Luiss
Business
School

Ministero dello
sviluppo economico

UIBM

Digital Services Act

Profili di responsabilità e strategie di lotta alla contraffazione online dei diritti di proprietà industriale

13 Dicembre 2021

LUISS

Sommario

Premessa *5*

Executive summary *6*

Introduzione. Tecnologie digitali ed impatto della contraffazione online. *12*

1. Il quadro regolamentare vigente: Direttiva e-commerce, sistemi di filtraggio e misure di blocco dei siti internet. *16*

2. La proposta di Digital Services Act della Commissione europea *24*

2.1 Ambito di applicazione e definizioni rilevanti **25**

2.1.1 Ambito di applicazione territoriale. 25

2.1.2 Ambito di applicazione soggettivo: le nuove definizioni di "servizi intermediari" e "piattaforme" del DSA. 27

2.2 La responsabilità delle piattaforme: esenzioni e nuovi obblighi. **28**

2.2.1 Esenzioni. 29

2.2.2 Obblighi applicabili a tutti i prestatori di servizi intermediari. 32

2.2.3 Disposizioni aggiuntive applicabili ai prestatori di servizi di hosting, comprese le piattaforme online. 34

2.2.4 Disposizioni aggiuntive applicabili alle piattaforme online 36

2.2.5 Obblighi supplementari a carico delle piattaforme online di dimensioni molto grandi per la gestione dei rischi sistemici 41

2.2.6 Altre disposizioni relative agli obblighi in materia di dovere di diligenza. 43

2.3 Attuazione, cooperazione, sanzioni ed esecuzione **45**

2.4 Osservazioni preliminari sulla compliance normativa al DSA per le diverse tipologie di piattaforme **53**

2.5 Osservazioni preliminari sul possibile impatto del DSA sui titolari dei diritti di proprietà industriale 56

3. Il dibattito con gli Stakeholders 58

4. Il dibattito istituzionale: punti critici e proposte di modifica 60

5. Le principali questioni oggetto del dibattito rilevanti per l'enforcement dei diritti di proprietà industriale online e l'impatto sugli stakeholders 64

5.1 Obblighi di *stay down*, rischi di blocco eccessivo e ambito soggettivo dei *trusted flaggers*..... 64

5.2 La *good samaritan clause* ed i meccanismi di incentivo per l'autoregolazione 67

5.3 Obblighi di tracciabilità degli utenti professionali e dei prodotti che circolano sulle piattaforme 71

5.4 *Compliance* normativa, approccio basato sul rischio ed obblighi per le microimprese e le piccole imprese.....75

6. Raccomandazioni preliminari di policy.....78

Premessa

Il presente studio è stato proposto, approvato e sviluppato ai sensi dell'Articolo 2 della Convenzione in vigore tra la Luiss e la Direzione Generale per la tutela della proprietà industriale-Ufficio Italiano Brevetti e Marchi (DGTPI-UIBM), firmata in data 27 Gennaio 2021.

Tale convenzione regola i rapporti tra le due istituzioni, nel biennio 2021-2022, rinnovando una collaborazione pluriennale incentrata sulla realizzazione del Master di II livello in "Open innovation & Intellectual property" in collaborazione con l'Università degli Studi di Torino – tramite la SAA School of Management.

In particolare, per il suddetto biennio la DGTPI-UIBM ha valutato l'opportunità di finanziare borse di studio in misura superiore, pari a 20, alle edizioni precedenti al fine di incrementare il numero dei possibili partecipanti alle prossime due edizioni del citato Master, tenuto conto del forte successo riscosso dalle cinque precedenti edizioni; la DGTPI-UIBM ha ritenuto inoltre di promuovere un programma di studio e ricerca su fenomeni inerenti la proprietà industriale e la lotta alla contraffazione con particolare riferimento alle nuove tecnologie digitali e alle nuove frontiere che si aprono per le imprese, in particolare quelle di piccola e media dimensione. Proprio in questo ambito, si posizione il presente studio, denominato "Digital Services Act. Profili di responsabilità e strategie di lotta alla contraffazione online dei diritti di proprietà industriale".

Executive Summary

La proposta di Regolamento Digital Services Act (DSA) licenziata nel Dicembre 2020 dalla Commissione europea mira a riformare la precedente Direttiva sul commercio elettronico (2000/31/CE), le cui disposizioni sono considerate insufficienti a contrastare la circolazione di contenuti illegali e a garantire una disciplina uniforme all'interno dell'Unione europea. Essa si inserisce, inoltre, in un quadro regolamentare più ampio, finalizzato ad accrescere le responsabilità e la trasparenza delle piattaforme digitali in ragione del crescente ruolo da esse svolto su numerosi mercati dell'economia digitale.

Nell'ambito dei contenuti illeciti, la cui circolazione online il DSA mira a prevenire o ad ostacolare in maniera efficace, particolare risalto è attribuito al fenomeno della contraffazione. Come segnalato dall'Impact Assessment che accompagna il DSA e dagli studi rilasciati dall'Organizzazione per la cooperazione e lo sviluppo economico (OECD) e dall'Ufficio europeo per la proprietà intellettuale (EUIPO) il valore complessivo della merce contraffatta in Europa ammonta a 119 miliardi di euro nel 2019 (tra cui piccoli lotti acquistati online attraverso e-commerce). Gli stessi studi evidenziano i costi sostenuti dalle imprese per l'enforcement dei diritti di proprietà industriale online, oltre ad altre possibili conseguenze negative.

A tal fine, pur confermando i principi alla base dell'impianto della Direttiva sul commercio elettronico (ossia (i) la responsabilità degli intermediari online presuppone la conoscenza effettiva del contenuto illecito e (ii) nessun obbligo generale di monitoraggio può essere imposto agli stessi), il DSA introduce una nuova ed ampia serie di obblighi a carico delle piattaforme "a geometria variabile", prevedendo una articolazione differenziata in ragione del ruolo e della dimensione delle stesse (all intermediaries, hosting services, online platforms e very large online platforms). Esso mira, inoltre, ad introdurre un quadro comune per l'enforcement, attraverso un miglior coordinamento tra le Autorità competenti.

Dopo un' analisi dei contenuti della proposta e delle principali differenze tra l'attuale quadro regolatorio (rappresentato dalla Direttiva e-commerce e dalle varie discipline settoriali) e la nuova cornice normativa offerta dal DSA, la presente ricerca discute i possibili impatti della proposta sui principali stakeholders, con focus sulla tutela online dei diritti di proprietà industriale, con

l'obiettivo di elaborare alcune osservazioni ed alcune conclusioni preliminari per contribuire al dibattito in corso nelle sedi istituzionali.

Nel momento in cui il presente Report è stato elaborato il processo di approvazione del DSA non è stato completato, essendo attualmente all'attenzione del Consiglio dell'Unione europea e del Parlamento europeo. Pertanto, il lavoro di analisi svolto ha come riferimento la proposta originaria formulata dalla Commissione europea. In quest'ottica, le conclusioni preliminari, di seguito sinteticamente riassunte, riguardano gli aspetti critici e le questioni più rilevanti emersi con riferimento alla lotta contro la contraffazione dei diritti di proprietà industriale perpetuata online ed hanno la finalità di fornire un contributo al dibattito pubblico in corso nelle sedi istituzionali.

