimento sulla disciplina afferente alla regolamentazione della responsabilità civile dei prestatori intermediari, si veda: R. BOCCHINI, *Il contratto di accesso a inter-*

tecnologia digitale e le relative soluzioni sociali e di mercato possono facilitare l'adeguamento e l'individuazione dell'utilizzo abusivo delle piattaforme *online*. Gli intermediari hanno degli incentivi per individuare gli abusi commessi attraverso i loro servizi, educare gli utenti e creare degli strumenti di auto-aiuto che consentano agli utenti di proteggersi ¹².

Dunque, i politici, i regolatori e le corti in diverse parti del mondo continuano a confrontarsi con la sfida di riuscire a definire le varie funzioni che svolgono i diversi tipi di intermediari.

Questa ricerca, attraverso il metodo comparatistico, l'ottica interdisciplinare e la prospettiva del giurista occidentale, mira a fornire una panoramica delle principali questioni ed evoluzioni in merito alla responsabilità degli intermediari *online* negli ordinamenti dell'Asia estremo orientale e dell'Oceania, nonché — nella prospettiva della circolazione dei modelli — degli Stati Uniti e dell'Unione Europea.

L'oggetto dello studio si concentra sui servizi che: (a) sono “nel mezzo” tra servizi/contenuti e utenti; (b) mostrano la rilevanza strutturale della condivisione di informazioni e della comunicazione pubblica per la fornitura di servizi/contenuti (ossia non

net, in R. BOCCHINI, A.M. GAMBINO (a cura di), *I contratti di somministrazione e di distribuzione*, Utet, 2011, p. 166. Cfr. altresì: A. DE CUPIS, *Tradizione e rinnovamento nella responsabilità civile*, in *Rivista di diritto civile*, 1979, Vol. II, p. 319.

¹² Su questi temi, il summenzionato Rapporto dell'UNESCO ha fornito un elenco di raccomandazioni incentrate sul rispetto dei diritti umani, della trasparenza, della partecipazione e della possibilità di dare maggiori poteri agli utenti: i) Le leggi e i regolamenti che regolano gli intermediari dovrebbero essere coerenti con le norme internazionali sui diritti umani, incluso il diritto alla libertà di espressione; ii) Le leggi, i regolamenti e le politiche governative, nonché le policy e le regole aziendali, dovrebbero essere sviluppati consultando tutte le parti interessate; iii) il rapporto sulla trasparenza e le altre azioni per comunicare con il pubblico in merito alle politiche e alle prassi aziendali dovrebbero essere completi e sufficientemente standardizzati in modo che sia possibile confrontare e analizzare i set di dati tra più imprese; iv) I regimi di protezione dei dati a livello nazionale sono vitali, così come lo sono i quadri giuridici e altri meccanismi per garantire che l'accesso dei governi ai dati degli utenti e le pratiche aziendali nella gestione delle richieste governative si basino su rigidi principi di necessità, proporzionalità e responsabilità in termini di meccanismi rimediali;

v) Le regole private degli intermediari e i relativi processi di applicazione, così come gli sforzi sostenuti dal governo per l'autoregolamentazione collettiva da parte delle imprese, dovrebbero essere compatibili con le norme sui diritti umani, incluso il diritto alla libertà di espressione. Dovrebbero aderire ai principi fondamentali di responsabilità, trasparenza e giusto processo; vi) Dovrebbe essere possibile per le persone presentare reclami e ottenere una riparazione dagli intermediari privati e dalle autorità statali, incluse le istituzioni nazionali per i diritti umani; vii) Affinché la libertà di espressione sia protetta e rispettata online, i governi e le imprese hanno la responsabilità di consultare le parti interessate sulle loro leggi e regole e illustrarle chiaramente. Hanno anche l'obbligo di educare gli utenti sui loro diritti in modo che le persone possano comprenderli ed esercitarli efficacemente; riconoscere quando i loro diritti sono stati limitati, violati o altrimenti interferiti; e sapere dove e come effettuare delle segnalazioni e chiedere la riparazione; viii) Le parti interessate alla tutela della libertà di espressione *online* dovrebbero considerare come sostenere e ampliare i meccanismi globali che rafforzano gli incentivi e la capacità degli intermediari di rispettare i diritti degli utenti di internet, in particolare nel settore dell'autoregolamentazione (si veda R. MACKINNON, E. HICKOK, A. BAR and H. LIM, *Fostering Freedom Online: The Role of Internet Intermediaries*, cit. p. 13).

sono meramente privati); e (c) non sono tradizionali servizi media, creatori di servizi/contenuti ¹³.

L'obiettivo dell'analisi è l'identificazione di alcuni punti chiave da prendere in considerazione nell'affrontare una problematica così articolata e dinamica.

II. QUESTIONI DI POLICY IN GIOCO.

II.1. *Libertà di espressione.*

Come sostenuto nelle conclusioni del citato Rapporto dell'UNESCO, limitare la responsabilità degli intermediari per i contenuti pubblicati o trasmessi da terze parti è essenziale per la prosperità dei servizi internet che facilitano l'espressione e la comunicazione ¹⁴.

Per quanto riguarda il valore degli intermediari *online* per la libertà di espressione, il relatore speciale delle Nazioni Unite Frank La Rue ha evidenziato la semplice logica che porta dalla responsabilità degli intermediari alla censura. Dato che gli intermediari possono ancora essere ritenuti finanziariamente responsabili o in alcuni casi perseguibili penalmente se non rimuovono il contenuto illecito al ricevimento della notifica da parte degli utenti, gli intermediari stessi sono inclini a censurare più di quanto dovrebbe essere fatto per diminuire il rischio ¹⁵.

I quattro relatori speciali delle Nazioni Unite nella loro dichiarazione congiunta del 2011 sulla libertà di espressione e su internet hanno raccomandato che nessuno che si limiti semplicemente a fornire servizi internet di tipo tecnico come ad esempio, fornire l'accesso, i servizi di ricerca, la trasmissione o la memorizzazione di informazioni, dovrebbe essere responsabile per il contenuto generato da altri che viene diffuso utilizzando tali servizi, a condizione che non intervengano specificamente sul contenuto o si rifiutino di obbedire ad un'ingiunzione del tribunale di rimuovere tali contenuti, laddove abbiano la capacità di farlo.

Gli intermediari non dovrebbero essere tenuti a monitorare i contenuti generati dagli utenti e non dovrebbero essere assogget-

¹³ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 2-4.

¹⁴ Si veda: R. MACKINNON, E. HICKOK, A. BAR and H. LIM, *Fostering Freedom Online: The Role of Internet Intermediaries*, United Nations Educational, Scientific and Cultural Organization Report, 2014, disponibile al seguente link: [http://unesdoc.](http://unesdoc.unesco.org/images/0023/002311/231162e.pdf)

unesdoc.unesco.org/images/0023/002311/231162e.pdf, p. 179.

¹⁵ Si veda: F. LA RUE, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Human Rights Council, May 2011, A/HRC/17/27, disponibile al link: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, p. 6-12.

tati a regole extragiudiziali di rimozione dei contenuti visto che le stesse non forniscono una protezione sufficiente per la libertà di espressione ¹⁶.

II.2. *Innovazione.*

Le condizioni stabilite nel contesto normativo sono state identificate come dei fattori importanti che influenzano le attività innovative delle imprese, delle industrie e dell'intera economia ¹⁷.

Mentre molti Paesi dell'Unione Europea, dell'Asia estremo orientale e dell'Oceania lasciano che gli intermediari, in determinate circostanze, siano responsabili per le azioni compiute dai loro utenti, gli Stati Uniti, generalmente, limitano la responsabilità ¹⁸.

Le limitazioni della responsabilità negli Stati Uniti hanno permesso alle aziende della Silicon Valley di preoccuparsi maggiormente di migliorare ed ampliare le proprie funzionalità e di attrarre e trattenere i clienti, piuttosto che controllare i propri servizi con il timore di azioni legali.

Il successo delle imprese di internet statunitensi è dipeso non solo dal fatto che gli imprenditori fossero creativi, predisposti all'innovazione e al rischio di fallimento, ed in grado di ottenere la disponibilità dei capitali necessari, ma anche da normative che hanno limitato i rischi giuridici nella costruzione di piattaforme utilizzabili da milioni di persone ¹⁹.

II.3. *Sorveglianza.*

Poiché gli intermediari raccolgono una grande quantità di dati sugli utenti nel corso della loro attività, i governi possono richie-

¹⁶ Ciò avviene nel caso di molte delle regole di "notice and take down" attualmente applicate. UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on Freedom of Expression and the internet, 2011, disponibile al link: www.osce.org/fom/78309?download=true.

¹⁷ Si veda: A. BUTENKO, P. LAROCHE, *Regulation for Innovativeness or Regulation of Innovation*, TILEC Discussion Paper No. 2015-007, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2584863; K. BLIND, *The Impact of Regulation on Innovation*, Nesta Working Paper No. 12/02, disponibile al link: <https://www.nesta.org>.

uk/sites/default/files/the_impact_of_regulation_on_innovation.pdf.

¹⁸ Si veda il regime di *safe harbor*, differenziato a seconda del ruolo svolto dall'ISP, per ogni violazione del diritto d'autore derivante dai contenuti ospitati e trasmessi dai siti Internet di cui al 17 U.S.C. § 512.

¹⁹ Si veda: R.D. ATKINSON, *Understanding the U.S. National Innovation System*, ITIF, June 2014, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3079822; A. CHANDER, *How law made Silicon Valley*, in *Emory Law Journal*, 2015, Vol. 63, 3. p. 639-94, disponibile al link:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340197, e Id., *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 6.

dere tali dati per scopi di sorveglianza e per altri scopi volti all'applicazione della legge ²⁰.

In particolare i governi autoritari, desiderosi di accedere alle informazioni che gli intermediari *online* potrebbero avere su coloro che divulgano le informazioni nei loro Paesi, hanno cercato di richiedere sempre più spesso agli intermediari *online* di archiviare i dati all'interno degli stessi, facilitando in questo modo l'accesso dei loro servizi di sicurezza ²¹.

In generale, comunque, se le informazioni sono memorizzate in un Paese ma richieste da un altro, le leggi dei due Stati possono entrare in conflitto. Nello specifico, soprattutto le leggi sull'accesso alle informazioni dell'uno possono interferire con le disposizioni di quelle sulla *privacy* dell'altro ²².

Si pensi ad esempio al riguardo al caso Microsoft Ireland, relativo ad e-mail archiviate in un *data center* in Irlanda e quindi non soggette alla legge degli Stati Uniti, e quindi alla questione se un'impresa possa rifiutare legalmente di fornire informazioni alle forze dell'ordine trasferendole in un Paese straniero. Mentre il caso era pendente innanzi alla Corte Suprema a seguito della decisione favorevole a Microsoft da parte della Corte d'Appello del Secondo Circuito, ad aprile 2018 il Congresso ha adottato il Clarifying Lawful Overseas Use of Data Act (CLOUD Act) ²³, che tra le altre previsioni ha modificato lo Stored Communications Act del 1986 ²⁴ per includervi specificamente l'archiviazione dei dati in *cloud* da parte dei provider di comunicazione negli Stati Uniti indipendentemente da dove si trovino i *server*. Pertanto, la Corte Suprema ha emesso un parere *per curiam* affermando che il caso

²⁰ In tal senso rilevano, ad esempio, le modifiche apportate d'urgenza ed in parte reiterate al Patriot Act statunitense, che al fine di fronteggiare il pericolo del terrorismo ha ampliato i poteri investigativi degli organi di polizia federale tanto da permettere a quest'ultimi sia di accedere ad una serie di documenti contenenti le informazioni strettamente personali di ogni singolo cittadino, sia di effettuare intercettazioni e perquisizioni sempre più invasive e lesive dei diritti sanciti nel Primo e Quarto Emendamento. Circa la possibilità che in una democrazia si assista ad una limitazione delle libertà in nome della sicurezza si veda per tutti: S. RODOTÀ, *Libertà personale. Vecchi e nuovi nemici*, in BOVERO M. (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Laterza, 2004, p. 54.

²¹ A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 6-7.

²² Uno studio per il Consiglio d'Europa riferisce che anche in alcuni degli

Stati membri le autorità amministrative, autorità di polizia o pubblici ministeri hanno poteri specifici per ordinare ai fornitori di accesso a internet di bloccare l'accesso senza un provvedimento dell'autorità giudiziaria. È comune che tali ordini richiedano un'azione da parte del fornitore di accesso a internet entro 24 ore e senza alcun preavviso dato al fornitore di contenuti o all'*host* stesso (Swiss Institute of Comparative Law 2015, 3).

²³ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), incluso nel Consolidated Appropriations Act 2018, H.R. 1625, 23 March 2018, disponibile al link: <https://www.congress.gov/bills/115th-congress/house-bill/1625/related-bills?q=%7B%22search%22%3A%5B%22consolidated+appropriations+act%22%5D%7D&r=3>.

²⁴ Stored Communications Act, 18 U.S.C. Chapter 121 §§ 2701—2712, Pub. L. 99-508, 21 October 1986, disponibile al link: <https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf>.

è stato reso privo di fondamento dalla normativa sopravvenuta e rinviando il caso alle corti di grado inferiore per l'archiviazione ²⁵.

II.4. *Le funzioni della regolazione.*

Il motivo principale per intervenire con la regolazione potrebbe avere a che fare con le esternalità, costringendo, ad esempio, gli intermediari *online* a sostenere tutti i costi del servizio piuttosto che trasferirli a terzi, o può essere motivato dal desiderio di garantire determinati livelli di servizi “essenziali” come un ecosistema di informazioni diversificato e con più fonti, oppure può essere finalizzato a bilanciare il potere di contrattazione ineguale ed a proteggere le persone vulnerabili come i bambini.

Tuttavia, la maggior parte degli approcci normativi ricade nella pratica nell'individuazione di tre categorie funzionali che si sovrappongono pur rimanendo analiticamente distinte: abilitazione, uniformazione o vincolo ²⁶.

L'esempio più importante in cui la regolazione svolge la funzione di abilitazione è il quadro normativo statunitense, che è caratterizzato da ampi “*safe harbor*” che limitano drasticamente l'esposizione degli intermediari *online* alla responsabilità.

Questo particolare contesto normativo ha consentito la crescita e lo sviluppo degli intermediari *online* negli Stati Uniti e, di conseguenza, ha promosso le funzioni svolte dagli intermediari stessi ²⁷.

Mentre i motivi storici per l'introduzione di questi limiti alla responsabilità sono piuttosto sfumati ²⁸, i dibattiti politici attuali fanno riferimento a questa funzione abilitante connettendola in gran parte o ai benefici economici, come gli incentivi per innovare senza il timore di incorrere nella responsabilità, o al contesto dei diritti fondamentali, ad esempio per eliminare gli ostacoli al

²⁵ Supreme Court, United States v. Microsoft Corporation, 17 April 2018, No. 17-2, 584 U.S. _ 2018, disponibile al link: https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf.

²⁶ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit. p. 10.

²⁷ Oltre alla suddetta dottrina, si veda: N. BRAMBLE, *Safe Harbors and the National Information Infrastructure*, in *Hastings Law Journal*, Vol. 64, No. 2, 2013, p. 325 ss., disponibile al link: <http://www.hastingslaw>

journal.org/wp-content/uploads/2014/04/Bramble-64.2.pdf.

²⁸ Nel caso dello U.S. Communications Decency Act, ad esempio, il legislatore voleva abilitare l'autoregolamentazione dei contenuti da parte degli intermediari *online* senza esporli alla responsabilità. Si veda: R. CANNON, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, in *Federal Communications Law Journal*, Vol. 49, No. 1, 1996, p. 51 ss., disponibile al link: <http://www.cybertelecom.org/cda/cannon2.htm>.

legittimo esercizio dei diritti connessi alla minaccia di sanzioni giuridiche ²⁹.

Un'altra funzione che la regolazione della responsabilità degli intermediari *online* può svolgere è quella di garantire l'uniformità nel trattamento dei vari casi.

Tracce di tale funzione possono essere riscontrate in diversi Paesi che utilizzano sistemi di *notice and take down* in cui il modello di *governance* si rivolge agli intermediari *online* per raggiungere un equilibrio tra gli interessi delle diverse parti, ad esempio tra le pretese dei titolari di *copyright* e gli utenti nell'ambito delle questioni relative al diritto d'autore.

Il cosiddetto diritto all'oblio, introdotto dalla decisione della Corte di Giustizia dell'Unione Europea sul caso Costeja ³⁰ e successivamente previsto nel Regolamento generale sulla protezione dei dati ³¹ all'art. 17, potrebbe essere visto come un'altra manifestazione di tale approccio, volto a garantire un "giusto equilibrio" tra gli interessi legittimi degli utenti di internet, potenzialmente interessati ad avere accesso alle informazioni e i diritti fondamentali del titolare dei dati ³².

In terzo luogo, la regolazione svolge tipicamente una funzione vincolante prescrivendo agli intermediari *online* di intraprendere azioni specifiche o di attuare determinate misure. Anche i regimi che utilizzano la regolazione quale strumento finalizzato a garantire l'uniformità spesso producono l'effetto di determinare dei

²⁹ Si veda: K. BANKSTON, D. SOHN, A. McDIARMID, *Shielding the Messengers: Protecting Platforms for Expression and Innovation*, Center For Democracy and Technology, December 2012, p. 1 ss., disponibile al link: <https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf>; ma cfr. anche: W. SELTZER, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, in *Harvard Journal of Law & Technology*, Vol. 24, No. 1, 2010, p. 171, disponibile al link: <http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf>.

³⁰ Corte di Giustizia dell'Unione Europea, decisione 13 maggio 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, case C-131/12, disponibile al link: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

³¹ Regolamento (EU) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei

dati) che entrerà in vigore il 25 maggio 2018, disponibile al link: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

³² Sulle numerose questioni problematiche sollevate dalla decisione, si vedano tra gli altri: Article 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12, 26 November 2014, disponibile al link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf; A. FOMPEROSA RIVERO, *Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, e Extraterritoriality*, *Stanford-Vienna European Union Law Working Paper* No. 19, 2017, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916608; S. KULK, F.J. ZUIDERVEEN BORGESIU, *Google Spain v. González: Did the Court Forget About Freedom of Expression?*, in *European Journal of Risk Regulation*, 2014, Vol. 5, No. 3, p. 389 ss.

vincoli, come nel caso dei regimi di *notice and take down* in cui gli intermediari *online* devono adempiere a determinati obblighi al fine di poter beneficiare della protezione concessa dal “*safe harbor*”³³.

Ma la ricerca rivela anche delle situazioni in cui gli effetti delle prescrizioni sono più specifici o mirati. Ad esempio, il regime delle licenze in Vietnam impone dei vincoli rigidi in base ai quali devono operare gli intermediari *online*. In Thailandia, la legge pone direttamente a carico degli intermediari stessi la responsabilità circa i contenuti al fine di garantire l'ordine pubblico ed in particolare per preservare l'onore del re o per consentire il controllo sul flusso di informazioni attraverso la censura e la sorveglianza³⁴.

III. APPROCCI REGOLATORI.

I diversi sistemi per regolare la responsabilità degli intermediari possono essere suddivisi in due grandi gruppi. Innanzitutto, esistono sistemi che si rivolgono esplicitamente agli intermediari e dove c'è un meccanismo di governance appositamente progettato per occuparsi di essi. In secondo luogo, esistono sistemi in cui vengono applicate regole generali agli intermediari.

Gli Stati Uniti possono essere utilizzati come esempio di un sistema nel quale vi è un quadro normativo specifico per gli intermediari. La sezione n. 230 del Communications Decency Act e la Sezione n. 512 del Digital Millennium Copyright Act sono gli elementi cardine della regolazione e costituiscono un regime di “*safe harbor*” per gli intermediari *online*.

Lo stesso vale, almeno in linea di principio, nell'Unione europea, dove la Direttiva 2000/31/CE sul commercio elettronico³⁵ prevede specifiche esenzioni di responsabilità per gli intermediari *online*³⁶. Tuttavia, a causa della portata limitata dell'esenzione — ad esempio, le ingiunzioni non sono contemplate dal regime — e di un certo grado di incertezza su come applicare le esenzioni,

³³ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 10-11.

³⁴ Si veda: P. RAMASOOTA, *Online Intermediary Liability in Thailand, The Global Network of Internet & Society Research Centers - Online Intermediaries Case Studies Series*, 2015, p. 4, disponibile al link: https://publixphere.net/i/noc/page/OI_Case_Study_internet_Intermediary_Liability_in_Thailand, p. 4, e le ulteriori informazioni riportate *infra*.

³⁵ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno

del 2000 su taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (“Direttiva sul commercio elettronico”), in OJ L 178, 17.7.2000, disponibile al link: <http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32000L0031>.

³⁶ In merito all'assenza di un obbligo di sorveglianza a carico degli ISP, si veda: G. PINO, *Assenza di un obbligo generale di sorveglianza a carico degli Internet Service Providers sui contenuti immessi da terzi in rete*, in *Danno e responsabilità*, 2004, p. 832.

l'armonizzazione europea non ha potuto prevenire l'emergere di un sistema piuttosto frammentato in materia di responsabilità degli intermediari ³⁷.

In Asia, mentre in Vietnam — e in una certa misura in Thailandia e India — gli intermediari affrontano principalmente richieste di rimozione dei contenuti per motivi di interesse pubblico (in senso lato, compresa la tutela dell'onore del re in Thailandia), nella maggior parte degli altri Paesi sono le divergenze tra gli utenti ad alimentare la maggior parte dei conflitti.

Il primo modello potrebbe derivare da un approccio più interventista di alcuni governi; tuttavia, potrebbe anche basarsi sulla diversa rilevanza che hanno i diritti personali e sulle diverse culture dei denunciati nei paesi esaminati. È interessante notare che le rivendicazioni basate sul diritto d'autore sono trattate con un sistema separato di responsabilità praticamente in tutti i paesi che rientrano nella presente ricerca.

Un'altra distinzione importante consiste nel comprendere se un regime di responsabilità fornisca un *safe harbor* per gli intermediari o meno. La sezione 512 del Digital Millennium Copyright Act negli Stati Uniti è probabilmente l'esempio più importante di una clausola che fornisce un tale "approdo sicuro". La regola di base stabilita è che se non si curano i contenuti, non vi è la responsabilità. Pertanto, in base al DMCA, il punto fondamentale è il modo in cui i *provider* trattano i contenuti ³⁸.

Vi sono alcune forme efficaci di protezione dalla responsabilità per gli intermediari anche in Giappone, Australia, Malesia, Singapore e Thailandia, ed un regime di *safe harbor* esiste altresì in una certa misura — in quanto limitato in termini reali o di fatto non efficace — in Cina, India e Vietnam ³⁹.

La suddetta clausola di *safe harbor* contenuta nella Direttiva sul commercio elettronico dell'Unione Europea dimostra che non tutti i porti sono ugualmente al riparo dal forte vento delle rivendicazioni dei terzi ⁴⁰. La Direttiva definisce differenti tipo-

³⁷ Si veda: C. ANGELOPOULOS, *Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe*, in *Intellectual Property Quarterly*, 2013, No. 3, p. 253 ss., disponibile al link: <http://papers.ssrn.com/abstract=2360997>.

³⁸ Si veda la sentenza *Viacom Int'l v. YouTube, Inc.*, 676 F.3d 19 (2nd Cir. 2012) che, riguardo al requisito della conoscenza, ha ribadito come la responsabilità di un ISP presuppone in ogni caso la conoscenza di specifici atti di violazione del diritto d'autore. Si veda anche il provvedimento *Capitol Records et al. v. Vimeo*, 826 F.3d 78 (2nd Cir. 2016), laddove si è affermato che

non fosse sufficiente a configurare in capo all'ISP una "*red flag knowledge*" la circostanza che alcuni impiegati di un provider avessero visionato video caricati dagli utenti e contenenti canzoni riconoscibili come protette dal diritto d'autore, spingendosi anche ad interagire con gli utenti postando commenti e "like" ai video in questione.

³⁹ Si veda *infra* al paragrafo III.1.

⁴⁰ Per una panoramica generale sulle predette questioni, si veda: L. BUGIOLACCHI, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet Provider. Una sintesi di diritto comparato*, in *Diritto dell'informazione e dell'informatica*, 2000, p. 836.

logie di intermediari a seconda del ruolo svolto e l'inquadramento in uno di questi ruoli comporta generalmente l'esonazione della responsabilità del fornitore. Tuttavia, nonostante l'obiettivo principale del provvedimento fosse quello di creare un approdo sicuro, in particolare per promuovere l'innovazione in Europa, la Direttiva ha di fatto fornito un regime di *safe harbor* solo in un numero limitato di casi ⁴¹.

Un'altra caratteristica significativa di qualsiasi regime di governo anche degli intermediari è se esso stabilisca o meno un meccanismo di *notice and take down* dei contenuti e laddove sussista tale procedura se la stessa costituisca un presupposto facoltativo per ottenere la protezione del *safe harbor* o un requisito obbligatorio di responsabilità per cui la mancata risposta ad un avviso legale fa scattare immediatamente la responsabilità. Può aversi un regime esplicito, come in India ⁴², o una situazione come quella europea, dove la decisione della Corte di Giustizia sul caso Costeja si è tradotta di fatto in una procedura di notifica e rimozione ⁴³.

III.1. *I multiformi approcci dei Paesi dell'Asia estremo orientale e dell'Oceania (da una prospettiva occidentale).*

Nel procedere ad un'analisi dei multiformi approcci dei Paesi dell'Asia estremo orientale e dell'Oceania alla questione della responsabilità degli intermediari *online*, in primo luogo occorre rilevare come, nella misura in cui si possa trovare una qualche comunanza, vi siano Paesi in cui esistono forme efficaci di protezione dalla responsabilità degli intermediari.

In Giappone, le protezioni attuali mirano a sostenere l'importanza della libertà di espressione, anche se vi sono delle incertezze rilevanti connesse alle recenti sfide legate al filtraggio per età e alla pressione politica per alzare il livello di responsabilità.

Nel 2001 la Dieta giapponese ha approvato la Legge relativa ai limiti di responsabilità per i danni dei fornitori di determinati servizi di telecomunicazioni ⁴⁴, in base alla quale un fornitore di servizi di telecomunicazione non può essere ritenuto responsabile

⁴¹ Per l'effetto della clausola di *safe harbor* e dei suoi limiti a livello europeo, si vedano in particolare le decisioni della CGUE del 12 luglio 2011, sul caso C-324/09, L'Oréal v eBay, del 24 novembre 2011 sul caso C-70/10, Scarlet v SABAM, e del 16 febbraio 2012 sul caso C-360/10, SABAM v Netlog.

⁴² Si veda: See: C. ARUN, S. SINGH, *Online Intermediaries in India, The Global Network of internet & Society Research Centers - Online Intermediaries Case Studies Series*, 2015, p. 21, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566952.

⁴³ Secondo alcuni in assenza di una base giuridica chiara. Si veda ad esempio: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 5-6.

⁴⁴ Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders, No. 137 of 2001, disponibile al link: www.soumu.go.jp/papers.ssrn.com/sol3/papers.cfm?abstract_id=2566952.

per le azioni compiute dai suoi utenti a meno che non sappia, o vi siano ragionevoli motivi che indicano che il fornitore di servizi possa sapere, che la violazione dei diritti altrui sia causata dalla distribuzione di informazioni tramite tali specifiche telecomunicazioni ⁴⁵.

Come per l'approccio europeo, la Legge si applica a tutte le attività di intermediazione, sia che coinvolgano i diritti d'autore, i marchi o gli illeciti civili, imponendo non solo un effettivo approccio di *notice and take down*, ma anche il più vago presupposto dei "ragionevoli motivi" che il fornitore "possa sapere".

Piuttosto che il regime di *safe harbor* relativamente chiaro del DMCA, la Legge giapponese ha rimosso qualsiasi protezione ove il *provider* sappia o avrebbe dovuto sapere dell'infrazione verificatasi attraverso il suo servizio, uno standard molto più incerto, soprattutto considerando la probabilità che alcuni utenti commettano le violazioni mediante qualsiasi tipo di servizio *web 2.0* ⁴⁶.

In particolare, la suddetta Legge stabilisce che quando un diritto di terzi viene violato dalla distribuzione di informazioni tramite specifiche telecomunicazioni, il fornitore di servizi non è responsabile di eventuali perdite dovute a tale violazione, a meno che non sia tecnicamente possibile adottare delle misure per impedire che tali informazioni siano trasmesse a persone non specificate e tale tipologia di violazione rientri in una delle ipotesi previste ⁴⁷.

Attualmente, il Ministero degli affari interni e delle comunicazioni, che è responsabile della legge, ha avviato una discussione volta ad emendare la medesima legge al fine di soddisfare i più recenti sviluppi tecnologici.

L'*internet Environment Development Law* ⁴⁸ prevede che i *provider* mobili forniscano un servizio per filtrare il contenuto dannoso per i giovani nei casi in cui la controparte del contratto è un giovane o su richiesta di una persona che riceve la fornitura del servizio internet ⁴⁹.

Attualmente tali disposizioni sono soggette a pressioni politiche perché i governi ed i gruppi rilevanti come le associazioni di categoria dei *provider* ritengono che la *ratio* del filtraggio non sia abbastanza elevata e possa essere un focolaio per i crimini *online* che coinvolgono i minori.

La Malesia allo stato attuale non fornisce alcuna protezione

main_sosiki/joho_tsusin/ eng/Resources/laws/ Compensation-Law.pdf.

⁴⁵ Law No. 137 of 2001, cit., art. 3.

⁴⁶ Cfr.: A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 5.

⁴⁷ Si veda la sezione 3, articolo 3.

⁴⁸ Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People, Act No. 79 of 2008, disponibile al link: <http://www8.cao.go.jp/youth/youth-harm/pdf/neteng.pdf>.

⁴⁹ Si vedano gli articoli 17-18.

circa la responsabilità degli intermediari, mentre esiste un regime di protezione rilevante per il *copyright*.

Il Communications and Multimedia Act del 1998 contiene il divieto di fornire contenuti offensivi e di utilizzare impropriamente le strutture della rete o i servizi di rete, ecc.⁵⁰. L'autorità di regolamentazione fa affidamento su tali disposizioni e sui reati previsti dal codice penale per richiedere la rimozione dei contenuti (in genere di quelli offensivi per questioni religiose). Nel 2016 il governo malese ha tentato di far passare le modifiche al CMA per imporre una maggiore responsabilità a carico delle piattaforme, ma tale progetto è stato abbandonato a fronte delle reazioni industriali e locali.

La legge sul *copyright*⁵¹, invece, fornisce limiti dettagliati delle responsabilità degli ISP, simili a quelli del DMCA, che sembrano funzionare bene⁵².

Singapore attualmente non fornisce un regime di protezione completa dalla responsabilità degli intermediari ma prevede alcune tutele specifiche.

L'Internet Code of Practice elaborato ai sensi della sezione 6(1) del Broadcasting Act⁵³ prevede che un fornitore di contenuti internet neghi l'accesso al materiale che viene considerato dall'Autorità come materiale vietato laddove ciò sia richiesto dall'Autorità⁵⁴. Pertanto, attualmente non esiste, secondo quanto stabilito dal Broadcasting Act e dalla legislazione sussidiaria, alcuna protezione circa la responsabilità degli intermediari. Inoltre, la legge è attualmente in fase di revisione ed appare possibile che vengano stabiliti dei requisiti come delle licenze per i servizi su richiesta e per la distribuzione di app.

Il Protection from Harassment Act prevede la possibilità di presentare una domanda al tribunale distrettuale per ottenere un ordine di protezione che dichiari che nessuno deve pubblicare o continuare a pubblicare la comunicazione incriminata o la falsa dichiarazione di fatto⁵⁵.

Tuttavia, qualsiasi soggetto diverso dal rispondente o dal destinatario di tale provvedimento non sarà ritenuto responsabile

⁵⁰ Si veda: Act No. 588/1998, sezioni 211 e 233, disponibile al *link*: https://www.unode.org/res/cld/document/mys/communications_and_multimedia_act_html/Malaysia_Communications_and_Multimedia_Act_1998.pdf.

⁵¹ Si veda: Copyright Act of 1987 (Act 322) e Copyright Amendments Act of 1990 (Act A775), e 2012 (Act 1420), disponibili al *link*: <http://cyberlaw.stanford.edu/page/wilmap-malaysia>.

⁵² Si vedano gli articoli 43C-43H.

⁵³ Broadcasting Act (Chapter 28), Revised Edition 2012, 31 August 2012, dispo-

nibile al *link*: <https://sso.agc.gov.sg/Act/BA1994>.

⁵⁴ Si veda: Info-communications Media Development Authority, Internet Code of Practice, October 2016, disponibile al *link*: <https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/acts-codes/19-policiesandcontentguidelinesinternetinternecodeofpractice.pdf?la=en>, par. 3.

⁵⁵ A meno che quella persona non pubblichi tale notifica come la District Court ritiene necessario per attirare l'attenzione sulla falsità e sui fatti veri. Cfr.: Protection

civilmente sulla base di una legge o di un contratto, per qualsiasi atto compiuto al fine di far rispettare tale ordine.

Nel Copyright Act, come nel caso della Malesia, esistono meccanismi di protezione dalla responsabilità per gli intermediari della stessa tipologia di quelli contenuti nel DMCA, con l'esenzione per i fornitori di servizi di rete dalla responsabilità per la rimozione di copie ecc. dalle reti⁵⁶. Attualmente è in corso una revisione della legislazione vigente ed il governo sta introducendo ulteriori limitazioni ed eccezioni per promuovere l'uso del *copyright* per l'innovazione.

Infine, secondo quanto stabilito dall'Administration of Justice Act, da un lato, il Procuratore generale, se ritiene che sia nell'interesse pubblico, con il permesso dell'Alta Corte, può ordinare all'editore di astenersi o dal cessare di pubblicare un contenuto. Dall'altro, nessuna responsabilità penale o civile è configurata se ciò che viene fatto o non viene fatto avviene con ragionevole cura e in buona fede nel conformarsi a tale indicazione⁵⁷.

In *Thailandia* sono in vigore delle protezioni che si basano sul meccanismo della notifica e conseguente rimozione, anche se vi sono delle criticità connesse al rischio della censura per conformarsi alle richieste del governo.

La rivisitata legge sui reati informatici è più chiara della precedente legge per quanto riguarda la differenziazione delle varie tipologie di intermediari, la proporzionalità delle sanzioni per il reato commesso, e la tendenza delle istituzioni a richiedere la cooperazione degli intermediari nel monitoraggio dei contenuti internet⁵⁸.

Qualsiasi fornitore di servizi *online* che collabora, acconsente o è connivente in relazione a determinati reati, ai sensi della legge, così come modificata, dovrà affrontare sanzioni penali, laddove, ad esempio, fornisca in maniera disonesta o ingannevole informazioni distorte o dati falsificati circa il proprio sistema informatico.