- *Obblighi di sorveglianza e procedure di "notifica e azione"*

Nell'ambito delle disposizioni relative alla responsabilità delle piattaforme, è opportuno che, rispetto alla previsione di un sistema di notice and action e alla possibile introduzione di obblighi di blocco permanente di alcuni contenuti (stay down), rilevanti per la tutela dei diritti di proprietà industriale online, si garantisca il coordinamento con la tutela del diritto d'autore online (con particolare riferimento all'Articolo 17 della nuova Direttiva Diritto d'Autore nel Mercato Unico Digitale - CDSM) e si assicuri il giusto equilibrio con la libertà di espressione, la libertà di concorrenza ed il principio di libera circolazione nel mercato interno.

- *Ambito soggettivo dei trusted flaggers*

Dato il ruolo che i segnalatori attendibili sono chiamati a svolgere nel DSA, è opportuno definire criteri chiari, oggettivi e stringenti al fine di circoscrivere attentamente il perimetro dei soggetti che ambiscono a conseguire tale status. Al contempo, potrebbe essere considerata l'inclusione dei titolari di diritti di proprietà industriale dal novero dei trusted flaggers in presenza di specifiche circostanze.

- *Good samaritan clause*

Ai fini di una maggiore operatività della previsione che estende il beneficio dell'esenzione da responsabilità alle ipotesi in cui gli intermediari intraprendano volontariamente misure proattive tese ad accrescere il loro livello di conoscenza sulle condotte illecite perpetrate sulle loro piattaforme, sarebbe opportuno che la good samaritan clause specificasse in maniera più precisa le azioni volontarie da non disincentivare (e.g. termini e condizioni più stringenti, azioni investigative volte allo specifico scopo di identificare e rimuovere contenuti illeciti, ad es. ove

l'illiceità sia già stata in precedenza accertata), accompagnando tale elencazione alla indicazione di misure di salvaguardia come – ad esempio- la supervisione umana in caso di controlli algoritmici. Appare necessario, infatti, favorire azioni significative da parte del fornitore di servizi, da un lato, e circoscrivere la portata della clausola e/o inserire eventuali ulteriori garanzie per prevenire abusi nei confronti degli utenti delle piattaforme, dall'altro lato.

- *Obblighi di compliance*

Al fine di evitare obblighi sproporzionati di compliance in capo alle imprese che gestiscono servizi di intermediazione, assicurando al contempo la finalità di contrasto all'illegalità online secondo un approccio basato sul rischio, la formulazione di alcune disposizioni potrebbe essere rimeditata. In particolare, l'Articolo 21 della proposta del DSA (che prevede la comunicazione da parte della piattaforma online in caso di sospetto di commissione di un reato grave che comporta una minaccia per la vita o la sicurezza delle persone) necessita di una definizione più precisa della portata dell'obbligo gravante sulle piattaforme.

Nella medesima ottica, sarebbe opportuno specificare meglio portata soggettiva e contenuto degli obblighi di informazione e verifica nell'ambito delle norme sulla tracciabilità degli operatori commerciali (KYBC), anche attraverso la promozione di standard e codici di condotta, seppur mantenendo inalterata la ratio della norma dato l'evidente impatto positivo su consumatori e titolari dei diritti. Si segnala, peraltro, come possa essere ragionevole una estensione dell'ambito soggettivo delle disposizioni KYBC anche oltre gli online marketplaces, tenendo in considerazione i servizi dove più frequentemente sono perpetrate condotte illecite. Inoltre, l'esclusione delle micro e delle piccole imprese dagli obblighi previsti per le piattaforme online potrebbe essere rimeditata. Potrebbe essere opportuno mantenere tale esclusione per obblighi che di fatto impongano oneri sproporzionati di compliance che non sono ragionevolmente esigibili da imprese di siffatte dimensioni, mentre ridimensionarla rispetto ad altri obblighi (come, ad esempio, l'obbligo di tracciabilità ai sensi dell'Art. 22), considerando la finalità perseguita dal DSA di contrasto all'illegalità online specialmente per quanto riguarda le attività di contraffazione.

- *Necessità di coordinamento con altri plessi normativi a livello europeo e nazionale*

A fronte dei diversi plessi normativi in vigore o in via di approvazione incidenti sui servizi digitali, si segnala in generale l'opportunità di un maggior coordinamento della disciplina orizzontale del DSA con altre fonti settoriali interferenti (ad esempio, proposta "Digital Markets Act", Direttiva sui Servizi Media Audiovisivi (SMAV), nuova Direttiva CDSM, Regolamento 2019/1150 "Platform to Business"),

al fine di assicurare un quadro di riferimento preciso, non aggravare eccessivamente la compliance normativa delle imprese e non creare frammentazione ed incertezza giuridica circa l'ambito di applicazione delle diverse normative. In questo senso, un aspetto molto rilevante è la definizione dell'ambito soggettivo di applicabilità delle nuove norme. Infatti, si rileva come le definizioni dei prestatori dei servizi intermediari adottate dalla Proposta DSA non coincidano con le definizioni contenute in altri strumenti normativi, in particolare: (i) il Regolamento P2B è applicabile ai "servizi di intermediazione online"; (ii) l'Art. 17 della Direttiva CDSM disciplina la responsabilità dei "prestatori di servizi di condivisione di contenuti online" per l'utilizzo di contenuti protetti dal diritto d'autore; (iii) la Direttiva SMAV impone determinati obblighi per i "servizio di piattaforma per la condivisione di video"; (iv) la proposta di DMA si applica ai "servizi di piattaforma di base forniti o offerti dai gatekeeper", ovvero un soggetto che "ha un impatto significativo sul mercato interno; gestisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; detiene una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro".

Allo stesso modo, si è già sottolineata la necessità di coordinamento del DSA con la tutela online del diritto d'autore prevista dall'Art. 17 Direttiva CDSM e dalle disposizioni nazionali rilevanti in merito (ad esempio, il Regolamento AGCOM in Materia di Tutela del Diritto d'autore sulle reti di Comunicazione Elettronica e Procedure Attuative ai sensi del Decreto Legislativo 9 aprile 2003, n. 70 (come da ultimo modificato dalla Delibera n. 233/21/CONS).

Infine, nella formulazione di alcuni obblighi specifici potrebbe essere utile adottare la tecnica normativa seguita da altre disposizioni contenute in fonti normative dirette a contrastare condotte illecite perpetrate online. Ad esempio, l'art. 21 della proposta DSA (che prevede la comunicazione da parte della piattaforma online in caso di sospetto di commissione di un reato grave che comporta una minaccia per la vita o la sicurezza delle persone) dovrebbe circoscrivere con maggiore precisione la portata degli obblighi di comunicazione, in modo simile alla tecnica usata dall'Art. 14.5 del Regolamento (UE) 2021/784 del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici online.

- *Autorità competenti per l'enforcement del DSA*

Una questione ancora aperta è rappresentata dall'attribuzione a livello eurounitario e nazionale di competenze per l'enforcement del DSA. Al momento la proposta DSA non fornisce indicazioni sui soggetti chiamati a ricoprire il ruolo di autorità competenti per l'applicazione e l'esecuzione del DSA in ambito nazionale, lasciando la relativa designazione agli Stati Membri (Capo IV, sez. I DSA).

In particolare, gli Stati Membri dovranno designare una delle autorità competenti come "coordinatore dei servizi digitali" (Art. 38). Rispetto a tale scelta si possono ipotizzare diverse soluzioni, quali ad esempio la creazione di una nuova Autorità ad hoc, oppure l'attribuzione di tale ruolo ad una delle autorità esistenti nell'ordinamento interno. Nel dibattito nazionale si segnala il documento finale approvato dalla IX Commissione (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati sulla proposta DSA. Nell'esprimere una valutazione favorevole sulla proposta, la Commissione osserva come risulti "opportuna una precisazione circa l'assetto delle competenze di applicazione del regolamento, con particolare riguardo al coordinamento tra autorità nazionali, Digital services coordinator *e Commissione europea, in particolare con riferimento al regime di supervisione e ai poteri di* enforcement *nei confronti delle piattaforme* on line *molto grandi; circa la concreta applicazione del regolamento sul piano nazionale, appare opportuno indicare l'Autorità per le garanzie nelle comunicazioni quale organismo di diritto interno più idoneo a svolgere le funzioni di* Digital services coordinator*".*

A tal proposito si ricorda che ad AGCOM sono già attribuite una serie di competenze per l'enforcement di altre normative sui servizi digitali interferenti con il DSA. In particolare, la legge 30 dicembre 2020, n. 178 (legge di Bilancio 2021) designa AGCOM per l'attuazione del Regolamento (UE) 2019/1150 (Platform to Business), mentre il Decreto legislativo di attuazione della Direttiva CDSM estende le competenze dell'Autorità nell'ambito della tutela del diritto d'autore online (in aggiunta alle competenze già attribuite dall'art. 182-bis L. 633/1941, Art.32-bis TUSMAR, D.Lgs 70/2003). Ulteriori competenze sono attribuite dal Decreto Legislativo di Attuazione della Direttiva SMAV.

Infine, nelle more della discussione interistituzionale sul testo finale del DSA non può essere esclusa l'ipotesi di una competenza esclusiva della Commissione con riferimento all'enforcement nei confronti di alcune categorie di piattaforme. In particolare, parallelamente alla competenza esclusiva della Commissione nei confronti dei gatekeepers soggetti al DMA, alla Commissione potrebbe essere attribuito lo stesso ruolo nei confronti delle piattaforme di dimensioni molto grandi ai sensi del DSA.

Considerate l'incertezza ancora esistente sull'assetto delle competenze di applicazione del Regolamento e la tendenza all'accentramento delle competenze di enforcement in capo al coordinatore nazionale ed eventualmente persino alla Commissione europea, in ragione delle dimensioni e del ruolo delle piattaforme coinvolte, allo stato di avanzamento dell'iter di approvazione della proposta è prematuro ipotizzare eventuali forme di coordinamento con altre autorità competenti che potrebbero essere designate a livello interno. Pertanto, l'eventuale ripartizione di competenze andrà esaminata a valle delle soluzioni finali adottate dal DSA.

Infine, si segnala che gli Artt. 8 e 9 del DSA potrebbero avere un impatto sull'ordinamento nazionale, in quanto tali disposizioni prevedono per le autorità giudiziarie o amministrative nazionali il potere di imporre ordini di contrasto ai contenuti illegali e di fornire informazioni nei confronti dei prestatori di servizi intermediari. Il DSA chiarisce che tali ordini potrebbero avere effetto oltre il territorio dello Stato membro dell'autorità in questione.

Introduzione. Tecnologie digitali ed impatto della contraffazione online.

L'avvento ed il progressivo diffondersi delle tecnologie digitali hanno prodotto effetti contrastanti per i comparti industriali caratterizzati da un elevato sfruttamento dei diritti di proprietà intellettuale (IPR intensive). A fronte, infatti, di un accesso più ampio per i consumatori ai contenuti digitali e, dunque, a nuove e potenzialmente maggiori opportunità di sfruttamento degli stessi da parte dei titolari, la dematerializzazione ha favorito altresì l'emergere di nuove forme di sfruttamento non autorizzato che si sono rivelate difficili da contrastare.

Nel recente IP Action Plan, la Commissione europea ha rilevato come, nonostante i costanti sforzi compiuti per invertire la tendenza, la contraffazione e la pirateria continuano a prosperare, proprio grazie allo sfruttamento delle tecnologie digitali [1] . Per quanto concerne il contesto europeo, gli studi rilasciati dall'Organizzazione per la cooperazione e lo sviluppo economico (OECD) e dall'Ufficio europeo per la proprietà intellettuale (EUIPO)[2] – aggiornati rispetto a quelli ripresi dall'impact assessment della Commissione europea della proposta di Regolamento sui servizi digitali (Digital Services Act - DSA) per giustificare l'intervento[3] - segnalano, infatti, che le importazioni di prodotti contraffatti in Europa ammontano a 119 miliardi di euro, un valore che rappresenta il 5,8 % delle

[1] Commissione europea, ***Sfruttare al meglio il potenziale innovativo dell'UE. Piano d'azione sulla proprietà intellettuale per sostenere la ripresa e la resilienza dell'UE***, COM (2020) 760 final, 4. ***Cfr.***, nell'ordinamento italiano, le priorità e l'agenda del Consiglio Nazionale per la Lotta alla Contraffazione e all'Italian Sounding (CNALCIS).
[2] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_EUIPO_OECD_Report_Fakes/2021_EUIPO_OECD_Trate_Fakes_Study_FullR_en.pdf
[3] Commission Staff Working Document, ***Impact assessment accompanying the document Proposal for a Regulation*** on a Single Market for Digital Services, SWD (2020) 348 final, Part 1, 13.

importazioni nel 2019 (stabile rispetto ai precedenti dati del 2016)[4]. Ogni anno questo si traduce in una perdita di vendite dirette pari a 50 miliardi di euro e in una perdita di 416 mila posti di lavoro[5]. Del resto, i comparti IPR intensive rappresentano il 45% del prodotto interno lordo dell'Unione, il 29% degli occupati ed il 96% dei prodotti esportati nel resto del mondo[6].