Esiste una specifica esenzione di responsabilità circa i contenuti per i fornitori di servizi *online* che si basa sulla procedura di notifica e rimozione. Il Ministro dell'economia e della società digitale può emettere un annuncio nel quale determina le procedure per l'adozione di un avviso di cessazione della circolazione dei dati e di rimozione dei dati dal sistema informatico. Un

from Harassment Act (Chapter 256A), Revised Edition 2015, 31 May 2015, disponibile al *link*: <https://sso.agc.gov.sg/Act/PHA2014>, artt. 12 e 15.

⁵⁶ Si veda: Copyright Act (Chapter 63), Revised Edition 2006, 31 January 2006, disponibile al *link*: <https://sso.agc.gov.sg/Act/CA1987>, art. 193.

⁵⁷ Cfr.: Administration of Justice (Protection) Act 2016, 22 September 2016, disponibile al *link*: <https://sso.agc.gov.sg/Act/AJPA2016>, art. 13.

⁵⁸ Si veda: P. RAMASOOTA, *Online Intermediary Liability in Thailand*, cit., par. II-IV.

fornitore di servizi sarà esentato da sanzioni penali se è in grado di dimostrare di avere rispettato tale avviso ⁵⁹.

Secondo alcuni commentatori, tuttavia, sebbene ciò possa sembrare che allevi la pressione a carico degli intermediari, far ricadere su di loro l'onere della prova potrebbe comportare una maggiore censura, soprattutto laddove gli intermediari debbano rimuovere i contenuti su richiesta del governo o censurino preventivamente se stessi ed i loro utenti per evitare lo scrutinio ⁶⁰.

Nel caso in cui circolino dei dati informatici con caratteristiche contrarie alla legge, alla pace e all'ordine pubblico o al buon costume, il Ministro può autorizzare un'autorità competente a presentare domanda e a produrre prove dinanzi al tribunale competente per ottenere la cessazione della circolazione di tali dati informatici o la cancellazione dei dati dai sistemi informatici ⁶¹.

Per quanto riguarda i contenuti, la monarchia thailandese presta un'attenzione specifica per quelli che comportano lesa maestà, che può determinare una pressione politica a carico degli intermediari. Mentre fino ad ora vi è stato un solo caso perseguito in associazione con la controversa disciplina sulla lesa maestà, a seguito di essa si è registrato un evidente “*chilling effect*” nei confronti degli operatori di internet ⁶².

In secondo luogo, vi sono dei Paesi in cui le protezioni attualmente esistenti sono limitate in termini reali o di fatto non efficaci.

In Cina, nonostante vi siano delle disposizioni che proteggono gli intermediari fino alla “scoperta”, vi sono previsioni normative, come ad esempio “dovrebbe essere a conoscenza dell'infrazione”, che sono ben diversi rispetto al solo “essere a conoscenza”, o di responsabilità per “misure precauzionali volte a fornire supporto tecnologico ai dipartimenti governativi”, e di “riesame delle in-

⁵⁹ Si veda: Computer Crimes Act (No. 2) 2017, 23 January 2017, sezione 15, disponibile al link: [https://en.wikisource.org/wiki/Translation:Computer_Crimes_Act_\(No._2\)_2017](https://en.wikisource.org/wiki/Translation:Computer_Crimes_Act_(No._2)_2017).

⁶⁰ Si veda: D. O'BRIEN, G. GEBHART, *The Amended Computer Crime Act and the State of internet Freedoms in Thailand*, December 2016, disponibile al link: <https://www.eff.org/deeplinks/2016/12/amended-computer-crime-act-and-state-internet-freedoms-thailand>.

⁶¹ Computer Crimes Act (No. 2) 2017, cit., sezione 20.2. Ciò riguarda solo i fornitori di rete e i fornitori di accesso (e non i fornitori di contenuti), che sono licenziatari nell'ambito del sistema della National Bro-

adcasting and Telecommunications Commission e sono quindi identificabili dall'autorità. Secondo la sezione 20.3, quindi, il Ministro ha l'autorità di nominare un comitato di verifica dei dati informatici, che può incaricare un funzionario di richiedere che la corte ordini la cessazione della circolazione dei dati informatici, o la cancellazione di dati informatici, in caso di diffusione di dati informatici che costituiscono un reato ai sensi della legge, incidano sulla sicurezza della Thailandia, o confliggano con la pace, l'ordine pubblico o il buon costume.

⁶² Ossia l'inibizione o lo scoraggiamento dell'esercizio legittimo di diritti a causa della minaccia di sanzioni giuridiche. Cfr. ancora: P. RAMASOOT, *Online Intermediary Liability in Thailand*, cit., par. III.

formazioni”, e stanno aumentando le pressioni per lo svolgimento di una verifica per garantire che il contenuto sia “sicuro”⁶³.

Il Regulation on Telecommunications of the People’s Republic of China del 2000 ha stabilito all’articolo 56 che nessuna organizzazione o individuo possa utilizzare reti di telecomunicazione per produrre, riprodurre, diffondere o trasmettere qualsiasi informazione che contenga dei contenuti che: (i) siano in contrasto con i principi di base così come sanciti nella Costituzione; (ii) mettano a repentaglio la sicurezza della nazione, divulgando segreti di stato, sovvertendo il regime nazionale o mettendo a repentaglio l’integrità dell’unità della nazione; (iii) danneggino l’onore o gli interessi della nazione; (iv) incitino all’odio contro i popoli, al razzismo o alla distruzione della solidarietà dei popoli; (v) interrompano le politiche nazionali sulla religione, diffondano culti del male e superstizioni feudali; (vi) diffondano pettegolezzi, disturbino l’ordine sociale o interrompano la stabilità sociale; (vii) diffondano oscenità, pornografia, gioco d’azzardo, violenza, omicidio, terrore o favoreggiamento di un reato; (viii) insultino o diffamino i terzi, violando i diritti e gli interessi legali dei terzi; e (ix) contengano qualsiasi altro tipo di contenuto proibito dalla legge o dalle norme amministrative.

La National People’s Congress Standing Committee “Decision Regarding Strengthening Network Information Protection” del 2012 ha specificato all’art. 5 che i fornitori di servizi di rete rafforzano la gestione delle informazioni che vengono loro rilasciate dagli utenti e, alla scoperta della pubblicazione o della trasmissione di informazioni vietate dalla legge o dai regolamenti, interrompano immediatamente la trasmissione di tali informazioni disponendo l’adozione di determinate misure, come la rimozione dei contenuti, conservino i dati rilevanti e segnalino il tutto all’agenzia competente.

Per quanto riguarda le informazioni con contenuti terroristici o estremisti, la China’s Counter-Terrorism Law del 2015 ha stabilito all’articolo 19 che, laddove un simile contenuto venga scoperto, la sua diffusione deve essere immediatamente interrotta, i documenti pertinenti devono essere salvati e le informazioni relative cancellate, e deve essere redatto un rapporto per gli organi di pubblica sicurezza o per i dipartimenti competenti.

⁶³ Si veda: D. FRIEDMANN, *Oscillating from Safe Harbor to Liability: China’s IP Regulation and Omniscient Intermediaries*, April 2017, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2969807; W. LI, H.K. HIE, *Technology Development and Legislation Progress: Third Party Liabilities of Internet Service Providers in China Tort Law*, in *Journal of*

Intellectual Property Rights, 2013, Vol. 13, p. 133 ss.; Q. TAO, *The knowledge standard for the Internet Intermediary Liability in China*, in *International Journal of Law and Information Technology*, 2012, Vol. 20, No. 1, p. 1 ss.; D. SENG, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, cit., p. 19 ss.

Con il rafforzamento sempre maggiore del controllo su internet, il governo richiede agli operatori di internet di assumersi maggiori responsabilità per garantire che la rete sia “sicura” fermando i contenuti “dannosi”.

Nel novembre 2012 la Corte suprema ha adottato, come supplemento della legge sul *copyright*, specificamente per le violazioni commesse su internet, delle previsioni in merito a questioni problematiche riguardanti l'applicazione della legge nei casi ricorrenti di controversie civili in materia di violazione del diritto di comunicazione tramite reti d'informazione ⁶⁴.

In generale, tali norme forniscono un *safe harbor* limitato per i fornitori di servizi internet ⁶⁵, ma a causa di una formulazione vaga e all'incertezza nel giudicare se gli ISP abbiano o meno colpa, in considerazione, altresì, delle altre leggi, sembra prevedibile che venga richiesto agli ISP di assumersi maggiori responsabilità circa i contenuti prodotti dagli utenti, le attività di gestione o di verifica preventiva.

Più recentemente, le Regulations on Internet Information Search Services, approvate a giugno 2016 come uno degli elementi della stretta governativa sul controllo della rete internet, hanno richiesto agli ISP di assumersi maggiori responsabilità in materia di censura dei contenuti e di controllo e gestione delle informazioni degli utenti o dei clienti.

Infine, la bozza di E-commerce law, ancora in discussione, definisce delle regole in materia di proprietà intellettuale ed aggrava la responsabilità degli ISP, stabilendo che le imprese del commercio elettronico debbano proteggere i diritti di proprietà intellettuale. Se una piattaforma di commercio elettronico terza è a conoscenza del fatto che un commerciante ha violato i diritti di proprietà intellettuale, tale piattaforma deve adottare le misure necessarie — quali la cancellazione, la protezione il “*delinking*” o la cessazione di transazioni o servizi — in conformità con la legge ⁶⁶.

In India, gli intermediari *online* sono assoggettati ad un quadro normativo complesso, che prevede la possibilità di incorrere nella responsabilità civile e penale. Le disposizioni più rilevanti che

⁶⁴ Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Hearing of Cases regarding Civil Disputes over Infringement of the Right of Communication via Information Networks, December 2012, disponibili al *link*: <http://en.pkulaw.cn/display.aspx?cgid=191740&lib=law>.

⁶⁵ Si vedano gli articoli 5-8, secondo cui, in particolare, se un fornitore di servizi di rete non ha adottato misure necessarie quali la cancellazione, il blocco e la discon-

nessione quando viene chiaramente a conoscenza o deve essere a conoscenza dell'infrazione, la People's Court giudica che il fornitore di servizi di rete ha collaborato nell'infrazione e, in base alla colpa del fornitore di servizi di rete, deve anche determinare se è soggetto a favoreggiamento e responsabilità civile.

⁶⁶ Si vedano gli articoli 53-54 della seconda bozza della E-commerce law, pubblicata a novembre 2017.

regolano gli intermediari possono essere riscontrate nell'Information Technology Act del 2000 e nel Copyright Act del 1957. Tuttavia, vi sono circostanze in cui trova applicazione la legislazione generale, come il codice penale indiano del 1860, lo Scheduled Caste and Scheduled Tribe (Prevention of Atrocities) Act del 1989, o il Protection of Children from Sexual Offences Act del 2012 o la legge sui *torts*. Se un intermediario *online* non ha diritto all'immunità dalla responsabilità, così come offerta dall'IT Act, allora potrebbe incorrere in sanzioni civili o penali per reati quali la diffamazione, l'oscenità o la violazione del *copyright* ⁶⁷.

È in corso un dibattito politico sul dare al governo più margine di manovra per eliminare i contenuti inappropriati o offensivi. Il sistema giudiziario sta anche testando i limiti per quanto riguarda la rimozione del contenuto.

L'Information Technology Act del 2000, sezione 79, prevede l'esonero dalla responsabilità dell'intermediario in determinati casi, per eventuali informazioni, dati o collegamenti di terze parti resi disponibili o ospitati da esso.

Le garanzie di esonero dalla responsabilità sono previste fino all'"effettiva notifica", che come stabilito dalla Corte significa fino a quando ne si ha effettiva conoscenza mediante un'ingiunzione del tribunale o in caso di notifica da parte di un organo governativo competente. Tuttavia i tribunali — compresa la Corte Suprema — nei loro provvedimenti interpretativi, stanno sempre più spingendo per una verifica proattiva ad esempio sulle questioni attinenti alla selezione prenatale dei bambini in base al sesso o nel caso di stupro.

Nel Copyright Act del 1999 è stato inserito un *safe harbor* nella sezione 52, nella quale si afferma che "la conservazione temporanea o incidentale di un'opera o la prestazione di un servizio puramente tecnico di trasmissione o la comunicazione elettronica al pubblico" non costituiscono violazioni del *copyright*; e che "la conservazione temporanea o incidentale di un'opera o la prestazione di un servizio allo scopo di fornire collegamenti, accesso o integrazione elettronica, laddove tali collegamenti, l'accesso o l'integrazione non siano stati espressamente vietati dal titolare del diritto" non costituiscono violazioni, a meno che l'intermediario non abbia dei "motivi ragionevoli" per ritenere che tale archiviazione sia una copia illecita ⁶⁸.

⁶⁷ Si veda: C. ARUN, S. SINGH, *Online Intermediaries in India*, cit., par. II. Gli intermediari *online*, invece, non sono soggetti al regime nazionale di licenze per i fornitori di servizi internet, dato che molti di loro non hanno uffici in India e sono quindi fuori dalla giurisdizione fisica entro cui il governo indiano è in grado di attuare

le sue leggi. Pertanto, sebbene gli ISP siano soggetti a diversi obblighi attraverso le loro licenze, gli intermediari *online* internazionali rimangono liberi da questi vincoli.

⁶⁸ Tuttavia, il problema qui è l'interpretazione di ciò che equivale a ragionevoli motivi per credere che un intermediario stia memorizzando contenuti in violazione; la

I procedimenti di notifica e di rimozione avviati ai sensi dell'Information Technology Act e del Copyright Act sono controversi, soprattutto in termini di limitazione della libertà di espressione. Altrettanto problematiche appaiono le numerose petizioni attualmente all'esame della Corte Suprema indiana. Mentre alcune di queste petizioni cercano di eliminare il procedimento di notifica e di rimozione istituito dall'IT Act perché tale meccanismo viola i diritti costituzionali, altre cercano di ripristinare un regime di responsabilità oggettiva per i contenuti osceni *online*.

La tendenza sembra essere verso una verifica proattiva commissionata dalla corte, specialmente laddove i contenuti abbiano un rilevante impatto sociale. Recentemente, la Corte Suprema ha imposto che gli intermediari debbano esaminare gli annunci e/o i contenuti relativi alla selezione del sesso prenatale (un processo che è illegale in India a causa del prevalente infanticidio femminile). La Corte è impegnata anche nei procedimenti relativi ai caricamenti di video sugli stupri e nell'elaborazione di soluzioni tecniche per la verifica proattiva prima del caricamento.

Sul fronte legislativo, il governo sta meditando una revisione dell'Information Technology Act, del 2000, con l'obiettivo di poter esercitare un maggiore controllo sulla rimozione dei contenuti. Ciò in seguito all'eliminazione, da parte della Corte Suprema, della precedente sezione 66, che era utilizzata per gli addebiti ai cittadini che avessero caricato contenuti "offensivi". In assenza di questa disposizione, il governo sta valutando una serie di modalità attraverso le quali possa assicurarsi di avere un maggiore controllo sul contenuto che possa provocare una comune disarmonia.

In Vietnam, secondo la legge sulla stampa adottata nel 1989 e modificata nel 2017, le agenzie di stampa in senso lato, compresi i fornitori di servizi di *social networking online* e i siti *web* di notizie generali, devono ottenere una licenza dal governo per poter operare in tal senso⁶⁹. Tuttavia, dal 2001, il Vietnam ha esplicitamente permesso l'utilizzo dei servizi di applicazioni internet forniti sia dagli operatori nazionali che da quelli esteri che

magistratura ha, in passato, visto l'inserimento di annunci generati dall'algoritmo come un'indicazione della conoscenza dell'infrazione; cfr.: Delhi High Court, *Super Cassettes Industries Ltd v. Myspace Inc*, 29 July 2011, M.I.P.R. 2011 (2) 303, disponibile al *link*: <https://indiankanon.org/doc/216257>. Si veda: C. ARUN, S. SINGH, *Online Intermediaries in India*, cit., par. II.C.; A. Padmanabhan, *Give Me My Space and Take Down His*, I.J.L.T., 2013, Vol. 9, p. 15-16, disponibile al *link*: <http://www.ijlt.in/archive/volume9/Ananth%20Padmanabhan.pdf>.

⁶⁹ Law No. 103/2016/QH13 of April 5, 2016 on the Press, articoli 3-6, disponibile al *link*: http://www.wipo.int/wipolex/en/text.jsp?file_id=447052, e Decree No. 51/2002/ND-CP of April 26, 2002, detailing the implementation of the Press Law and the law amending and supplementing a number of articles of the Press Law, disponibile al *link*: <http://hethongphapluatvietnam.com/decree-no-51-2002-nd-cp-of-april-26-2002-detailing-the-implementation-of-the-press-law-and-the-law-amending-and-supplementing-a-number-of-articles-of-the-press-law.html>.

non hanno alcuna presenza locale in Vietnam⁷⁰. Pertanto, il governo ha richiesto l'utilizzo di meccanismi finalizzati a controllare le attività *online* che avvengono non solo tramite gli intermediari *online* con licenza locale, ma anche tramite gli intermediari *online* stranieri⁷¹.

L'Information Technology Act del 2006 attribuisce agli intermediari *online* la responsabilità per aver contribuito attivamente alla produzione e alla distribuzione dei contenuti illegali, laddove generino, curino o modifichino tali contenuti, mentre esenta esplicitamente gli intermediari dalla responsabilità in determinate circostanze. Gli intermediari *online*, su richiesta delle competenti autorità, devono adottare le misure necessarie per bloccare l'accesso o per rimuovere le informazioni illegali. Tuttavia, la legge prevede anche che i fornitori di servizi IT non siano responsabili per il monitoraggio delle informazioni digitali prodotte da terze parti o per indagare sugli atti illeciti compiuti dai terzi durante la trasmissione o l'archiviazione delle loro informazioni⁷².