Tra i diritti di proprietà intellettuale interessati, i marchi si presentano come uno strumento essenziale di un'economia di mercato, rappresentando la percentuale più elevata del prodotto interno lordo europeo (37%)[7]. Sul versante degli attori coinvolti, invece, social media e piattaforme di commercio elettronico sono di fatto e in maniera crescente gli strumenti privilegiati dai soggetti attivi nella contraffazione, la quale, rispetto al passato, non è più incentrata su prodotti di marca e di lusso, bensì coinvolge in maniera crescente farmaci e cosmetici, prodotti elettronici, giocattoli, bevande e cibo, parti di ricambio delle autovetture, prodotti per la casa[8]. A conferma del ruolo svolto dalle piattaforme nel fenomeno contraffattivo, l'impact assessment del DSA segnala come l'80% dei prodotti contraffatti individuati dalle autorità riguarda piccoli colli, i quali sono generalmente considerati una proxy del commercio elettronico[9].

Le imprese risultano, inoltre, fortemente danneggiate dalle attività di contraffazione online non solo per quanto attiene alle mancate vendite, ma altresì per i significativi costi sostenuti per contrastare la violazione dei propri diritti di proprietà intellettuale. Analisi recenti segnalano, infatti, come la contraffazione provochi un danno significativo alla profittabilità delle imprese innovative

[4] OECD e EUIPO, ***Trends in Trade in Counterfeit and Pirated Goods***, (2019) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/trends_in_trade_in_counterfeit_and_pirated_goods/trends_in_trade_in_counterfeit_and_pirated_goods_en.pdf.
[5] EUIPO, ***2020 Status Report on IPR Infringement***, (2020) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Commission Staff Working Document, ***supra*** nota 2, 13.

soprattutto per i costi operativi sopportati per l'enforcement dei diritti interessati[10].

La Commissione ha dunque ravvisato la necessità di intensificare gli sforzi per contrastare la contraffazione e la pirateria responsabilizzando maggiormente le piattaforme online e tentando di eliminare i disincentivi alle loro azioni volontarie volte a contrastare i contenuti illegali da esse intermediati[11]*. Dal momento che, in ambito digitale, i servizi degli intermediari sono sempre più utilizzati da terzi per attività illecite (non solo limitate alla contraffazione), infatti, le piattaforme online vengono considerate i soggetti più idonei a porre fine a dette attività "secondo l'idea che ciò che è illecito offline debba esserlo anche online"* (come recentemente sottolineato dal Presidente Mario Draghi, nel suo intervento in Senato del 21 ottobre 2021).

La proposta di DSA è intesa proprio ad armonizzare una serie di obblighi specifici per le piattaforme online in un quadro di vigilanza rafforzato[12]*. Del resto, dai tempi dell'adozione della Direttiva 2000/31/EC sul commercio elettronico (Direttiva e-commerce) l'ecosistema digitale si è evoluto diventando sempre più articolato e complesso. Sono emersi nuovi modelli di business e servizi, come i social networks e gli online marketplaces, che consentono ad imprese e consumatori di condividere informazioni e concludere transazioni commerciali nelle modalità più svariate*[13]*. Sono altresì emerse nuove tecnologie che hanno migliorato disponibilità, velocità, sicurezza e affidabilità dei sistemi di trasmissione e immagazzinamento dei dati*[14]*.*

La proposta contenuta nel DSA mira a riformare il quadro regolamentare della Direttiva sul commercio elettronico, mantenendo in vita i principi cardine del regime di responsabilità degli intermediari online, ma al tempo stesso

[10] Vincenzo Butticè, Federico Caviggioli, Chiara Franzoni, Giuseppe Scellato, Piotr Stryszowski, Nikolaus Thumm, ***Counterfeiting in digital technologies: An empirical analysis of the economic performance and innovative activities of affected companies***, 49 Research Policy (2020); EUIPO, ***Private costs of enforcement of IPR***, (2017) https://euipo.europa.eu/ohimportal/it/web/observatory/news/-/action/view/3477009.
[11] Commissione europea, ***supra*** nota 1, 17.
[12] Commissione europea, ***Proposta di Regolamento relativo a un mercato unico dei servizi digitali (Digital Services Act) e che modifica la direttiva 2000/31/CE***, COM (2020) 825 final.
[13] Ibid. Considerando 1.
[14] Ibid. Considerando 27.

aggiornando il quadro definitorio degli attori coinvolti e introducendo nuovi obblighi differenziati in base al ruolo e alla dimensione delle piattaforme.

Essendo la proposta di Regolamento ancora al suo stadio iniziale, nel prosieguo sarà fotografato il DSA, come strutturato dalla Commissione europea nella proposta originaria, illustrandone contenuto e principali innovazioni rispetto al quadro precedente.

Il presente Report è strutturato come segue.

Il ***primo paragrafo*** *ha l'obiettivo di fornire una disamina del quadro regolamentare attualmente vigente in Europa, dando conto delle disposizioni rilevanti e della casistica giurisprudenziale pertinente.*

Il ***secondo paragrafo****, strutturato in diverse sezioni tematiche, è dedicato ad una analisi puntuale delle disposizioni della proposta di Regolamento della Commissione sul DSA, con un focus particolare sulla responsabilità delle piattaforme in caso di contraffazione online di diritti di proprietà industriale. Tale paragrafo si chiude con alcune osservazioni preliminari sui profili innovativi proposti in materia di compliance normativa a tale tipo di atto.*

Il ***terzo ed il quarto paragrafo*** *riportano le principali criticità sollevate sinora sulla proposta della Commissione nell'ambito del dialogo con i vari portatori di interesse e nell'ambito del dibattito istituzionale.*

Il ***quinto paragrafo*** *affronta le principali questioni oggetto di dibattito rilevanti per l'enforcement dei diritti di proprietà industriale online, analizzandone anche l'impatto sui diversi stakeholders.*

Il ***sesto paragrafo*** *fornisce alcune conclusioni preliminari.*

1. Il quadro regolamentare vigente: Direttiva e-commerce, sistemi di filtraggio e misure di blocco dei siti internet[15].

La Direttiva 2000/31/CE sul commercio elettronico prevede un'esenzione di responsabilità (*safe harbor*) per le attività di semplice trasporto (*mere conduit*), memorizzazione temporanea (*caching*) e *hosting*. Resta impregiudicata la facoltà per gli Stati membri di adottare normative che attribuiscano all'autorità giudiziaria o amministrativa il potere di esigere, attraverso un provvedimento inibitorio, che il *provider* ponga fine ad una violazione o la impedisca, nonché di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime (*notice-and-takedown*).

Il principio è ripreso dalla Direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale ('**Direttiva *enforcement*'**), che all'Articolo 11 impegna gli Stati membri ad assicurare che i titolari possano chiedere un provvedimento ingiuntivo nei confronti di intermediari i cui servizi sono utilizzati da terzi per violare un diritto di proprietà intellettuale. Impegno, quest'ultimo, che, come la giurisprudenza della Corte di giustizia ha avuto modo di chiarire, deve intendersi riferito all'adozione di provvedimenti che in modo effettivo siano in grado non solo di porre fine alle violazioni, ma anche di prevenire nuove violazioni[16]. A questo fine, tali ingiunzioni devono essere efficaci, proporzionate, dissuasive e non devono creare ostacoli al commercio legittimo.

Analizzando nel dettaglio il *safe harbor* della Direttiva sul commercio elettronico, l'Art. 12 prevede che, per le attività di semplice trasporto, il prestatore non è responsabile delle informazioni trasmesse a condizione che egli: *i*) non dia origine alla trasmissione; *ii*) non selezioni il destinatario della trasmissione; *iii*) non selezioni né modifichi le informazioni trasmesse. Allo stesso modo l'Art. 13, per l'attività di *caching*, prevede che il prestatore non sia responsabile della memorizzazione automatica, intermedia e temporanea delle informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che egli: *i*) non modifichi le informazioni; *ii*) si conformi alle condizioni di accesso alle informazioni; *iii*) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; *iv*) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; *v*) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione dell'accesso. L'Art. 14 esenta, invece, colui che offre un

[15] Il paragrafo riprende e sviluppa i lavori precedentemente pubblicati da Giuseppe Colangelo e Mariateresa Maggiolino, ***ISPs' copyright liability in the EU Digital Single Market Strategy***, 26 International Journal of Law and Information Technology 142 (2018); Giuseppe Colangelo, ***Digital Single Market Strategy, diritto d'autore e responsabilità delle piattaforme online***, Analisi giuridica dell'economia, 2017, 2, 603.
[16] Corte di giustizia, 12 luglio 2011, causa C-324/09.

servizio di *hosting* da ogni responsabilità relativa alle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: *i*) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione; *ii*) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

In ogni caso, precisa l'Art. 15, nella prestazione dei suddetti servizi, gli Stati membri non possono imporre agli intermediari *online* un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite: gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.

Le pronunce della Grande Sezione della Corte di giustizia in *Google France c. Louis Vuitton*[17] e *L'Oréal c. eBay*[18] hanno precisato gli ambiti di applicazione dell'esenzione di cui all'art. 14, affermando che la stessa vale solo per i *providers* che non abbiano svolto un ruolo attivo in grado di consentire loro di avere conoscenza o controllo circa i dati memorizzati. Occorre, dunque, esaminare se il ruolo svolto dal prestatore di servizi sia neutrale, in quanto il suo comportamento è meramente tecnico, automatico e passivo: così non è allorché l'intermediario abbia prestato un'assistenza consistente nell'ottimizzare la presentazione delle offerte in vendita e nel promuovere tali offerte. Il prestatore di servizio che non ha svolto un ruolo attivo non può comunque avvalersi dell'esonero dalla responsabilità qualora sia venuto a conoscenza della natura illecita dei dati o delle attività e abbia omesso di rimuove prontamente i dati o disabilitare l'accesso agli stessi.

Più di recente, nel caso *YouTube,* la Grande Sezione della Corte di giustizia è tornata sul punto per meglio chiarire i contorni del ruolo attivo dei *providers*[19]. Dopo aver premesso che per beneficiare dell'esenzione di cui all'Art. 14, il *provider* deve svolgere un ruolo neutro che implica la mancanza di conoscenza o di controllo sui contenuti che memorizza, e che la conoscenza richiesta si riferisce ad attività e informazioni illecite concrete, la Corte ha stabilito che l'indicizzazione automatizzata dei contenuti, la predisposizione di funzioni di ricerca e l'inoltro di suggerimenti e consigli sui contenuti in funzione del profilo o delle preferenze degli utenti, non rappresentano elementi sufficienti per considerare che detto gestore sia concretamente al corrente di attività illecite realizzate sulla medesima piattaforma o di informazioni illecite ivi memorizzate[20].

La distinzione tra i profili di responsabilità dei *providers* introdotta dalla Direttiva sul commercio elettronico è stata confermata, in ambito nazionale, dalle sentenze della Corte di Cassazione n. 7708 e 7709 del 19 marzo 2019, con particolare riferimento alla figura di *hosting provider* attivo e alla mera attività neutrale di *caching.*

[17] Corte di giustizia, 23 marzo 2010, causa C-236/08.
[18] ***eBay, supra*** nota 16.
[19] Corte di giustizia, 22 giugno 2021, cause riunite C-682/18 e C-683/18, ***YouTube c. Cyando.***
[20] ***YouTube, supra*** nota 24, para. 114.

In questo scenario, la Corte di giustizia dell'Unione europea è intervenuta a più riprese per chiarire il rapporto (ed il potenziale conflitto) tra *enforcement* della proprietà intellettuale e tutela della libertà di impresa, affrontando in particolare il tema relativo alla possibilità di imporre agli intermediari *online* misure capaci non solo di porre fine alle violazioni, ma anche di prevenirne di nuove, quali l'adozione di sistemi di filtraggio delle comunicazioni elettroniche, o di intervenire direttamente bloccando l'accesso degli utenti ad un sito Internet, in linea con quanto richiesto dall'art. 11 della Direttiva *enforcement.* In particolare, distinguendo gli obblighi di sorveglianza generali da quelli applicabili in casi specifici, la Corte ha ammesso che sia possibile ingiungere ad un intermediario di prevenire talune infrazioni, esercitando una forma di sorveglianza mirata del suo servizio.

Con riferimento ai sistemi di filtraggio, nei casi *Scarlet*[21] (relativo ad un *access provider*) e *Netlog*[22] (relativo ad un *social network*), la Corte ha stabilito come la normativa europea non consenta di imporre un sistema di filtraggio che si applichi indistintamente a tutta l'utenza dell'*internet service provider*, a titolo preventivo, a sue spese esclusive e senza limiti nel tempo. Una ingiunzione di questo genere, infatti, implicherebbe l'obbligo di procedere a una sorveglianza attiva su tutti i dati di ciascun utente per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale, contravvenendo al principio espresso dall'Art. 15 della Direttiva sul commercio elettronico che vieta appunto di imporre sia un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate dal *provider* sia un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Infine, una siffatta ingiunzione causerebbe una grave violazione della libertà di impresa dell'intermediario *online*, obbligandolo a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico, il che risulterebbe contrario alle condizioni stabilite dall'Art. 3.1 della Direttiva *enforcement*, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale siano eque, proporzionate e non inutilmente complesse o eccessivamente costose.

Per quanto concerne, invece, la compatibilità con la normativa europea di un provvedimento di blocco dell'accesso a un sito Internet (*website blocking*) che mette a disposizione del pubblico materiali illeciti, il riferimento è rappresentato dalla decisione *Telekabel*[23]. Secondo i giudici comunitari, l'adozione di un provvedimento di blocco di accesso al sito, pur limitando la libertà d'impresa, non ne pregiudica la sostanza: da un lato, una siffatta ingiunzione lascia al suo destinatario l'onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito, con la conseguenza che quest'ultimo può scegliere di adottare misure che più si adattino alle risorse e alle capacità di cui dispone e che siano compatibili con gli altri obblighi e sfide cui deve far fronte nell'esercizio della propria attività; dall'altro lato, consente al suo destinatario di sottrarsi alla propria responsabilità qualora dimostri di aver adottato tutte le misure ragionevoli, circostanza che è giustificata dal fatto che quest'ultimo non è l'autore della violazione del diritto fondamentale della proprietà intellettuale che ha dato luogo alla pronuncia della suddetta ingiunzione.