Secondo quanto previsto dalla Joint Circular No. 07 on the Liabilities of Intermediary Service Suppliers in Protection of Copyrights and Related Rights on the Internet and Telecommunications Network Environment del 2012, gli intermediari *online* sono direttamente responsabili dei contenuti illeciti solo in limitate circostanze, come, ad esempio, quando essi avviano la pubblicazione, la trasmissione o la fornitura di contenuti illeciti su internet o sulle reti di telecomunicazioni, modificano o copiano il contenuto illecito, eludono deliberatamente le misure tecnologiche applicate dai titolari dei diritti per proteggere i diritti d'autore o i diritti connessi o operano come distributori secondari del contenuto illecito⁷³.

Il progetto di decreto sui servizi informatici, non ancora pubblicato, è stato reso disponibile al pubblico nel 2010 e successivamente in altre due versioni nel 2012. La versione di aprile 2012 richiedeva che i *server* e le infrastrutture per la fornitura di determinati servizi IT fossero situati in Vietnam, compresi i servizi di *cloud computing*, i servizi di portale di ricerca *web* ed i servizi di *data center*⁷⁴. Questo requisito di localizzazione è stato rimosso dalla versione successiva del decreto di agosto 2012. La versione di aprile 2012 aveva anche vietato la fornitura transfrontaliera di determinati servizi, tra cui i servizi di portale di ricerca *web*, i servizi di *cloud computing* e i servizi di *data*

⁷⁰ Decree No. 55/2001/ND-CP of August 23, 2001, on the management, provision and use of internet services, art. 22.2, disponibile al link: <http://hethongphapluatvietnam.com/decree-no-55-2001-nd-cp-of-august-23-2001-on-the-management-provision-and-use-of-internet-services.html>.

⁷¹ Si veda: T. NGUYEN, *Roles and Liabilities of Online Intermediaries in Vietnam - Regulations in the Mixture of Hope and Fear*, cit., par. II.A.

⁷² Si vedano gli articoli 16-20.

⁷³ Cfr. gli articoli 3.1 e 5.

⁷⁴ Si veda l'articolo 15.

center ed aveva richiesto ai fornitori di servizi stranieri di stabilire un'entità locale e di localizzare i propri *server* nel territorio nazionale per poter essere idonei ad ottenere una licenza di esercizio in Vietnam ⁷⁵. La versione di agosto 2012 ha modificato la precedente disposizione in modo che l'offerta transfrontaliera di servizi di *cloud computing*, di servizi di *database* di base e di servizi di portale di ricerca web è consentita a condizione che ciò avvenga attraverso le filiali locali o gli intermediari locali ⁷⁶.

Infine, nella stessa prospettiva, la Circular 38/2016 on cross border provision of public information, in vigore da maggio 2017, richiede agli OTT di avere dei rappresentanti locali e prevede un meccanismo di rimozione 24 ore su 24 dei contenuti identificati dal governo. La non conformità consente al governo di adottare "misure tecniche e sanzioni" per le società ed i relativi rappresentanti, ma i dettagli della disposizione non sono ancora chiari.

Infine, vi sono dei Paesi che sono relativamente neutrali in relazione alla questione della responsabilità degli intermediari *online*.

In Corea del Sud, le protezioni circa la responsabilità degli intermediari sono limitate all'obbligo di sospendere i contenuti su richiesta, comunque valutabile, anche se ciò ha sollevato delle critiche connesse al rischio di incoraggiare la censura privata ⁷⁷.

Secondo quanto disposto dal Network Act del 2015 ⁷⁸, gli intermediari sono tenuti ad eliminare il contenuto entro 30 giorni su richiesta di qualsiasi presunta vittima o di vari organi amministrativi e di monitorare le "informazioni illegali" come ad esempio, quelle che costituiscono una violazione della *privacy*, diffamazione, oscenità o pornografia infantile, a pena di incorrere nel pagamento di una sanzione o in responsabilità penale. Anche se gli intermediari adottano delle determinate misure, l'esenzione dalla responsabilità non è garantita, ma tale responsabilità può essere mitigata o evitata.

In particolare, l'articolo 44-2 della legge stabilisce che, laddove le informazioni fornite attraverso la rete siano rese intenzionalmente pubbliche coinvolgendo la *privacy* di altre persone, diffamino altre persone o violino il diritto di altre persone, la vittima di tale violazione può richiedere al fornitore di servizi di informazione e comunicazione che ha gestito le informazioni di eliminarle o di pubblicare una dichiarazione confutabile. Il fornitore

⁷⁵ Articoli 15 e 20.1.

⁷⁶ Si veda l'articolo 19.3.

⁷⁷ Cfr.: K.S. PARK, *Intermediary Liability - Not Just Backward but Going Back*, cit., par. III.B-III.D. e IV; D. SENG, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, cit., p. 36 ss.

⁷⁸ Si veda: Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (ICNA, Information and Communications Network Act), Act No. 3848 of May 12, 1986, as amended up to Act No. 13280 of March 27, 2015, disponibile al link: <http://www.wipo.int/wipolex/en/details.jsp?id=15671>.

in tal caso, deve adottare una misura temporanea entro un periodo che non deve superare i trenta giorni, o qualsiasi altra misura necessaria, dandone avviso al richiedente e a colui che ha pubblicato l'informazione. In tali casi, il fornitore deve anche far sapere ciò agli utenti, pubblicando un avviso pubblico sulla pertinente bacheca o in qualsiasi altro modo. Il governo ha proposto una legge di modifica per rafforzare la responsabilità degli intermediari, che è rimasta bloccata per oltre due anni.

L'Act on the Protection of Children and Juveniles against Sexual Abuse afferma che qualsiasi fornitore di servizi *online* che non adotta le misure prescritte dal decreto presidenziale per rilevare la pornografia infantile o giovanile nella rete di informazione e comunicazione gestita da se stesso, o che non riesce ad eliminare immediatamente il materiale pornografico giovanile o infantile rilevato e non adotta misure tecniche per prevenire o bloccare la trasmissione dello stesso, deve essere punito con il carcere con i lavori forzati per un periodo non superiore a tre anni o con una multa non superiore a venti milioni di won.

Tuttavia, ciò non trova applicazione se il fornitore di servizi *online* non è stato negligente nel prestare la debita attenzione a rilevare la pornografia giovanile o infantile nella rete di informazione e comunicazione, o anche laddove esso abbia tentato di impedire o bloccare la trasmissione del materiale pornografico giovanile o infantile ma sussistano sostanziali difficoltà tecniche ⁷⁹.

Infine, il Copyright Act prevede che quando un fornitore di servizi *online* è invitato a sospendere la riproduzione o la trasmissione interattiva, esso deve sospendere immediatamente la riproduzione o la trasmissione interattiva delle opere, ecc. Quindi, gli intermediari sono obbligati a bloccare il contenuto su richiesta e non vi è alcuna discrezionalità nel determinare se le opere notificate violino il *copyright* ⁸⁰.

Ad Hong Kong, le protezioni attualmente vigenti non sono chiare, ma la loro assenza non sembra causare particolari problemi.

La Control of Obscene and Indecent Articles Ordinance contiene il divieto di pubblicare articoli osceni ⁸¹. Nel 2009 e nel 2012, il governo ha tenuto due sessioni consultive per riesaminare e

⁷⁹ Si veda: Act on the Protection of Children and Juveniles Against Sexual Abuse, as amended by Act No. 11690, March 23, 2013, art. 17, disponibile al *link*: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=28311&lang=ENG. Nel novembre 2015, in base all'articolo 17 della legge, l'ex amministratore delegato della Kakao è stato perseguito per non aver adottato misure tecniche per monitorare e cancellare contenuti

pornografici infantili all'interno del loro servizio SNS mobile chiuso.

⁸⁰ Si veda: Copyright Act, last amended by Act No. 12137, 30 December 2013, art. 103, disponibile al *link*: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25455&lang=ENG.

⁸¹ Cap. 390 Control of Obscene and Indecent Articles Ordinance, 1 September

modificare il provvedimento. Alcuni hanno insistito affinché venisse elaborata una definizione più chiara di ciò che è “osceno” o “indecente”, andando oltre il tradizionale contenuto sessuale e per far includere i contenuti “violenti, depravati o repulsivi”. Il processo di revisione, tuttavia, non è proseguito oltre le consultazioni pubbliche, e ciò è dovuto in parte al sentimento negativo generale su questioni sensibili che potrebbero essere viste come una limitazione dei media.

L'*Australia* non annovera alcuna ampia protezione per la responsabilità del contenuto divulgato tramite internet, ma finora è stata applicata nei confronti delle società di telecomunicazioni la legge generale (in assenza di una giurisprudenza utile). Non ci sono protezioni per i diritti d'autore o per la diffamazione, mentre c'è un obbligo di segnalazione preventiva a carico degli intermediari per la sicurezza dei contenuti per l'infanzia che è utile per ridurre il volume di questioni segnalate al Commissario ⁸².

Il Broadcasting Services Act del 1992 sembra fornire un *safe harbor* per i fornitori di contenuti *online*, ma è stato ampiamente applicato nei confronti dei fornitori di servizi di telecomunicazione piuttosto che per gli intermediari *online* e non definisce chiaramente come tale regime di approdo sicuro debba essere applicato ⁸³. A causa di questa ambiguità, la legge non è stata in gran parte applicata nei confronti dei fornitori di contenuti su internet e non è stata neanche elaborata nei tribunali australiani.

La legge sul *copyright* del 2015, attualmente in fase di revisione, non contempla alcun regime di *safe harbor* per la protezione degli intermediari *online* ⁸⁴.

Nella legge sulla diffamazione, ancora, non vi è un chiaro regime di “approdo sicuro” per gli intermediari *online*. Le associazioni di categoria hanno iniziato a sollecitare una revisione, ma ciò richiederà un processo lungo dato che occorrerà trovare l'accordo tra i vari Stati/territori.

Infine, la legge Enhancing Online Safety for Children 2015 ⁸⁵ prevede che l'ufficio del Commissario richieda che tutti i denun-

1987, disponibile al *link*: <https://www.legislation.gov.hk/hk/cap390!en>.

⁸² Cfr.: K. PAPPALARDO, *Duty and Control in Intermediary Copyright Liability: An Australian Perspective*, in *IP Theory*, 2014, Vol. 4, No. 1, p. 9 ss., disponibile al *link*: <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1029&context=ipt>; D. Seng, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries - Part I*, 2010, disponibile al *link*: <http://www.wipo.int/publications/en/details.jsp?id=4144&plang=EN>.

⁸³ Si veda paragrafo 5, clausola 91(1),

disponibile al *link*: http://www9.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/bsa1992214/sch5.html.

⁸⁴ Si veda: Copyright Amendment (Online Infringement) Act 2015, No. 80/2015, disponibile al http://www.austlii.edu.au/cgi-bin/sinodisp/au/legis/cth/num_act/caia2015398/sch1.html. Gli ISP stanno spingendo per l'inclusione di un regime di *safe harbor*, mentre i titolari dei diritti si oppongono e cercano di estendere il dibattito all'autorizzazione e alla *secondary liability*.

⁸⁵ Si veda il paragrafo 3, clausola 18(5).

cianti abbiano preventivamente notificato l'intermediario, e si stanno cercando di sviluppare dei criteri in grado di dimostrare che ciò sia effettivamente accaduto.

La Nuova Zelanda ha una serie di tutele utili ma non esaustive per il *copyright* e delle protezioni più ampie che si basano sulla notifica all'autore e sulla contro-notifica per i contenuti dannosi, piuttosto complesse da applicare ⁸⁶.

Il Copyright Act del 1994 fornisce una limitata forma di *safe harbor* per i fornitori di servizi internet se l'utente viola il *copyright* ⁸⁷ e per la memorizzazione di materiale illecito ⁸⁸ o per la copia di dati già elaborati ⁸⁹. La politica sul *copyright* è in via di sviluppo ma il processo appare lento. Il governo ha recentemente completato uno studio su diritto d'autore e settore creativo ⁹⁰ e potrebbe prendere in considerazione la possibilità di rivedere il Copyright Act, ma tale questione ha una scarsa priorità e se dovesse progredire ciò avverrebbe comunque in un arco temporale di due-quattro anni. Anche se la legge fosse riesaminata, non vi è alcuna certezza che sarebbe modificato il regime di *safe harbor*, poiché l'attenzione politica si è concentrata su un regime di eccezioni flessibili.

L'Harmful Digital Communications Act del 2015 fornisce un

⁸⁶ L.C. RODRIGUEZ RENCIFO, *Internet Intermediaries Liability: Participative Networking Platforms and Harmful Content*, 2016, p. 20 ss., disponibile al link: <http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/5225/paper.pdf?sequence=1>; D. SENG, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, cit., p. 33 ss.

⁸⁷ Un fornitore di servizi internet non viola il diritto d'autore sull'opera, né autorizza una violazione del diritto d'autore sull'opera da parte dei suoi utenti, semplicemente perché il fornitore di servizi internet è a conoscenza dell'infrazione, a condizione che, in relazione alla presunta violazione, il fornitore di servizi internet si conformi a tutti i suoi obblighi (cfr.: Act No. 143/1994, section 92B, disponibile al link: <http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM345634.html>).

⁸⁸ Il fornitore di servizi internet non viola il diritto d'autore sull'opera archiviando il materiale a meno che a) il fornitore di servizi internet (i) sappia o abbia ragionevoli motivi per ritenere che il materiale violi il copyright; e (ii) non appena possibile dopo aver preso conoscenza del materiale illecito, elimini il materiale o ne impedisca l'accesso; oppure b) l'utente del servizio che ha fornito il materiale agisce per conto o sotto la direzione del fornitore di servizi internet (sezione 92C).

⁸⁹ Un fornitore di servizi internet non viola il diritto d'autore su un'opera memorizzando materiale se il fornitore di servizi internet a) non modifica il materiale; b) rispetta le condizioni imposte dal titolare del copyright del materiale per l'accesso a tale materiale; c) non interferisce con l'uso lecito della tecnologia per ottenere dati sull'uso del materiale; d) aggiorna il materiale in conformità con la ragionevole prassi del settore. Tuttavia, un fornitore di servizi internet viola il diritto d'autore memorizzando materiale se il fornitore di servizi internet non elimina il materiale o impedisce l'accesso degli utenti ad esso il più presto possibile dopo che è venuto a conoscenza che (a) il materiale è stato cancellato dalla sua fonte originale; o (b) è stato impedito l'accesso al materiale alla sua fonte originale; o (c) una corte ha ordinato che il materiale sia cancellato dalla sua fonte originale o che l'accesso al materiale alla sua fonte originale sia impedito (sezione 92E).

⁹⁰ Ministry of Business, Innovation & Employment, Copyright and the Creative Sector: Study on the Role of Copyright and Registered Designs in the Creative Sector in New Zealand, December 2016, disponibile al link: <http://www.mbie.govt.nz/info-services/business/intellectual-property/copyright/copyright-and-the-creative-sector/copyright-and-the-creative-sector.pdf>.

regime di protezione per aver ospitato contenuti *online* in relazione a qualsiasi tipo di contenuto digitale pubblicato dagli utenti se l'*host* segue un processo dettagliato ma complesso. L'*host* deve avvisare l'autore del contenuto e adottare le conseguenti azioni in base alla contro-notifica dell'autore del contenuto che acconsente o rifiuta la rimozione del contenuto o che non presenta una contro-notifica valida. Tali azioni comprendono l'eliminazione o la disattivazione del contenuto entro 48 ore dalla notifica o dalla contro-notifica ⁹¹.

L'*Indonesia* fornisce un regime di protezione dalla responsabilità degli intermediari *online* che è molto debole ed è improbabile sia rafforzata, specialmente per la diffamazione. Le disposizioni si rivolgono, inoltre, alle piattaforme di *e-commerce* e lasciano incertezza attorno al loro ambito di applicazione. Le pressioni politiche incentrate sulla rimozione e sui tempi di risposta hanno portato, infine, ad elaborare un progetto di regolamento sugli OTT.

La Law on Electronic Information and Transactions n. 11/2008, parzialmente emendata con legge n. 19/2016 ⁹², è la fonte delle altre discipline derivate. La legge ha ridotto la sanzione penale per la diffusione di contenuti contro proprietà, gioco d'azzardo, ingiurie o diffamazioni, estorsioni o minacce, fino ad un massimo di quattro anni dai precedenti sei anni, che sono ancora applicabili invece alla diffusione di informazioni false e fuorvianti che portano danni ai consumatori, o di informazioni volte ad alimentare l'odio o il dissenso negli individui e/o nei confronti di determinati gruppi etnici, religiosi, razziali ⁹³.

Alla riforma della sanzione, tuttavia, non ha fatto seguito un miglioramento procedurale, quindi, il tasso dei casi di diffamazione individuale è ancora alto ⁹⁴. Finora, generalmente gli individui hanno segnalato casi di diffamazione ad altri individui. Ma dato il modo in cui è stata scritta la disposizione, la stessa potrebbe essere estesa anche agli intermediari *online*.

Il Ministerial Regulation No. 19 of 2014 on Negative Content, definiti come contenuti che coinvolgono la pornografia e altre attività considerate illegali ai sensi delle leggi vigenti, fornisce una procedura dettagliata di notifica e rimozione.

Le istituzioni governative, le forze dell'ordine ed il pubblico, in generale, possono presentare una relazione al ministro, tramite il direttore generale dell'informatica, con la quale richiedono che

⁹¹ Si veda: Act No. 63/2015, sections 23-25 disponibile al *link*: <http://www.legislation.govt.nz/act/public/2015/0063/latest/DLM5711810.html>.