Più nello specifico, secondo la Corte, i diritti fondamentali riconosciuti dall'Unione non ostano a che sia vietato, con un'ingiunzione pronunciata da un giudice, a un fornitore di accesso a Internet di concedere ai suoi abbonati l'accesso a un sito Internet che metta in rete materiali protetti senza il

[21] Corte di giustizia, 24 novembre 2011, causa C-70/10.
[22] Corte di giustizia, 19 aprile 2012, causa C-461/10
[23] Corte di giustizia, 27 marzo 2014, causa C-314/12.

consenso dei titolari dei diritti, qualora tale ingiunzione non specifichi quali misure il fornitore di accesso deve adottare e quest'ultimo possa evitare sanzioni per la violazione di tale ingiunzione dimostrando di avere adottato tutte le misure ragionevoli. Ciò a condizione, tuttavia, che, da un lato, le misure adottate non privino inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili e, dall'altro, che tali misure abbiano l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del destinatario di questa stessa ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà intellettuale.

La pronuncia è di particolare interesse in ragione del fatto che, negli ultimi anni, i *website blocking* stanno emergendo come un rimedio complementare alla procedura di *notice-and-takedown*, sebbene non manchino perplessità sulla loro efficacia. Si verifica, infatti, sovente che, mentre un'autorità giudiziaria competente ha emesso un'ingiunzione con riferimento a determinati nomi di dominio, appaiano rapidamente siti speculari sotto altri nomi di dominio che non sono colpiti dall'ingiunzione.

Rispetto a tale problematica, in alcuni Paesi si è fatta largo l'adozione di ingiunzioni flessibili, dinamiche e *catalogue-wide.* Si tratta di ingiunzioni che possono essere emesse nei casi in cui lo stesso sito web diventi disponibile immediatamente dopo l'emissione di un'ingiunzione con un indirizzo IP o un URL differenti, oppure di ingiunzioni che impongano agli intermediari di impedire ulteriori violazioni di tutti i diritti detenuti da un titolare di diritti o che fanno parte di un catalogo o del repertorio di un titolare di licenza, in base alla violazione constatata di un campione di tali diritti[24].

In tema si segnalano, in particolare, due importanti decisioni della High Court britannica: la prima (*Cartier*[25]) per i principi e le condizioni individuati per autorizzare un provvedimento di blocco di un sito Internet, la seconda (*Football Association Premier League*[26]) per la particolare tipologia di *website blocking* implementato.

In *Cartier* vengono individuate quattro *threshold conditions* (ossia che il provvedimento sia diretto nei confronti di un *internet service provider*; che gli utenti e/o il gestore del sito in questione abbiano violato diritti d'autore e che a tal fine abbiano utilizzati i servizi del *provider*; infine, che il *provider* abbia conoscenza effettiva, anziché generalizzata, della violazione, il che può essere il risultato di una denuncia ricevuta da parte degli aventi diritto) e sette principi che devono accompagnare la decisione di accordare il provvedimento in questione (dovendo garantire che quest'ultimo sia necessario, efficace, dissuasivo, non indebitamente costoso o complesso, inidoneo a creare barriere al commercio legittimo, equo ed in grado di realizzare un giusto equilibrio tra i diritti fondamentali coinvolti, nonché proporzionato). Il principio di proporzionalità svolge di fatto un ruolo chiave finendo per abbracciare tutti gli altri fattori e postula di prendere in considerazione la natura delle misure tecniche che i *providers* sono chiamati ad adottare, la loro efficacia e capacità dissuasiva, il loro costo di implementazione (e dunque anche la disponibilità di misure alternative meno onerose), nonché l'impatto sugli utenti che non commettono violazioni. Rispetto al provvedimento in questione, la Corte

[24] Per una comparazione delle ***dynamic injunctions*** adottate sinora ***cfr.*** Giancarlo Frosio e Oleksandr Bulayenko, ***Study on Dynamic Blocking Injunctions in the European Union***, (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3807277; European Parliament Research Service, ***Challenges facing sports event organizers in the digital environment,*** (2020) 50, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654205/EPRS_STU(2020)654205_EN.pdf.
[25] [2014] EWHC 3354 (Ch), confermata in appello ([2016] EWCA Civ 658).
[26] [2017] EWHC 480 (Ch) e [2018] EWHC 1828 (Ch).

britannica segnala come, in un'analisi costi-benefici, il *website blocking* sia una misura superiore a tutte le altre opzioni sul campo, compresi la procedura di *notice and takedown*, la deindicizzazione dai motori di ricerca, la sospensione dei sistemi di pagamento adoperati dal sito, il sequestro del nome di dominio ed il sequestro doganale.

La decisione *Football Association Premier League* si caratterizza, invece, per l'adozione di un ordine di blocco *live*, ossia limitato alla finestra temporale nella quale il contenuto protetto è trasmesso via streaming. Il provvedimento contempla inoltre un procedimento di individuazione di *target servers* fortemente sospettati di operare sistematicamente in violazione dei diritti in questione, la cui lista deve essere aggiornata ogni settimana durante la stagione calcistica. Il provvedimento di *live blocking* è stato adottato anche nella successiva pronuncia *UEFA*[27], in quanto, secondo la Corte, la misura è efficace e non risultano prove di *overblocking*.

Tale approccio è stato condiviso dalla Commissione europea, la quale, nella Comunicazione sugli "Orientamenti in merito ad alcuni aspetti della direttiva 2004/48/CE sul rispetto dei diritti di proprietà intellettuale"[28], ha evidenziato come siffatte ingiunzioni possano costituire uno strumento efficace per impedire il proseguimento di una violazione dei diritti di proprietà intellettuale. Sebbene tali ingiunzioni dinamiche siano intervenute specialmente in casi di violazione di diritti d'autore o diritti connessi, esse costituiscono validi precedenti anche per l'*enforcement online* di altri diritti IP.

Da ultimo, sebbene non relativa a diritti di proprietà intellettuale, è opportuno segnalare la sentenza della Corte di giustizia nel caso *Eva Glawischnig-Piesczek c. Facebook*[29]. In questa occasione, i giudici europei hanno valorizzato la specificità dell'obbligo imposto al *provider*, trattandosi di una ingiunzione puntuale riguardante la ricerca e il blocco di una puntuale informazione a carattere diffamatorio. Alla luce di ciò, si è affermato che l'Art. 15 della Direttiva *e-commerce* non osta a che un giudice di uno Stato membro possa ordinare a un prestatore di servizi di *hosting* di rimuovere le informazioni da esso memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime (c.d. ***stay down***), purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illiceità e che contiene gli elementi specificati nell'ingiunzione e le differenze nella formulazione di tale contenuto equivalente rispetto a quella che caratterizza l'informazione precedentemente dichiarata illecita non siano tali da costringere il prestatore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto. Secondo la Corte, tale provvedimento può essere imposto a livello mondiale.

L'impianto regolamentare appena ricostruito non ha mancato di sollevare critiche e perplessità.

In primo luogo, si è sottolineato come appaia sempre meno opportuno considerare gli *internet service providers* come un gruppo monolitico. Con riferimento alle procedure di *notice-and-takedown,* ad esempio, il quadro complessivo sembra essersi evoluto verso un ecosistema altamente complesso nel quale, accanto agli intermediari tradizionali, sono emerse figure diverse quali i *providers* che ricorrono a servizi automatizzati per gestire la mole enorme di notifiche ricevute e che adottano misure ulteriori

[27] [2017] EWHC 3414 (Ch) e [2018] EWHC 1900 (Ch).
[28] COM (2017) 708 final.
[29] Corte di giustizia, 3 ottobre 2019, Causa C-18/18.

rispetto a quelle previste dalla normativa, come ad esempio sistemi di filtraggio, accordi di collaborazione con i titolari dei diritti, procedure di *takedown* diretto in favori di alcuni titolari di diritti considerati attendibili[30].

A tal proposito, si è, inoltre, evidenziato come le procedure di *takedown*, soprattutto se affidate a sistemi di gestione automatizzata, si prestino a forme di *misuse* sotto forma di *over-removal* non garantendo adeguatamente né l'accuratezza delle indagini sull'effettivo carattere illecito del materiale esaminato né la salvaguardia dei principi del giusto processo[31]. Dalla prospettiva dell'intermediario, infatti, l'approccio economicamente razionale, in quanto più semplice, meno costoso e meno rischioso, è quello di processare ogni richiesta di rimozione senza indagare sulla effettiva illiceità del contenuto (approccio '*if in doubt, take it down*'). E dubbi ulteriori si pongono naturalmente con eventuali obblighi preventivi di ***notice and stay down***.

Infine, ulteriori perplessità sono state sollevate con riferimento all'impatto economico di una eventuale predisposizione obbligatoria di tecnologie di filtraggio, come sembra suggerire l'Articolo 17 della recente Direttiva 2019/790 sul diritto d'autore nel mercato unico digitale (CDSM)[32]: nello specifico, si teme che i costi per l'implementazione di tali misure tecnologiche siano insostenibili per *start-ups* e *providers* di piccole dimensioni, e allo stesso tempo si denuncia la loro limitata efficacia, in quanto facili da aggirare ed incapaci di identificare numerose tipologie di contenuti. In quest'ottica, l'Art. 17(6) della Direttiva esclude dall'applicazione di questi obblighi i nuovi prestatori di servizi di condivisione di contenuti *online* i cui servizi sono disponibili al pubblico da meno di tre anni e che hanno un fatturato annuo inferiore a 10 milioni di euro.

Resta invece particolarmente acceso il dibattito sulle implicazioni giuridiche dell'Art. 17 e sulla sua compatibilità con i diritti fondamentali, come dimostrano le diverse proposte avanzate a livello nazionale per la sua implementazione nonché il ricorso presentato dalla Polonia dinanzi alla Corte di giustizia al fine di chiedere l'annullamento di alcune disposizioni dell'Articolo 17[33].

Da una parte, rispetto all'obbligo di monitoraggio sui contenuti la suddetta previsione sembra codificare il requisito della doppia specificità emerso nella casistica giurisprudenziale della Corte di giustizia prima richiamata, ossia che, affinché il divieto di obbligo generale di sorveglianza sia rispettato, è necessario che venga specificamente individuato sia il materiale protetto sia i potenziali

[30] Jennifer M. Urban, Joe Karaganis, Brianna Schofield, ***Notice and Takedown in Everyday Practice,*** UC Berkeley Public Law Research Paper No. 2755628 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

[31] French Ministére de la Culture, ***Report Hadopi Content Recognition Tools***, (2020) http://traduction.culture.gouv.fr/url/Result.aspx?to=en&url=https://www.culture.gouv.fr/Sites-thematiques/Propriete-litteraire-et-artistique/Conseil-superieur-de-la-propriete-litteraire-et-artistique/Travaux/Missions/Mission-du-CSPLA-sur-les-outils-de-reconnaissance-des-contenus-proteges-par-les-plateformes-de-partage-en-ligne-etat-de-l-art-et-propositions; Jon Penney, ***Privacy and Legal Automation: The DMCA as a Case Study***, 22 Stanford Technology Law Review 412 (2019); Sharon Bar-Ziv e Niva Elkin-Kore, ***Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown***, 50 Connecticut Law Review 339 (2018); Lenka Fiala e Martin Husovec, ***Using Experimental Evidence to Design Optimal Notice and Takedown Process***, Tilec Discussion Paper No. 2018-28, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218286. Sui rischi di blocco eccessivo di contenuti leciti, si vedano anche le Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe, 15 luglio 2021, Causa C-401/19, ***Repubblica di Polonia c. Parlamento europeo e Consiglio dell'Unione europea,*** paras. 141, 142 e 147, secondo il quale "[a]l fine di sottrarsi a qualsivoglia rischio di responsabilità, tali intermediari possono avere la tendenza a dar prova di zelo e a bloccare in maniera esagerata tali informazioni ***al minimo dubbio sulla loro liceità***" Tali rischi, prosegue Øe, sono accresciuti laddove le normative obblighino ***de facto***, in un elevato numero di casi, i prestatori di servizi di condivisione a ricorrere a strumenti di riconoscimento automatico di contenuto.

[32] GUUE (2019) L130/92.

[33] Causa C-401/19. Si vedano anche Christophe Geiger e Bernd Justin Jutte, ***Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match***, 4 GRUR International (2021); Martin Husovec e Joao Quintais, ***How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms***, 4 GRUR International (2021); Martin Husovec, ***Over-Blocking: When is the EU Legislator Responsible?***, (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149.

contraffattori[34]. L'Art. 17(4)(b) e (c) della Direttiva CDSM richiede, infatti, ai titolari dei diritti di fornire "informazioni pertinenti e necessarie" e "una segnalazione sufficientemente motivata", prima di obbligare i prestatori di servizi di condivisione di contenuti *online* a compiere i massimi sforzi per impedire il caricamento di materiali protetti dal diritto d'autore e ad agire tempestivamente per disabilitare l'accesso o rimuovere dai loro siti web i suddetti materiali. Al tempo stesso, tuttavia, resta da comprendere se e come lo stesso requisito possa essere rispettato nel momento in cui sistemi di filtraggio automatico dei contenuti vengono implementati.