⁹² Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

⁹³ Si vedano gli articoli 27, 28 e 45.

⁹⁴ Fino ad oggi, centoquaranta persone sono state condannate in base alla clausola di diffamazione. Il governo è sotto pressione dalla coalizione delle ONG per rinnovare la legge nella sua interezza.

determinati siti *web* siano bloccati a causa di contenuti illeciti. Dopo aver ricevuto il rapporto, il Direttore Generale includerà il sito *web* segnalato nell'elenco TRUST + Positive, che è un sistema di database che elenca i siti con contenuto negativo.

I fornitori di servizi internet devono bloccare l'accesso a tutti i siti *web* contenuti nell'elenco TRUST + Positive. I fornitori di servizi internet sono tenuti ad aggiornare regolarmente ed almeno una volta alla settimana il proprio *database* di siti *web* vietati in conformità con l'elenco TRUST + Positive. Nei casi in cui è necessario che siano adottati immediatamente dei provvedimenti, l'aggiornamento deve essere effettuato entro un giorno dal momento in cui il sito *web* è incluso nell'elenco TRUST + Positive.

I titolari dei siti *web* bloccati ed i membri del pubblico possono presentare al Direttore generale una richiesta di sblocco di un determinato sito Web inserito nell'elenco TRUST + Positive. Se il sito *web* segnalato non contiene materiale pornografico o illegale, il Direttore Generale rimuoverà il sito *web* dall'elenco TRUST + Positive ⁹⁵.

Nel dicembre 2016, poi, è stata emessa la Safe Harbour Ministerial Circular Letter, in cui, per garantire l'attuazione di un sistema elettronico sicuro, affidabile e responsabile che supporti la crescita dell'*e-commerce*, si è prevista una tutela giuridica per la piattaforma di *e-commerce* e per l'utente della medesima piattaforma determinando la responsabilità di ciascuna parte che conduce attività commerciali attraverso il sistema elettronico e proteggendo gli UGC dai venditori che utilizzano la piattaforma per vendere merci illegali.

Tuttavia, la versione finale del progetto di regolamento sugli OTT, pubblicata nell'agosto 2017, si sovrappone al summenzionato provvedimento relativo al *safe harbor* prevedendo un regime molto rigoroso per le società OTT, definite in senso lato includendo nel proprio ambito una varietà di applicazioni internet e di servizi di contenuti quali transazioni finanziarie e commerciali, *social networking*, giochi, media, email, motori di ricerca, ecc. In particolare, vengono stabiliti dei requisiti come quello di stabilire una presenza locale e di registrarsi prima di fornire dei servizi in Indonesia, di detenere le entrate derivanti da vendite o da servizi forniti in Indonesia su un conto bancario locale e di fornire un meccanismo per il filtraggio e l'accesso ai contenuti funzionali per le intercettazioni legali e per l'acquisizione delle prove per l'investigazione di casi criminali.

⁹⁵ Si vedano gli articoli 5, 6, 8, 9 and 13-16. Questo provvedimento è in fase di revisione. La revisione si concentrerebbe: a) sui siti bloccati in modo permanente che si ritiene abbiano pubblicato continuamente

contenuti negativi dopo la rimozione del blocco temporaneo; b) sull'aggiunta dell'elenco di questioni illegali attualmente dichiarate sull'art. 4. Ciò è innescato dal sollevarsi del problema delle cd. *fake news*.

Esiste un *safe harbor* per le piattaforme di *e-commerce* che riscontrano difficoltà nello sviluppare un sistema di filtraggio dei contenuti ed un meccanismo di censura, in tali casi l'intermediario non sarà direttamente responsabile per tutti i post pubblicati dal venditore. Tuttavia, il sistema di filtraggio dei contenuti ed il meccanismo di censura esistono ancora nel contesto degli OTT e questi ultimi devono seguire le istruzioni del governo per cancellare il contenuto o la pubblicazione se è ritenuto illegale dalle leggi indonesiane.

III.2. *La responsabilità degli intermediari negli Stati Uniti.*

Gli Stati Uniti sono il Paese in cui hanno avuto origine la maggior parte dei più importanti intermediari *online* globali e dove si è sviluppata una solida industria dei contenuti. Quindi, da una parte, non sorprende che la legge statunitense incorpori delle protezioni significative per gli intermediari *online* ed i fornitori di contenuti. D'altra parte, il bilanciamento degli interessi tra gli intermediari e l'industria dei contenuti è la principale sfida da affrontare.

La legge americana sancisce robuste protezioni per la libertà di espressione nel Primo Emendamento della Costituzione degli Stati Uniti. Pertanto, le leggi federali e statali ed i tribunali che le applicano devono contemporaneamente prendere in considerazione, nell'adozione dei rispettivi provvedimenti, il diritto alla libertà di espressione della persona che ha creato i contenuti, i diritti del soggetto di quella stessa espressione ed il ruolo dell'intermediario ⁹⁶.

Negli anni '90, il Congresso degli Stati Uniti ha approvato due leggi che si sono rivelate essenziali per lo sviluppo della rete internet globale così come la conosciamo oggi: il Communications Decency Act del 1996 ⁹⁷ e il Digital Millennium Copyright Act del 1998 ⁹⁸.

⁹⁶ Si veda tra gli altri: A. HOLLAND, C. BAVITZ, J. HERMES, A. SELLARS, R. BUDISH, M. LAMBERT, N. DECOSTER, *Intermediary Liability in the United States, The Global Network of internet & Society Research Centers - Online Intermediaries Case Studies Series*, 2015, par. I, disponibile al link: https://publixphere.net/i/noc/page/OI_Case_Study_Intermediary_Liability_in_the_United_States; G.B. DINWOODIE, *A Comparative Analysis of the Secondary Liability of Online Service Providers*, cit., p. 25 ss.; S. ERICSSON, *The Commodification of Internet Intermediary Safe Harbors: Avoiding Premature Harmonization Around a Suboptimal Standard*, in H. ULLRICH, R.M.

HILTY, M. LAMPING, J. DREXL (a cura di), *TRIPS plus 20: From Trade Rules to Market Principles*, Springer, 2016, p. 265 ss., disponibile al link: <https://ssrn.com/abstract=2777486>.

⁹⁷ Anche chiamato Titolo V del Telecommunications Act del 1996, Public Law 104-104, 8 febbraio 1996, disponibile al <http://transition.fcc.gov/Reports/tcom1996.txt>.

⁹⁸ Digital Millennium Copyright Act, Public Law 105-304, 28 October 1998, disponibile al link: <https://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf>.

Come accennato in precedenza, queste normative hanno contribuito ad incoraggiare lo sviluppo degli intermediari di internet aumentando la loro fiducia nel fatto che non sarebbero stati ritenuti responsabili se un utente avesse utilizzato i loro servizi per violare i diritti di qualcun altro.

Il DMCA ha stabilito un regime di *notice and take down* che non ha imposto a carico dell'intermediario di internet l'onere del controllo per la scoperta della violazione del *copyright*⁹⁹. Piuttosto che monitorare le proprie reti alla ricerca di possibili violazioni del *copyright* — un compito costoso e difficile — gli intermediari *online* possono aspettare che i titolari dei diritti di *copyright* li informino circa le specifiche violazioni.

La sezione 512 del DMCA¹⁰⁰ prevede quattro circostanze in cui un fornitore di servizi internet non è ritenuto responsabile: il transito delle comunicazioni digitali, i sistemi di *caching*, le informazioni risiedono su sistemi o reti a direzione degli utenti e gli strumenti di localizzazione delle informazioni.

Per godere del regime di *safe harbor* stabilito dal DMCA, deve essere vero che l'intermediario *online*: A) i) non ha conoscenza effettiva del fatto che il materiale o che un'attività che utilizza il materiale sul proprio sistema o sulla sua rete stia ponendo in essere una violazione; ii) in assenza di tali effettive conoscenze, non è consapevole di fatti o circostanze da cui risulti l'attività illecita; o iii) dopo essere venuto a conoscenza o avendo la consapevolezza, agisce rapidamente per rimuovere o disabilitare l'accesso al materiale; B) non riceve alcun diretto beneficio finanziario dallo svolgimento dell'attività illecita, nel caso in cui il fornitore di servizi abbia il diritto o la capacità di controllare tale attività; e C) in seguito alla notifica di una presunta violazione, agisce tempestivamente provvedendo alla rimozione o alla disattivazione dell'accesso al materiale che si ritiene contravvenga o che sia oggetto di attività illecite.

La sezione 230 del Communications Decency Act¹⁰¹ ha scongiurato anche le richieste di risarcimento derivanti da responsabilità degli intermediari per diffamazione e per tutta una serie di altre rivendicazioni civili. In particolare, la Sezione 230 del CDA ha posto al riparo le imprese di internet da una varietà di cause derivanti da azioni federali e statali¹⁰².

⁹⁹ A proposito della procedura di *notice and take-down*, si veda tra le altre la sentenza *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015).

¹⁰⁰ 17 U.S. Code § 512 - Limitations on liability relating to material online.

¹⁰¹ 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material.

¹⁰² Questo include, per esempio, il Federal Fair Housing Act, Title II of the Civil Rights Act of 1964, il Washington State Consumer Protection Act, e azioni di common law come la violazione della *privacy*, la negligenza e le interferenze illecite nei rapporti commerciali. Cfr.: M. A. LEMLEY, *Rationalizing Internet Safe Harbors*, in *Journal*

Come osservato dall'US Fourth Circuit Court of Appeals degli Stati Uniti, infatti, un sistema di *notice and take down* conduce inevitabilmente le imprese a scegliere di rimuovere i contenuti controversi piuttosto che trovarsi ad affrontare una qualunque responsabilità ¹⁰³.

III.3. La responsabilità degli intermediari nell'Unione Europea.

Le disposizioni di legge dell'Unione europea in materia di responsabilità degli intermediari *online* si sono rivelate meno attrattive per gli imprenditori di internet rispetto alla legge statunitense. L'Europa adotta un approccio uniforme alla questione della responsabilità dell'intermediario, stabilendo gli stessi presupposti per la responsabilità, indipendentemente dalla natura della violazione sottostante ¹⁰⁴.

La direttiva 2000/31/CE ¹⁰⁵ stabilisce quali siano i *safe harbor* dalla responsabilità per il compimento da parte degli intermediari di specifiche attività, ossia l'agire come "*mere conduit*" ¹⁰⁶, "*caching*" o "*hosting*" ¹⁰⁷.

In primo luogo, l'approccio europeo si ferma ben al di sotto

on *Telecommunications and High Technology Law*, 2007, No. 6, p. 101 ss.

¹⁰³ Si veda: A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 3-4.

¹⁰⁴ Secondo un approccio "orizzontale" diverso da quello americano, che, come noto, offre diverse regole per la responsabilità dell'intermediario per le violazioni del copyright, marchi commerciali e altri reati. Si veda: M. PEGUERA, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, in *Columbia Journal of Law & the Arts*, 2009, Vol. 32, No. 4, p. 481 ss., disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1468433. Si veda, poi, Corte di Giustizia dell'Unione europea, 23 marzo 2010, C-236/08, C-237/08 e C-238/08, secondo cui: "La sezione 4 della direttiva 2000/31, che comprende gli artt. 12-15, recante l'intestazione 'Responsabilità dei prestatori intermediari', è diretta a limitare le ipotesi in cui, conformemente al diritto nazionale applicabile in materia, può sorgere la responsabilità dei prestatori di servizi intermediari. È pertanto nell'ambito di tale diritto nazionale che vanno ricercati i requisiti per accertare una siffatta responsabilità, fermo restando però che, ai sensi della sezione 4 di tale direttiva, talune fattispecie non possono dar luogo a una responsabilità dei prestatori di servizi intermediari" (cfr. anche, nello stesso senso, Corte

di Giustizia dell'Unione europea, 12 luglio 2011, C-324/09). Su questi temi, nella dottrina italiana, si vedano tra gli altri: R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico*, ESI, 2003, p. 178; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, ESI, 2003, p. 294.

¹⁰⁵ Direttiva 2000/31/CE sul commercio elettronico, cit.

¹⁰⁶ In proposito si segnala Corte di Giustizia dell'Unione europea, 15 settembre 2016, causa C-484/14, *Mc Fadden c. Sony Music Entertainment Germany*.

¹⁰⁷ Circa gli ambiti di applicazione dell'esenzione si vedano le pronunce della Corte di Giustizia dell'Unione europea, 23 marzo 2010, causa C-236/08 *Google France c. Louis Vuitton*; 12 luglio 2011, causa C-324/09, *L'Oréal c. eBay*. Per un approfondimento sulla quarta sezione della direttiva, artt. 12-15, v. tra gli altri: R. D'ARRIGO, *La responsabilità degli intermediari nella nuova disciplina del commercio elettronico*, in *Danno e responsabilità*, 2004, pp. 248-254; G.M. RICCIO, *La responsabilità civile degli internet providers*, Giappichelli, 2002; Circa l'esenzione che caratterizza l'attività di hosting la norma è oggetto di numerosi dibattiti da parte della dottrina, cfr.: G.M. RICCIO, *La responsabilità degli Internet Service Provider. Situazione legislativa e problemi aperti*, in V. D'ANTONIO, S. VIGLIAR, (a cura di) *Studi di diritto della comunicazione*,

della completa esclusione di responsabilità offerta dal CDA per le violazioni relative a questioni non di proprietà intellettuale ¹⁰⁸.

In secondo luogo, la Direttiva sul commercio elettronico dell'Unione Europea adotta ampiamente l'approccio del DMCA di notifica e rimozione, ma lascia aperta la possibilità di responsabilità aggiuntive dell'intermediario *online*. Anche se esclude qualsiasi dovere di monitoraggio, la legislazione dell'UE contempla espressamente l'imposizione, da parte degli Stati membri, di "doveri di diligenza" a carico degli intermediari per individuare e prevenire determinate attività ¹⁰⁹.

In terzo luogo, la Direttiva europea non prevede un obbligo di notifica e rimozione, creando maggiore incertezza tra i fornitori europei in merito al fatto che abbiano in qualche modo acquisito conoscenze sufficienti per essere ritenuti responsabili se non eliminano il materiale per conto proprio ¹¹⁰.

Recentemente, la Commissione europea ha avviato alcune iniziative volte a sostenere lo sviluppo di un contesto, nel quale operano le cd. "piattaforme" *online*, basato sulla fiducia, sulla legalità e sull'innovazione. A tal fine, la Comunicazione della Commissione sulle piattaforme *online*, pubblicata nel corso del mese di maggio 2016, ha individuato i principali ambiti nei quali è necessario porre maggiore attenzione. I principi guida della politica perseguita dalla Commissione sono: i) la parità di condizioni per i servizi digitali comparabili; ii) la garanzia che le piattaforme *online* si comportino in modo responsabile per proteggere i valori fondamentali; iii) la promozione della fiducia, della trasparenza e dell'equità; iv) lo sviluppo di mercati aperti e

persone, società e tecnologie dell'informazione, Cedam, 2009 p. 161.

¹⁰⁸ Per un'analisi generale si vedano: M. DE CATA, *La responsabilità civile dell'internet service provider*, Giuffrè, 2010; P. SANNA, *Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione*, in *Responsabilità civile e previdenza*, 2004, p. 279-302.

Si veda anche G. CASSANO e A. CONTALDO, *La natura giuridica e la responsabilità civile degli Internet Service Providers (ISP): il punto sulla giurisprudenza*, in *Corriere giuridico* 9/2009, pag. 1206 ss. Parte della dottrina ritiene che le cause di esonero da responsabilità del provider sarebbero tassative Cfr. G. M. RICCIO, in P. STANZIONE, S. SICA, *Professioni e responsabilità civile*, Bologna, Zanichelli Editore, 2006, p. 749. Alcuni ritengono che la Direttiva sia finalizzata a garantire una sorta di immunità ai provider che si limitano a svolgere un ruolo tecnico di intermediazione; cfr. Di CIOMMO, *op. cit.*, p. 293, G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli*

internet service Providers, in *Danno e responsabilità*, 2002 p. 9; T. PASQUINO, *Servizi telematici e criteri di responsabilità*, Milano, 2003, p. 289.

¹⁰⁹ In argomento, si vedano tra gli altri: G.M. RICCIO, *La responsabilità civile degli internet providers*, cit.; P. SANNA, *Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione*, in *Responsabilità civile e previdenza*, 2004, p. 279; M. DE CATA, *La responsabilità civile dell'internet service provider*, cit., p. 186; R. D'ARRIGO, *La responsabilità degli intermediari nella nuova disciplina del commercio elettronico*, cit..

¹¹⁰ Si veda: A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 4; M. PEGUERA, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, cit., p. 490; S. ERICSSON, *The Commodification of Internet Intermediary Safe Harbors: Avoiding Premature Harmonization Around a Suboptimal Standard*, cit. p. 465.

non discriminatori ed evitare le discriminazioni per favorire un'economia basata sui dati ¹¹¹.

Nella revisione di medio termine della strategia per il mercato unico digitale ¹¹², la Commissione europea si è impegnata a promuovere due azioni principali: a) preparare delle proposte che affrontino le questioni relative alle clausole contrattuali abusive e alle pratiche commerciali scorrette identificate nelle relazioni tra piattaforme e imprese, prendendo in considerazione i meccanismi di risoluzione delle controversie, i criteri di correttezza e la trasparenza ¹¹³; b) assicurare un migliore coordinamento del dialogo con le piattaforme all'interno del mercato unico digitale, focalizzandosi sui meccanismi e le soluzioni tecniche per la rimozione dei contenuti illegali, al fine di migliorarne l'efficacia nel pieno rispetto dei diritti fondamentali.

Nel settembre 2017, così, la Commissione ha presentato una Comunicazione nella quale ha individuato delle linee guida relative alla lotta contro i contenuti illegali *online*: incitamento al terrorismo, illecito incitamento all'odio, materiale pedopornografico, nonché violazioni dei diritti di proprietà intellettuale e protezione dei consumatori *online* ¹¹⁴. La Comunicazione ha definito una serie di linee guida e principi per le piattaforme *online* volti a rafforzare la lotta contro i contenuti illegali *online* in cooperazione con le autorità nazionali, gli Stati membri e le altre parti interessate.

Quindi, nel marzo 2018 è giunta la Raccomandazione sulle misure per un effettivo contrasto ai contenuti illegali online, in cui la Commissione ha fornito una serie di indicazioni riguardo ai meccanismi di notifica, di informazione dei fornitori di contenuti e di contro-notifica, alla trasparenza delle *policy* alle tutele da predisporre e alle attività svolte da parte dei fornitori di servizi internet, alla cooperazione tra questi, con gli Stati membri e con

¹¹¹ Si veda: Commissione europea, Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, cit., par. 5; per ulteriori riferimenti in merito alle attività della Commissione sulle piattaforme *online* v.: <https://ec.europa.eu/digital-single-market/en/policies/online-platforms>.

¹¹² Digital Single Market Mid-term Review, in cui la Commissione ha sollecitato una rapida adozione delle proposte chiave e una mappatura delle sfide future, disponibile al link: <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review>; cfr., in particolare: Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy A

Connected Digital Single Market for All, 10 May 2017, COM(2017)/0228 final, disponibile al link: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228>.

¹¹³ I dettagli della revisione sono disponibili al link: <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review>.

¹¹⁴ Commissione europea, Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms, 28 September 2017, COM(2017) 555 final, disponibile al link: <https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms>.

i *trusted flagger*¹¹⁵, alla risoluzione alternativa delle controversie, etc.¹¹⁶.

Pertanto, la Commissione europea continua il percorso intrapreso negli ultimi anni con varie iniziative come, ad esempio, l'EU Internet Forum, il Better Internet for Kids, il Memorandum d'intesa contro le merci contraffatte e il Codice di condotta sull'illecito incitamento all'odio, che comprende tutta una serie di impegni assunti da Facebook, Microsoft, Twitter e YouTube per combattere la diffusione di tali contenuti in Europa. L'implementazione del predetto Codice è monitorata dalla Commissione attraverso un meccanismo di valutazione realizzato dalle organizzazioni non governative e dagli organismi pubblici in 24 Stati membri¹¹⁷.

Inoltre, nel 2017-2018 la Commissione ha ritenuto opportuno effettuare un'analisi della questioni poste dal processo decisionale basato sugli algoritmi. Il progetto pilota, avviato su richiesta del Parlamento europeo, mira a fornire uno studio e a diffondere consapevolezza in merito al ruolo che svolgono gli algoritmi nel contesto delle piattaforme *online*, in particolare, su come essi possono modellare, filtrare o personalizzare i flussi di informazioni che intermediano¹¹⁸.

Ad aprile 2018, dunque, la Commissione ha pubblicato una bozza di Regolamento sulla promozione dell'equità e della trasparenza per gli utenti aziendali dei servizi di intermediazione *online*¹¹⁹, nonché una Comunicazione su un "New Deal" per i consumatori e due relative proposte di Direttiva su una migliore applicazione e modernizzazione delle norme dell'UE in materia di

¹¹⁵ Ossia individui o entità considerati da un fornitore di servizi "segnalatori di fiducia" in quanto hanno particolari competenze e responsabilità al fine del contrasto dei contenuti illegali *online*.

¹¹⁶ Cfr.: Commission Recommendation of 13.2.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final), disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online>. Peraltro, il processo di analisi sul tema da parte della Commissione è tuttora in corso; si veda: Public consultation on measures to further improve the effectiveness of the fight against illegal content online, 30 April 2018, disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/public-consultation-measures-further-improve-effectiveness-fight-against-illegal-content-online>.

¹¹⁷ Si veda: Code of Conduct on Countering Illegal Hate Speech, 31 May 2016, disponibile al *link*: http://ec.europa.eu/justice/fundamental-rights/files/hate-speech_code_of_conduct_en.pdf, e il suo secondo monitoraggio disponibile al *link*: http://europa.eu/rapid/press-release_IP-17-1471_en.htm. Nello stesso senso, ad aprile 2018 la Commissione europea ha chiesto alle piattaforme *online* e ai *social network* di raggiungere un accordo su un codice di condotta contro la disinformazione in rete (v.: http://europa.eu/rapid/press-release_IP-18-3370_en.htm).

¹¹⁸ Si veda: Call for tender: Study to raise awareness about algorithms, July 2017, disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/call-tender-study-raise-awareness-about-algorithms>.

¹¹⁹ Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, 26 April 2018, COM(2018) 238 final, disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services>.

protezione dei consumatori e su azioni rappresentative per la protezione degli interessi collettivi degli stessi ¹²⁰.

Le nuove proposte normative, così come le precedenti sul contrasto ai contenuti illegali *online*, da un lato, ribadiscono che il regime di *safe harbor* della Direttiva sul commercio elettronico per gli ISP è fondamentale per lo sviluppo della società dell'informazione ¹²¹ e che qualsiasi misura futura adottata in base a tali leggi dovrebbe ancora rispettarla ¹²²; dall'altro, esse richiedono chiarezza e trasparenza dei termini e condizioni delle piattaforme e delle procedure di cessazione, sospensione o rimozione ¹²³.

Infine, unitamente a una Comunicazione nella quale ha indicato una strategia per l'intelligenza artificiale in Europa ¹²⁴, la Commissione ha pubblicato una valutazione degli attuali quadri di sicurezza e responsabilità nelle "tecnologie digitali emergenti" ¹²⁵, che non contempla alcun suggerimento regolamentare immediato

¹²⁰ Rispettivamente: Comunicazione "Un 'New Deal' per i consumatori", COM(2018) 183 final; Proposta di direttiva che modifica la direttiva 93/13/CEE del Consiglio del 5 aprile 1993, la direttiva 98/6/CE, la direttiva 2005/29/CE e la direttiva 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'UE relative alla protezione dei consumatori, COM(2018) 185 final; Proposta di Direttiva relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE, COM(2018) 184 final; tutte dell'11 aprile 2018. L'insieme dei documenti e iniziative presentati dalla Commissione nell'ambito del "New Deal" per i consumatori" è disponibile al *link*: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=620435.

¹²¹ Riguardo all'assenza di un obbligo di sorveglianza a carico degli ISP, cfr.: G. Pino, Assenza di un obbligo generale di sorveglianza a carico degli Internet Service Providers sui contenuti immessi da terzi in rete, cit..

¹²² Così, tali iniziative prendono le distanze dall'attuale spinta verso obblighi di monitoraggio che la stessa Commissione ha viceversa inserito nel contesto della Proposta di direttiva sul diritto d'autore nel mercato unico digitale presentata nel settembre 2016, COM(2016) 593 final, disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market> (art. 13).

¹²³ Sia le Direttive che il Regolamento affermano quindi che i termini e condizioni delle piattaforme dovrebbero rivelare i parametri principali che determinano le classifiche e i risultati di ricerca, chiarendo

quando e come i risultati sono sponsorizzati ed evitando di privilegiare i beni o i servizi offerti dalla piattaforma stessa e da altre aziende che utilizzano la piattaforma, secondo il Regolamento le corti potrebbero dichiarare "non vincolanti" clausole dei termini e condizioni di una piattaforma se non sono sufficientemente chiari e specifici nello stabilire quando la piattaforma può sospendere o terminare il proprio servizio a un utente aziendale.

¹²⁴ Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final, disponibile al *link*: https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe?utm_source=POLITICO.EU&utm_campaign=fb25ba8e0f-EMAIL_CAMPAIGN_2018_04_25&utm_medium=email&utm_term=0_10959edeb5-fb25ba8e0f-189775021&utm_source=POLITICO.EU&utm_campaign=bfd4608123-EMAIL_CAMPAIGN_2018_04_25&utm_medium=email&utm_term=0_10959edeb5-bfd4608123-189665609.

¹²⁵ European Commission Staff Working Document: Liability for emerging digital technologies, accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions "Artificial Intelligence for Europe", 25 April 2018, disponibile al *link*: <https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies>.

ma accenna all'ipotesi che ulteriore regolamentazione potrebbe includere il software, introdurre una responsabilità oggettiva per ciò che fa uso di intelligenza artificiale, un "concetto di tutela" per robot avanzati, estendere la responsabilità al contesto *business to business* e includere danni consequenziali e puramente economici.

III.4. *Le linee guida internazionali.*

Infine, nell'arena internazionale, gli standard per il regime di responsabilità degli intermediari potrebbero essere oggetto di accordi tra Paesi nel contesto di accordi commerciali bilaterali o multilaterali.

In questa prospettiva, impulsi rilevanti a livello internazionale provengono dalle normative in materia di diritti umani — di particolare importanza in questo contesto sono la Dichiarazione universale dei diritti umani¹²⁶ e la Convenzione internazionale sui diritti civili e politici¹²⁷ — e anche dagli sforzi compiuti a livello globale e *multi-stakeholder*, come nel caso del tentativo di creare una simile piattaforma per la *governance* di internet con la cd. NETmundial Initiative¹²⁸.

Nel 2015 un gruppo di organizzazioni della società civile, tra cui la Electronic Frontier Foundation, il Centre for internet Society India e l'Article 19, ha proposto i "Manila Principles" sulla responsabilità degli intermediari. I Manila Principles sono un insieme di linee guida e di *best practices* volte a limitare la responsabilità degli intermediari in relazione ai contenuti e a promuovere la libertà di espressione e l'innovazione.

I sei Manila Principles sono: *i*) Gli intermediari devono essere protetti dalla legge per la responsabilità derivante dai contenuti di terzi. *ii*) i contenuti non devono essere limitati senza che vi sia un provvedimento di un'autorità giudiziaria. *iii*) Le richieste di restrizione dei contenuti devono essere chiare, non essere ambigue e seguire il giusto processo. *iv*) Le leggi, i provvedimenti e le pratiche di limitazione dei contenuti devono essere conformi ai test di necessità e proporzionalità. *v*) Le leggi, le politiche e le pratiche di limitazione dei contenuti devono rispettare il giusto processo. *vi*) I principi di trasparenza e di responsabilità devono essere considerati nelle leggi e nelle pratiche di restrizione dei contenuti¹²⁹.

¹²⁶ Universal Declaration of Human Rights, 10 dicembre 1948, disponibile al link: <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=itn>.

¹²⁷ International Covenant on Civil and Political Rights, 16 dicembre 1966, disponibile al link: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

¹²⁸ Cfr.: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 14-15.

¹²⁹ Si vedano: Manila Principles on Intermediary Liability Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression

I Manila Principles si concentrano sul giusto processo, comprendendo il rispetto dei principi di trasparenza e responsabilità tra i requisiti che devono rispettare i provvedimenti giudiziari per la rimozione dei contenuti ¹³⁰.

Infine, possono essere considerati come ulteriore esempio i negoziati sull'accordo di partenariato Trans-Pacifico ¹³¹.

IV. MODELLI DI GOVERNANCE.

IV.1. *Legal process.*

L'analisi rivela che i governi — oltre ai fattori tecnologici e di mercato — sono le forze più importanti che modellano il panorama degli intermediari *online* di un determinato paese.

I relativi ruoli che il governo può svolgere sono piuttosto differenti e spesso si sovrappongono e vanno dai “governi come utenti” ai “governi come regolatori” degli intermediari. Concentrandosi su quest'ultima ipotesi, la ricerca dimostra che, anche all'interno del ruolo svolto dal governo quale regolatore degli intermediari *online*, vi possono essere importanti sfumature funzionali in termini di differenti manifestazioni e interpretazioni di questo ruolo.

Inoltre, l'analisi suggerisce che possono essere coinvolte nel rispettivo regime di governo degli intermediari *online* diverse istituzioni, a seconda del modello e della strategia di regolazione sottostanti. In alcuni paesi, le agenzie governative sono i regolatori chiave; altri regimi di governo fanno, invece, molto affidamento sulle corti ¹³².

Il modello di base e i differenti gradi di coinvolgimento del governo portano a domande chiave sugli incentivi, la legittimità, la responsabilità e la trasparenza.

Oltre a queste questioni fondamentali, l'analisi va oltre suggerendo anche una dimensione inesplorata della problematica relativa alla *governance*: il ruolo della conoscenza quando si tratta della regolazione degli intermediari *online*, e di come tali competenze — ad esempio per quanto riguarda la comprensione di come agiscono tecnicamente i diversi tipi di intermediari — possano essere distribuite in modo diseguale tra i diversi rami dell'amministrazione coinvolti nel rispettivo regime di *governance*.

and Innovation, 24 March 2015, disponibili al link: <https://www.manilaprinciples.org>.

¹³⁰ Si veda di nuovo: A. CHANDER, *Internet Intermediaries as Platforms for Expression and Innovation*, cit., p. 7.

¹³¹ Sul ruolo della responsabilità dell'intermediario nel commercio, si veda: The Internet Association, *Harmonizing Interme-*

diary Immunity for Modern Trade Policy, May 2014, disponibile al link: <http://internetassociation.org/wp-content/uploads/2014/05/May2014-Section230.pdf>

¹³² Cfr.: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 9.

La maggior parte dei regimi di *governance* studiati nel corso di questa ricerca, per mettere in pratica il relativo modello di regolazione degli intermediari *online*, fanno molto affidamento sul sistema giudiziario. Un tipo alternativo di regime quando si tratta di intermediari *online* pone l'accento sulle agenzie governative.

Per quanto riguarda le questioni che non fanno parte delle problematiche legate al *copyright*, la Corea è un esempio in cui un'agenzia governativa, sotto forma della Korean Communication Standards Commission, svolge un ruolo importante all'interno del quadro normativo della *governance* degli intermediari ¹³³.

Una versione estrema dei regimi di *governance* che si basano sul ruolo svolto dalle agenzie governative sono i Paesi che prevedono requisiti di licenza. In Vietnam, ad esempio, i fornitori di siti di *social networking online* e di siti *web* di notizie generali devono ottenere una licenza dal governo prima di poter offrire tali servizi ¹³⁴.

I regimi incentrati sul ruolo delle corti sono caratteristici dei Paesi democratici, mentre i contesti normativi degli intermediari incentrati sul ruolo delle agenzie sono più diffusi nei Paesi con uno stato di diritto limitato. Il regime di governo degli Stati Uniti, con la sua forte dipendenza dalle corti giudiziarie, è all'estremità opposta dell'ampio spettro di casi ¹³⁵ rispetto alla Thailandia, che attua uno stretto controllo sugli intermediari *online* attraverso il National Council for Peace and Order ¹³⁶. Inoltre, i regimi di *governance* basati sulle corti svolgono un ruolo particolarmente importante per quanto riguarda le questioni relative al *copyright*, in quanto anche alcuni Paesi con un coinvolgimento di agenzie governative relativamente forte in questioni non di *copyright* si rivolgono ai tribunali in questo settore, come illustra il caso della Corea ¹³⁷.

Ma anche in Paesi con regimi ampiamente incentrati sul ruolo delle corti giudiziarie, i contorni potrebbero essere offuscati. Mentre la *governance* degli intermediari negli Stati Uniti si basa fortemente sulle corti, le agenzie governative possono svolgere un

¹³³ Si veda: K.S. PARK, *Intermediary Liability - Not Just Backward but Going Back, The Global Network of internet & Society Research Centers - Online Intermediaries Case Studies Series*, 2015, par. II.C, disponibile al link: https://publixphere.net/i/noc/page/OI_Case_Study_Intermediary_liability_Not_Just_Backward_but_Goin_g_Back.

¹³⁴ Si veda: T. NGUYEN, *Roles and Liabilities of Online Intermediaries in Vietnam - Regulations in the Mixture of Hope and Fear, The Global Network of internet & Society Research Centers - Online Intermediaries Case Studies Series*, 2015, par. II.A,

disponibile al link: https://publixphere.net/i/noc/page/OI_Case_Study_Roles_and_Liabilities_of_Online_Intermediaries_in_Vietnam.

¹³⁵ Cfr.: A. HOLLAND, C. BAVITZ, J. HERMES, A. SELLARS, R. BUDISH, M. LAMBERT, N. DECOSTER, *Intermediary Liability in the United States*, cit.

¹³⁶ Si veda: P. RAMASOOTA, *Online Intermediary Liability in Thailand*, cit., par. II.C-II.D.

¹³⁷ Si veda di nuovo: K.S. PARK, *Intermediary Liability - Not Just Backward but Going Back*, cit., par. III.D.

ruolo preminente, almeno nel momento in cui si tratta dell'esecuzione, come dimostra il ruolo del governo statale nel contesto della Sezione 230 CDA ¹³⁸. Allo stesso modo, le agenzie governative sotto forma di autorità per la protezione dei dati sono attori importanti nell'UE quando si tratta di *governance* degli intermediari online ¹³⁹. In Asia, invece, diversi Paesi danno direttamente al governo o alle agenzie il potere di attuare le disposizioni di legge sulla responsabilità degli intermediari.

IV.2. *Regolazione contestuale.*

I regimi della responsabilità su internet possono servire da modello per la regolazione contestuale. Le leggi non regolano il comportamento di un operatore o di un intermediario vietando o ordinando direttamente un comportamento specifico ¹⁴⁰. Piuttosto, il nucleo centrale di un regime di responsabilità è generalmente costituito da un insieme di condizioni in base alle quali l'operatore sarà ritenuto responsabile per il contenuto prodotto da terze parti.

A seconda dei meccanismi di applicazione e di attuazione, questi regimi possono portare alla formazione di strutture di *governance* specifiche all'interno dell'organizzazione operativa di un intermediario, basti pensare ad una procedura di notifica e rimozione finalizzata a gestire i conflitti tra gli utenti di una piattaforma *online*. La maggior parte dei Paesi esaminati nella ricerca non governa direttamente gli intermediari, ma piuttosto li governa indirettamente attraverso meccanismi di regolazione contestuale.

Sebbene in alcune giurisdizioni, come quella della Thailandia, esistano dei regimi di licenza, è interessante notare come tali meccanismi vengono meno utilizzati per la regolazione diretta, intesa in senso tradizionale — ad esempio tramite la determinazione delle condizioni di licenza — ma piuttosto vengano utilizzati come meccanismi di applicazione ¹⁴¹.

L'esito di tale regolazione indiretta dipende molto dagli incentivi e dai disincentivi creati dal sistema. Per il funzionamento di un regime di *governance* degli intermediari, la scelta dei giusti incentivi è fondamentale. Innanzitutto, questo è vero per l'operatore dell'intermediario. Il caso della Corea dimostra che questo è un compito difficile nel complesso ambiente definito dalla regola-

¹³⁸ Cfr. ancora: A. HOLLAND, C. BAVITZ, J. HERMES, A. SELLARS, R. BUDISH, M. LAMBERT, N. DECOSTER, *Intermediary Liability in the United States*, cit., p. 6.

¹³⁹ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 11-12.

¹⁴⁰ Si veda: R. BALDWIN, M. CAVE, M. LODGE, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2012, p. 105 ss.

¹⁴¹ Cfr. di nuovo: P. RAMASOOTA, *Online Intermediary Liability in Thailand*, cit., par. III.

zione di internet. La clausola della legge coreana che menziona le “azioni temporanee” crea un incentivo per l’operatore di un intermediario a rimuovere il contenuto dopo avere ricevuto la notifica, indipendentemente dal fatto che il contenuto sia legale o illegale. Anche se questo non sembra essere l’intento della legge, è razionale che gli intermediari agiscano in tal modo se vogliono evitare la responsabilità ¹⁴².

In India, nel 2015, la Corte Suprema ha emesso una sentenza storica riguardante la costituzionalità di diverse disposizioni dell’Indian Information Technology Act, che erano state criticate per aver creato degli incentivi a rimuovere tutto il contenuto — illegale o legale — in caso di notifica. La Corte Suprema ha statuito che gli standard vaghi per bloccare e rimuovere i contenuti *online* sono incostituzionali. Inoltre, il blocco dei contenuti deve essere imposto solo mediante un provvedimento motivato di un organo giudiziario, amministrativo o governativo e deve essere trasparente ¹⁴³.

Tale riflessione sugli incentivi si è già concentrata sui diversi attori di un determinato modello di *governance*. Osservare la struttura di *governance* in generale, così come emerge — o è almeno influenzata — dal regime di responsabilità, rivela la struttura delle regole ed il ruolo dei diversi attori nel medesimo regime. In molti casi la struttura non sembra essere il risultato di una strategia normativa, ma il prodotto dell’interazione di diverse azioni ¹⁴⁴.

Questo racconta, altresì, la storia del ruolo svolto da un altro attore del regime di *governance*: le corti. Mentre la sentenza della Corte di giustizia sui motori di ricerca è un caso assai particolare,

¹⁴² Si veda ancora: K.S. PARK, *Intermediary Liability - Not Just Backward but Going Back*, cit., par. III.B-III.C.

¹⁴³ Si veda: G. FROSIO, *Landmark Intermediary Liability Decision from the Indian Supreme Court*, 27 March 2015, disponibile al link: <http://cyberlaw.stanford.edu/blog/2015/03/landmark-intermediary-liability-decision-indian-supreme-court>.

¹⁴⁴ Si prenda ad esempio l’attuazione della sentenza della CGUE sul caso Costeja. Qualsiasi decisione del motore di ricerca può, naturalmente, essere soggetta al controllo da parte del responsabile della protezione dei dati o dei tribunali, tuttavia, la decisione iniziale rimane del motore di ricerca. Non solo, in assenza di criteri più dettagliati — nella direttiva o nel ragionamento della Corte — su come bilanciare l’interesse della persona che vuole rimuovere un collegamento e l’interesse del proprietario della rispettiva pagina web o del pubblico in generale per avere accesso alla pagina web, Google ha dovuto elab-

borare regole anche su come risolvere tali conflitti e bilanciare i diritti coinvolti. Di fatto, la CGUE ha creato una procedura obbligatoria di notifica e rimozione, le cui regole sono governate dai motori di ricerca. Solo l’Article 29 Data Protection Working Party, come menzionato sopra, ha successivamente fornito delle linee guida sull’attuazione della sentenza della CGUE, cit. Cfr.: D. KROSLAK, *Practical Implementation of the Right to Be Forgotten in the Context of the Google Spain Decision*, in *Communication Today*, 2015, Vol. 6, No. 1, p. 58 ss., disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808392; A. KUCZERAWY, J. AUSLOOS, *European Union and Google Spain, The Global Network of internet & Societies Research Centers - Online Intermediaries Case Studies Series*, 2015, disponibile al link: https://publixphere.net/i/noc/page/OI_Case-Study_European_Union_and_Google_Spain; E. LEE, *The Right to Be Forgotten v. Free Speech*, in *I/S: A Journal of Law and Policy for the*

in vari Paesi le singole decisioni delle corti sono molto rilevanti nel dare forma al regime di *governance* degli intermediari. Tuttavia, le corti con le loro procedure e con i loro strumenti per acquisire ed elaborare le conoscenze non sono progettate per anticipare gli effetti secondari dei loro giudizi. Gli incentivi creati dalle sentenze e la struttura di governance che ne deriva non possono essere anticipati facilmente dalle corti.

Il fatto che il procedimento di *notice and take down* sia diventato molto “di moda” nel trattare i conflitti tra gli utenti di una piattaforma che opera quale intermediario è stato criticato dal punto di vista normativo, nella misura in cui la procedura diventi un test obbligatorio circa la responsabilità degli intermediari. Il relatore speciale delle Nazioni Unite sulla libertà di espressione Frank La Rue ha chiaramente affermato che un operatore di un intermediario non dovrebbe essere messo in condizione di dover decidere se rimuovere il contenuto o meno; dovrebbe spettare ad un tribunale indipendente o ad un altro organismo indipendente il potere di giudicare la legalità o l'illegalità dei contenuti resi disponibili ¹⁴⁵.

Due aspetti della procedura di *notice and take down* sembrano essere maggiormente significativi. Il primo è il *design* della procedura; i modelli vanno dall'assenza di requisiti procedurali ai modelli con procedure predefinite in una legge locale, come quello stabilito dall'amministrazione in India ¹⁴⁶. L'altro aspetto significativo è il trattamento del gestore del sito *web* interessato e l'interesse generale per un facile accesso alle informazioni *online*. Solo molto raramente è previsto l'obbligatorio di avvisare l'operatore della pagina *web* prima che si verifichi la rimozione di un contenuto ¹⁴⁷, oppure vi è una procedura di appello strutturata attivata dall'operatore in questione. A seconda della natura del reclamo, il procedimento adottato dall'intermediario, per gestire le notifiche, può consistere in un sistema automatico come quello Content ID di YouTube, che consente a YouTube di identificare il contenuto protetto da *copyright* e di rimuoverlo, o in un sistema manuale, come la procedura che ha adottato Google per gestire le oltre 670.000 richieste che a partire dalla fine di ottobre 2014

Information Society, 2015, Vol. 12, No. 1, p. 85 ss., disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2651141, e Id., *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 2015, in *U.C. Davis L. Rev.*, 2016, Vol. 49, p. 1017 ss., disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2636856.

¹⁴⁵ Si veda: F. LA RUE, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Op-*

nion and Expression, United Nations Office of the High Commissioner of Human Rights, April 2013, disponibile al link: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

¹⁴⁶ Si veda: C. ARUN, S. SINGH, *Online Intermediaries in India*, cit., p. 5.

¹⁴⁷ Cfr.: U.S. 17 U.S.C. 512(g)(2)(A) (g) Replacement of Removed or Disabled Material and Limitation on Other Liability.

hanno fatto seguito alla sentenza della CGUE. In alternativa, esistono sistemi ibridi in cui viene gestita automaticamente una grande quantità di contenuti potenzialmente protetti, ma i casi difficili vengono trattati manualmente ¹⁴⁸.

IV.3. Coregolazione.

Un ulteriore e più semplice esempio di regolazione indiretta è data dall'aumento della diffusione degli approcci di coregolazione che vengono sempre più spesso adottati sia negli Stati Uniti che nell'Unione Europea.

Ad esempio, molte delle preoccupazioni sollevate dagli intermediari di internet hanno riguardato la *privacy* a causa degli enormi set di dati che questi ultimi acquisiscono. Negli Stati Uniti, la Federal Trade Commission ha stipulato degli accordi con Facebook, Google, Snapchat e Twitter, in base ai quali tali società pagano per effettuare dei controlli indipendenti sulla *privacy* da condurre su base biennale per venti anni. Questi controlli sono volti a garantire che tali imprese si comportino secondo quanto da loro stesse promesso, in relazione alla *privacy*, nei termini di utilizzo. Nell'Unione Europea, il Regolamento generale sulla protezione dei dati ¹⁴⁹ promuove l'uso dei codici di condotta e delle certificazioni al fine di: a) garantire il rispetto dei requisiti previsti dal provvedimento; b) segnalare agli interessati e ai regolatori che una determinata organizzazione è conforme al regolamento sulla *privacy*; c) offrire la supervisione di terze parti come altra forma di controllo sulle pratiche in uso per gestire e processare i dati ¹⁵⁰.

Nella stessa prospettiva, Facebook, Google, Microsoft e Twitter sono stati sempre più spesso chiamati a bloccare gli *account* dei *social media* di entità presumibilmente associate al terrorismo internazionale o all'incitamento all'odio.

Alla riunione dei Ministri degli interni del G7 che si è svolta nel corso del mese di ottobre 2017, in Italia, i paesi del G7 e Google, Microsoft, Facebook e Twitter hanno convenuto che le società di internet debbano continuare a svolgere un ruolo proattivo e ad

¹⁴⁸ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 6-8.

¹⁴⁹ Regolamento (EU) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR), cit.

¹⁵⁰ GDPR, articoli 40-41. È probabile che i codici di condotta siano ben presenti nei piani aziendali per i legittimi trasferimenti di dati transfrontalieri. Se dovessero

rivelarsi efficaci, potrebbero inoltre essere alla base di meccanismi di trasferimento dati globali, coerenti con i sistemi già utilizzati negli Stati Uniti e nell'ambito dell'Asia Pacific Economic Cooperative, e con minori costi di conformità alla *privacy* in tutto il mondo. Si veda: R. Heimes, *Top 10 operational impacts of the GDPR: Part 9 - Codes of conduct and certifications*, febbraio 2016, disponibile al link: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications>.

assicurare azioni decisive nel rendere le loro piattaforme più ostili al terrorismo sostenendo, altresì, azioni volte a responsabilizzare i partner della società civile nello sviluppo di narrative alternative *online*. In particolare, i partecipanti hanno convenuto che fosse necessario aumentare gli sforzi congiunti in quattro aree principali: *i*) uso della tecnologia automatizzata per la rapida individuazione e rimozione di contenuti terroristici e la prevenzione della loro ulteriore diffusione, *ii*) condivisione delle migliori pratiche e della tecnologia per migliorare la capacità di resistenza delle piccole imprese, *iii*) migliorare lo sviluppo delle conoscenze di base attraverso la ricerca e lo sviluppo e *iv*) autorizzare i partner della società civile a sviluppare narrative alternative ¹⁵¹.

Nell'Unione Europea, il summenzionato Codice di condotta sull'illecito incitamento all'odio include una serie di impegni presi dalle stesse società per combattere la diffusione di tali contenuti. L'attuazione del Codice è monitorata dalla Commissione Europea attraverso un meccanismo di valutazione realizzato dalle organizzazione non governative e dalle istituzioni di 24 Stati Membri.

IV.4. Enforcement.

Le sezioni precedenti hanno illustrato chiaramente come i governi non solo stabiliscano le condizioni generali — e a volte specifiche — in cui operano gli intermediari *online*, ma diventino anche lo strumento attraverso il quale attuare e favorire l'applicazione di un determinato modello di *governance*.

A livello più astratto, l'analisi comparativa dei diversi regimi di *governance* indica che le strutture e gli incentivi creati dai governi, sia che siano progettati o che derivino dalla semplice prassi, sono fondamentali per comprendere la conformità e le modalità di attuazione del quadro normativo relativo alla *governance* degli intermediari *online*.

Una questione chiave identificata attraverso la presente ricerca riguarda la creazione, da parte di un particolare governo, di una struttura di incentivi simmetrica o asimmetrica per far eliminare o meno i contenuti agli intermediari *online* al fine di evitare la responsabilità. Negli Stati Uniti, ad esempio, la Sezione 230 del CDA fornisce una struttura simmetrica di incentivi nel senso che le corti sono state coerenti nel lasciare gli intermediari *online* immuni dalla responsabilità, a condizione che questi ultimi non siano gli autori del contenuto — indipendentemente dal fatto che lo eliminino, lo lascino pubblicato, o persino se ripristinano il

¹⁵¹ Si veda: Joint Press Release on countering the terrorist threat on the internet following the G7 Interior Ministers' meeting (Ischia, 20 ottobre 2017), disponibile al

link: http://www.g7italy.it/sites/default/files/documents/G7%20Press%20release%20EN_0.pdf.

contenuto che è stato rimosso ¹⁵². Al contrario, i regimi di *governance* in India, Corea e Thailandia hanno creato strutture di incentivazione asimmetrica, in cui gli intermediari sono spinti ad eliminare il contenuto al fine di evitare la responsabilità, anche se ciò si traduce in sovra-conformità ¹⁵³.

Una seconda osservazione relativa agli incentivi asimmetrici e ai conseguenti livelli di conformità riguarda gli intermediari *online* locali e internazionali. L'analisi indica che nei casi in cui i requisiti di licenza si applicano *de facto* solo agli intermediari locali ma non a quelli internazionali, gli intermediari locali sono portati a garantire una maggiore conformità, o forse anche un'eccessiva conformità, alle richieste governative. I casi dell'India, della Thailandia e del Vietnam sono i migliori esempi che evidenziano questa asimmetria tra gli attori locali e quelli internazionali. In terzo luogo, la ricerca illustra non solo i diversi regimi e le strategie di applicazione ¹⁵⁴, compresi gli incentivi e gli attori coinvolti, ma indica anche la gamma di tecniche di applicazione che possono essere utilizzate come parte dei diversi modelli di *governance*. Le sezioni precedenti hanno già evidenziato il ruolo dei requisiti di licenza come strumento di applicazione della normativa, in particolare nei casi di India, Thailandia e Vietnam ¹⁵⁵.

Un altro tema interessante che emerge dall'analisi fin qui svolta riguarda il ruolo degli algoritmi nell'applicazione della legge. Il fenomeno della conformità degli algoritmi computazionali è diventato più visibile nel contesto statunitense, in cui il *software* svolge un ruolo chiave nell'affrontare i problemi su larga scala di violazione del *copyright* su piattaforme di contenuti create dagli utenti, in particolare YouTube ¹⁵⁶. Gli algoritmi svolgono un ruolo non solo negli "ordini privati" sul modello YouTube, ma anche quando si tratta di obblighi di monitoraggio e filtraggio imposti dal governo, come dimostrano i casi della Thailandia e dell'India ¹⁵⁷.

¹⁵² Si veda: A. HOLLAND, C. BAVITZ, J. HERMES, A. SELLARS, R. BUDISH, M. LAMBERT, N. DECOSTER, *Intermediary Liability in the United States*, cit., p. 5-7.

¹⁵³ Si vedano: C. ARUN, S. SINGH, *Online Intermediaries in India*, cit., par. II.C.; A. PADMANABHAN, *Give Me My Space and Take Down His*, cit., p. 15-16; P. RAMASOOTA, *Online Intermediary Liability in Thailand*, cit., par. III; D. O'BRIEN, G. GEBHART, *The Amended Computer Crime Act and the State of internet Freedoms in Thailand*, cit.

¹⁵⁴ Ad esempio, *ex post* contro *ex ante*.

¹⁵⁵ Si veda: See: C. ARUN, S. SINGH, *Online Intermediaries in India*, cit., par.

II.A.; P. RAMASOOTA, *Online Intermediary Liability in Thailand*, cit., par. IV.B; T. NGUYEN, *Roles and Liabilities of Online Intermediaries in Vietnam - Regulations in the Mixture of Hope and Fear*, cit., par. II.A.

¹⁵⁶ Si veda: A. HOLLAND, C. BAVITZ, J. HERMES, A. SELLARS, R. BUDISH, M. LAMBERT, N. DECOSTER, *Intermediary Liability in the United States*, cit., p. 31-34.

¹⁵⁷ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 12-14.

V. CONSIDERAZIONI FINALI.

V.1. *Interazioni tra responsabilità degli intermediari, sviluppo, cultura e diritti fondamentali.*

La ricerca evidenzia dunque come una prospettiva molto rilevante dalla quale analizzare i regimi di *governance* degli intermediari sia il processo di sviluppo del quadro normativo nazionale ed il suo contesto culturale. Una prima osservazione, piuttosto ovvia, è che il dibattito politico nei diversi Paesi ha riconosciuto l'importanza della disciplina degli intermediari in diversi momenti. Gli Stati Uniti sono stati rapidi nell'affrontare il problema e, di conseguenza, il loro regime è in vigore da diversi anni e si è dimostrato efficace ed in grado di favorire l'innovazione. L'Unione Europea ha adottato un approccio unitario alla questione, che in effetti ha funzionato abbastanza bene, nonostante le ricorrenti critiche e le richieste di emendamenti. Altri Paesi stanno ancora progettando un sistema. Nello scenario dell'Asia estremo orientale e dell'Oceania, in particolare, mentre vi sono Paesi in cui esistono alcune forme efficaci di protezione dalla responsabilità degli intermediari, in altri le protezioni attualmente esistenti sono limitate in termini reali o di fatto non efficaci, mentre altri ancora assumono delle posizioni relativamente neutre in materia.

Un aspetto estremamente rilevante sembra essere il contesto culturale. Gli Stati Uniti tradizionalmente basano la loro regolazione su una considerazione condivisa dell'importanza della libertà di espressione; quindi il contesto culturale è la chiave. In Asia, ad esempio, l'esigenza di proteggere l'onore del re in Thailandia è profondamente radicata nella società e deve essere garantita contro la diffamazione *online* e *offline*. Di conseguenza, viene affrontato il ruolo di tutti gli attori, inclusi gli intermediari. I Paesi che aspirano a governare la società più strettamente di una democrazia occidentale affrontano il dilemma di dover trovare un modo per riuscire a governare internet — compresi gli intermediari — senza interferire con l'innovazione e il potenziale economico di internet. Il Vietnam può servire come esempio di un Paese alle prese con un tale equilibrio.

Quello che possiamo vedere nello sviluppo della *governance* degli intermediari *online*, così come in altri settori della regolazione, è che a volte singoli eventi cambiano il percorso di sviluppo. Un evento significativo è risultato ad esempio quello della sentenza della Corte di Giustizia dell'Unione Europea sul caso Costeja, che ha alimentato il dibattito sulla responsabilità degli intermediari a livello europeo e globale. La decisione della Corte di Giustizia ha evidenziato un aspetto chiave dei regimi di *governance* degli intermediari, che è il rapporto tra la responsabilità degli stessi e i diritti costituzionali. La sentenza è stata criticata

per non prendere sufficientemente in considerazione la libertà di espressione e la libertà di informazione ¹⁵⁸.

In Asia, analogamente, il regime di responsabilità è stato contestato a causa di motivi costituzionali in India, e lo stesso è avvenuto in Corea del Sud.

Negli Stati Uniti e non solo, il recente caso Facebook/Cambridge Analytica, a seguito degli articoli di stampa che nel marzo 2018 hanno rivelato come decine di milioni di dati degli utenti di Facebook fossero stati ceduti alla società Cambridge Analytica, ha riportato al centro del dibattito il tema delle responsabilità dei *provider*, con conseguenze ancora imprevedibili ¹⁵⁹.

Almeno due aspetti sono degni di nota quando si tratta dei diritti costituzionali connessi alla responsabilità degli intermediari. Il primo è che i sistemi di responsabilità non possono confidare sull'editore di una pagina *web* per difendere il suo diritto alla libertà di espressione se questi non viene informato del *takedown* della pagina, se è costoso rispondere, o se l'editore non è interessato a perseguire la questione. Inoltre, l'interesse generale ad un facile accesso alle informazioni su internet non è protetto dalle clausole sulla libertà di informazione perché è definito come un diritto soggettivo, non oggettivo. Tuttavia, alcune corti hanno sottolineato il ruolo di internet in questo senso ¹⁶⁰.

Infine, per quanto riguarda gli attori, può esservi uno squilibrio a seconda che vi sia, da una parte, una persona molto interessata a rimuovere il contenuto, dall'altra, una persona che potenzialmente non lo sia. In secondo luogo, anche il ruolo dell'intermediario è rilevante. Da un lato, l'operatore potrebbe godere dei privilegi connessi alla libertà di espressione — ma le condizioni in cui questo caso si possa verificare non sono facili da interpretare. Dall'altra parte, l'operatore potrebbe essere una potente entità che decide che l'accessibilità ad un'informazione debba essere vincolata al rispetto della libertà di espressione anche per gli utenti ¹⁶¹.

¹⁵⁸ Si veda sopra al paragrafo IV.2.

¹⁵⁹ Finora il caso ha dato luogo all'avvio di un'inchiesta da parte della Federal Trade Commission e l'audizione del CEO di Facebook Marc Zuckerberg innanzi al Congresso, nonché a livello europeo ad analoghi avvio di un'indagine da parte dell'Article 29 Working Party e richiesta di audizione del CEO da parte del Parlamento europeo.

¹⁶⁰ Si veda, ad esempio: ECHR, *Times Newspapers Ltd v. the United Kingdom* (nos. 1 and 2), 10 March 2009, application nos. 3002/03 and 23676/03, [2009] EMLR 14, § 27, disponibile al link: <http://www.5rb.com/case/times-newspapers-ltd-nos-1-and-2-v-th>

e-united-kingdom; e *Id.*, Ashby Donald and Others v. France, 10 January 2013, application no. 36769/08, § 34, disponibile al link: <http://echrblog.blogspot.it/2013/01/copyright-vs-freedom-of-expression.html>.

¹⁶¹ Cfr.: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 15; E. VOLOKH, D.M. FALK, *First Amendment Protection for Search Engine Search Results*, *UCLA School of Law Research Paper* No. 12-22, disponibile al link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055364.

V.2. *Efficienza economica e considerazioni di policy.*

Limiti adeguati alla responsabilità degli intermediari hanno avuto un ruolo fondamentale nello sviluppo di internet. In effetti, richiedere agli intermediari *online* di monitorare ogni singola parte del contenuto o imporre loro ampie responsabilità ostacolerebbe l'innovazione, la libertà di espressione e la *privacy*.

In tale prospettiva, questa ricerca ha evidenziato l'importanza del contesto culturale e politico, che non si riflette solo nelle rispettive norme giuridiche volte a regolare gli intermediari o a fornire loro *safe harbor*, ma si esprime anche attraverso diversi punti di vista e percezioni riguardo alla loro funzione socio-economica.

Diversi approcci culturali e politici rispetto agli intermediari *online* hanno condotto a differenti considerazioni della loro funzione sociale e quindi a diverse soluzioni regolatorie. Mentre negli Stati Uniti e parzialmente nell'Unione Europea¹⁶², nonché in alcuni Paesi dell'Asia estremo orientale e dell'Oceania, sono stati introdotti regimi di *safe harbor* più o meno efficaci volti a preservare l'utilità degli intermediari rispetto alla libertà di espressione e all'innovazione, oppure gli ordinamenti sono rimasti neutrali rispetto alla disciplina della responsabilità degli stessi, in alcuni Paesi dell'Estremo oriente sono state adottate normative che hanno previsto requisiti di licenza o localizzazione a fini di sorveglianza, ovvero obblighi ampi di eliminazione dei contenuti al fine di poter evitare la responsabilità, nonostante ciò possa tradursi in sovra-conformità con lesione di altri diritti fondamentali.

D'altronde, molte delle caratteristiche dei vari approcci di *governance* degli intermediari difficilmente possono essere comprese senza prendere in considerazione il contesto economico, in connessione con le caratteristiche demografiche e con le relative modificazioni.

Regolare gli intermediari è efficiente, nel senso che gli intermediari possono affrontare il danno ad un costo inferiore rispetto alle alternative. Data la decentralizzazione di internet, sarebbe impossibile o almeno molto difficile per le persone perseguire chi le diffama o per i titolari di *copyright* citare individualmente ciascun trasgressore. Dove c'è un diritto dovrebbe esserci qualche

¹⁶² Sul punto, si vedano: A. PIERUCCI, *La responsabilità del provider per i contenuti illeciti della Rete*, in *Rivista critica del diritto privato*, 2003, p. 143; L. BUGIOLACCHI, *Verso un sistema della responsabilità civile dell'internet provider? Considerazioni su un recente "anteprojecto" spa-*

gnolo di recepimento della direttiva 2000/31/CE sul commercio elettronico, in *Responsabilità civile e previdenza*, 2003, p. 293; G. BELLÌ, *La responsabilità civile dei service providers*, in *La responsabilità civile*, 2011, p. 693.

rimedio, e aumentare la responsabilità sembra essere la migliore alternativa.

Tuttavia, devono essere presi in considerazione anche altri elementi importanti, come il rischio di danneggiare l'innovazione, gli investimenti e l'accesso ai mercati digitali, e quindi di soffocare i benefici di internet per la società. L'innovazione tecnologica dipende in larga misura dall'avere quadri normativi chiari. Anche laddove la regolazione attuale sia relativamente chiara, potrebbe essere ancora onerosa da implementare, specialmente per i piccoli, medi o nuovi imprenditori, che potrebbero trasferire i costi sugli utenti finali, e le regole potrebbero diventare rapidamente obsolete via via che la tecnologia evolve.

Più in generale, l'analisi ha rivelato una serie di dinamiche e di sfide di *policy* trasversali, tra cui il problema della definizione di intermediario *online*, la questione dei diversi tipi di intermediari, la creazione di sistemi di *notice and takedown*, i costi dell'*enforcement*, ecc.

Circa il ruolo dei governi, l'analisi suggerisce che possono svolgere tre funzioni fondamentali ossia abilitare, uniformare o vincolare. Analizzando l'assetto istituzionale di base dei diversi regimi di *governance*, i vari Paesi, a seconda delle questioni in gioco, adottano delle strategie e tecniche normative che o adottano un sistema basato sulle corti o fanno affidamento sulle agenzie governative, con contorni tra i due modelli spesso sfumati¹⁶³.

Al fine di comprendere e valutare le caratteristiche e le *performance* dei vari modelli o approcci di *governance*, la ricerca ha evidenziato i ruoli chiave: a) del bilanciamento dei diritti fondamentali e degli obiettivi di *policy*; b) dell'analisi degli incentivi dei diversi attori che fanno parte del contesto nel quale operano gli intermediari, tenendo conto anche dell'interazione tra loro.

La questione degli incentivi, infatti, gioca un ruolo decisivo quando si tratta di analizzare le questioni dell'adempimento e dell'*enforcement*, compresa la questione dell'eccessivo adempimento in caso di regolazione asimmetrica. Inoltre, a questo proposito, si deve anche considerare che le società hanno degli incentivi di mercato per affrontare i reali rischi in quanto i consumatori non utilizzeranno più i loro servizi se il contesto è inadeguato, ed in alcuni ambiti hanno anche degli incentivi giuridici, come ad esempio nel contesto del *copyright* tramite il meccanismo di *notice and takedown* o di *notice and action*¹⁶⁴.

¹⁶³ Si veda: U. GASSER, W. SCHULZ, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, cit., p. 16.

¹⁶⁴ Anche laddove l'immunità per gli intermediari può sembrare illimitata, po-

trebbe esservi una discussione sugli incentivi giuridici. Ad esempio, negli Stati Uniti, il CDA 230 è spesso considerato un'immunità generale per gli *host* di contenuti. Tuttavia, un terzo dei casi in cui è stata tentata una difesa ex CDA 230 è fallita. Si veda:

In uno scenario così variegato, tuttavia, l'analisi comparatistica degli elementi fondamentali dei quadri normativi relativi agli intermediari *online*, dei vari *stakeholder* e delle relative questioni in gioco rivela alcuni elementi chiave da prendere in considerazione per quanto riguarda i modelli di *governance* degli intermediari. Queste sono, in particolare:

i) Caratteristiche e funzioni degli intermediari *online*. Gli intermediari costituiscono un fenomeno complesso ed allo stesso tempo sono un *driver* nonché rispecchiano la rivoluzione digitale. Dal punto di vista funzionale, gli intermediari *online* pongono prima di tutto delle questioni definitorie, poiché sfidano le nozioni tradizionali di ciò che è qualificato come intermediario: infatti, gli intermediari online non sono la fonte creativa dei contenuti, sono sempre più coinvolti nella loro diffusione, combinazione, ecc.

Anche l'economia degli intermediari è un elemento chiave da considerare nell'analisi, data la presenza di forti effetti di rete e di mercati a due versanti come fattori chiave per il successo aziendale e il relativo benessere sociale.

La ricerca evidenzia anche l'importanza di una profonda comprensione funzionale dei ruoli degli intermediari *online* quando si cerca di elaborare un quadro normativo adeguato. La maggior parte dei dibattiti sulla responsabilità degli intermediari finisce in ultima analisi sulla capacità di una parte di eliminare il contenuto di qualcun altro. D'altronde, si è rilevato che: a) gli intermediari non sono nella posizione di giudicare la legalità del materiale pubblicato in rete; b) spesso non vi sono limiti chiari ai modi in cui un simile metodo possa essere applicato, dalla rimozione dei contenuti, agli obblighi di monitoraggio dannosi che limitano la libertà di espressione e invadono la *privacy*, fino alla rimozione dei contenuti leciti¹⁶⁵.

ii) Dimensione normativa e costi complessivi della regolazione. Recentemente, l'interazione tra la responsabilità degli intermediari e l'economia digitale, e sempre più anche l'etica digitale, ha guadagnato un'attenzione significativa in tutte le giurisdizioni. Come menzionato nel corso della ricerca, vista la complessità dell'ecosistema digitale, la regolazione degli intermediari *online* è considerata efficiente e sembra comportare una riduzione dei costi. Persino gli architetti di sistemi con regimi di

D.S. ARDIA, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, in *Los Angeles Law Review*, 2010, Vol. 43, No. 2, p. 373 ss., disponibile al link: <http://ssrn.com/abstract=1625820>.

¹⁶⁵ In termini di argomentazione economica qui, dal momento che gli intermediari

online non internalizzano tutti i vantaggi dei vari tipi di contenuti pubblicati sulle loro piattaforme, essi non hanno incentivi sufficienti per frenare la sovrabbondanza. Si veda: A. HAMDANI, *Who's Liable for Cyberwrongs*, disponibile al link: <http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Hamdani.pdf>.

safe harbor piuttosto ampi sembrano concentrarsi principalmente sul vantaggio economico della regolazione degli intermediari. Dal punto di vista etico, quindi, dall'abilità si passa al dovere; gli intermediari hanno la responsabilità etica di eliminare i danni e tale responsabilità dovrebbe essere tradotta in legge.

Sebbene le argomentazioni economiche ed etiche siano naturalmente importanti nei dibattiti di *policy*, si dovrebbe anche enfatizzare la dimensione normativa, in particolare l'impatto dei diversi regimi di governo sui diritti fondamentali. Tale prospettiva multidisciplinare ma incentrata sulla normativa evidenzia il rischio che l'eccesso di regolazione possa produrre un impatto negativo sui diritti fondamentali degli utenti, nonché sull'innovazione e sull'economia digitale. La ricerca suggerisce anche l'importanza di tenere conto dei costi meno visibili degli interventi, come il rischio di rafforzare degli intermediari già potenti costringendoli a fare delle scelte relative ai contenuti che dovrebbero essere affidate alle autorità pubbliche.

iii) Ampia gamma di meccanismi di regolazione o autoregolazione. La ricerca ha mostrato che gli intermediari sono regolati da diversi meccanismi, direttamente e indirettamente, *ex ante* ed *ex post*, attraverso degli obblighi "pesanti" o "leggeri". Inoltre, l'autoregolazione è spesso molto rilevante e più efficace. Diversi attori seguono approcci differenti, hanno diversi tipi di risorse a loro disposizione e mostrano vari livelli di esperienza. Al fine di analizzare e valutare lo stato della regolazione e dei suoi effetti, è fondamentale avere una visione olistica e considerare tutti gli elementi rilevanti e la loro interazione.

iv) Metodo comparatistico e apprendimento reciproco. Nonostante tutte le peculiarità dei diversi contesti, la ricerca rivela problematiche e sfide simili tra i Paesi che hanno adottato dei sistemi di *notice and takedown*, con problemi come la definizione dei requisiti per le notifiche, se e come informare il titolare dei contenuti interessati, la supervisione normativa, ecc. Pertanto, la ricerca suggerisce di fatto un grande potenziale per l'apprendimento transnazionale, integrando l'approccio operativo degli intermediari, che tendono ad assumere una prospettiva globale quando progettano i loro servizi o prodotti, la *governance* interna e gli strumenti di autoregolamentazione.

v) Efficacia dell'attribuzione di maggiori poteri agli utenti. L'attenzione agli intermediari non deve mettere da parte l'importanza di promuovere strumenti per potenziare gli utenti e l'educazione alla responsabilità e all'autotutela dei diritti *online*. Persone diverse hanno valori, punti di vista e preferenze diversi riguardo ai loro diritti e dare loro il controllo può essere un modo molto efficace per garantire i diritti individuali senza ostacolare a) le libertà fondamentali quali la libertà di espressione e la libertà di condurre un'impresa; o b), ostacolare l'innovazione tecnolo-

gica, l'accesso ai mercati digitali e il relativo benessere socio-economico.

Abstract

Online intermediary liability is the concept of holding an online platform responsible for the illegal or harmful acts of Internet users.

Who counts as an “intermediary” is relatively abstract, but it often includes access providers, search engines, hosting platforms, email providers, payment processors, social networks and many more.

The commonality between these entities is that they enable others to do things on the Internet, they are intermediaries in the sense that they provide services that allow for user A to interact with user B in different ways.

This research provides a comparative overview of the multi-fold approaches of the Far East and Oceania countries regarding online intermediary liability, through a western perspective inspired by the US and EU legal frameworks.

The outcome of the analysis are some key points to be taken into account in dealing with such a multi-faceted and dynamic issue.