Nelle Conclusioni presentate davanti alla Corte chiamata a pronunciarsi sul ricorso presentato dalla Polonia, l'Avvocato generale Øe, pur riconoscendo che la suddetta disposizione comporta effettivamente un'ingerenza nella libertà di espressione degli utenti dei servizi di condivisione, ha tuttavia affermato che l'Articolo 17 della Direttiva CDSM conterrebbe garanzie sufficienti per ridurre al minimo l'impatto di un tale filtraggio su siffatta libertà e proteggere gli utenti nei confronti di misure di blocco abusive o arbitrarie dei loro contenuti[35]. Infatti, in conformità al paragrafo 7 di tale articolo, i prestatori di servizi di condivisione non sono autorizzati a bloccare *ex ante* la totalità dei contenuti che riproducono le opere e gli altri materiali protetti identificati dai titolari dei diritti, inclusi quelli che possono essere leciti; dall'altro, in forza del paragrafo 8, i prestatori possono essere tenuti a rilevare e bloccare soltanto i contenuti che sono identici ed equivalenti a tali materiali, ossia la cui illiceità appare manifesta alla luce delle informazioni pertinenti e necessarie fornite dai titolari dei diritti. In simili casi, poiché la contraffazione è altamente probabile, tali contenuti possono essere presunti illeciti ed è, di conseguenza, proporzionato bloccarli *ex ante*, incombendo agli utenti interessati di dimostrarne la liceità nell'ambito del meccanismo di reclamo.

In ogni caso, la regola relativa al monitoraggio generale nell'ambito del diritto d'autore presenta significative differenze rispetto alla sua declinazione nel contesto dei marchi. In particolare, si è sottolineato come gli obblighi di sorveglianza preventiva previsti dall'Art. 17(4)(b) della Direttiva CDSM (ai sensi del quale i prestatori di servizi di condivisione di contenuti online sono responsabili per atti non autorizzati di comunicazione al pubblico, di materiali protetti dal diritto d'autore, a meno che non dimostrino di aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti) sarebbero, nel contesto dei marchi, probabilmente in contrasto con la libertà di concorrenza ed il principio di libera circolazione nel mercato interno.[36] In *eBay*, infatti, la Corte di Giustizia dell'Unione Europea ha affermato che un obbligo di sorveglianza non può avere l'oggetto o l'effetto di imporre un divieto generale e permanente di messa in vendita, in un mercato, di prodotti contrassegnati da alcuni marchi[37]. Sarà dunque da verificare se e come tale interpretazione sarà recepita nel DSA.

[34] Martin Senftleben e Christina Angelopoulos, ***The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market***, (2020) https://ssrn.com/abstract=3717022.
[35] Øe, ***supra*** nota 31.
[36] Senftleben e Angelopoulos, ***supra*** nota 34.
[37] ***eBay, supra*** nota 16, para. 140.

È di tutta evidenza, in ogni caso, come alcune delle preoccupazioni emerse in ambito di diritto d'autore (ad esempio, le possibili limitazioni alla libertà di espressione[38]) non siano applicabili al contesto dei marchi in ragione delle significative differenze che i due strumenti di tutela presentano con riferimento sia alle finalità perseguite sia all'oggetto di protezione[39].

[38] In tema di diritto d'autore, la Corte di giustizia, in ***YouTube***, ***supra*** nota 19, para. 116, ha precisato che, per procedere al ***takedown*** di un contenuto protetto illecitamente comunicato al pubblico tramite una piattaforma, la notifica deve contenere elementi sufficienti per consentire al gestore di tale piattaforma di accertarsi, senza un esame giuridico approfondito, del carattere illecito di tale comunicazione "e della compatibilità di un'eventuale rimozione del suddetto contenuto con la libertà di espressione".

[39] Oltre alla Direttiva 2019/790, si segnalano ulteriori tentativi di armonizzazione della responsabilità degli ISP in altri ambiti. Cfr. ad esempio la Direttiva (UE) 2017/541 del Parlamento Europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAIdel Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (si veda, inoltre, infra, il Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online); la Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011 , relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio; la Decisione quadro 2008/913/GAI del Consiglio, del 28 novembre 2008 , sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.

2. La proposta di Digital Services Act della Commissione europea

La proposta di DSA nasce principalmente da due esigenze. La prima attiene alla necessità di adeguare il quadro regolamentare all'evoluzione dell'ecosistema digitale. A vent'anni di distanza dalle Direttiva *e-commerce*, nuovi operatori, modelli di business e servizi sono emersi e si sono affermati, rendendo opportuno non solo un aggiornamento delle regole, ma altresì una revisione dell'approccio apparentemente semplicistico o eccessivamente lineare ad un ecosistema che oggi si presenta invece particolarmente complesso. Da questo punto di vista, l'aspetto più significativo è rappresentato dall'abbandono della unitarietà della caratterizzazione di fornitore di servizi di intermediazione (l'ISP che svolge attività di *hosting*), semplicemente distinto da quanti svolgono attività di mero trasporto o di memorizzazione automatica, per approntare, invece, una regolazione che riconosca il ruolo e le dimensioni delle piattaforme online.

Il ruolo sistemico di alcune piattaforme online che, in ragione delle loro dimensioni, fungono da *gatekeeper* [40] dell'accesso a mercati, clienti e informazioni, era già stato sottolineato nella Comunicazione 'Plasmare il futuro digitale dell'Europa', laddove, tra le azioni principali da intraprendere, veniva individuata la predisposizione di regole nuove per aumentare e armonizzare le responsabilità delle piattaforme online e dei prestatori di servizi di informazione, rafforzando la sorveglianza sulle politiche dei contenuti delle piattaforme nell'UE. [41] La prima esigenza consiste, pertanto nell'aggiornare il quadro normativo, trovando un bilanciamento tra impulso all'innovazione, rafforzamento della sicurezza e della fiducia nell'ambiente online e tutela dei diritti fondamentali.

La seconda esigenza è quella di adottare uno strumento (un Regolamento appunto) che assicuri il massimo livello di armonizzazione, al fine di scongiurare un mosaico frammentario di normative nazionali, dare ulteriore impulso al mercato unico digitale ed assicurare un livello di tutela adeguato ed uniforme per consumatori ed imprese.

Il cambio di paradigma avviene nel rispetto dei principi fondanti la Direttiva *e-commerce*. La proposta di DSA, infatti, conferma sia le disposizioni sull'esenzione di responsabilità degli ISP e, quindi, la necessità che venga dimostrata la conoscenza effettiva del materiale illecito eventualmente da essi trasmesso o ospitato, sia il divieto di un obbligo generale di monitoraggio che prevenga la trasmissione

[40] Il termine, tuttavia, non compare nel DSA, essendo, invece, centrale nella proposta di Regolamento ***Digital Markets Act*** (DMA): Commissione europea, ***Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act)***, COM (2020) 842 final**.** Come infatti spiegato dall'***impact assessment*** del DSA (***supra*** nota 2, paras. 1 e 2), "[t]he Digital Services Act together with the Digital Markets Act are intended as a comprehensive package of measures for the provision of digital services in the European Union and seek to address in particular the challenges posed by online platforms. In the Digital Services Act, which is underpinned by this impact assessment report, the intervention focuses on deepening the single market for digital services and establishing clear responsibilities for online platforms as well as other intermediary services to protect their users from the risks they pose, such as illegal activities online and risk to their fundamental rights. The Digital Markets Act complements these provisions and focuses on the gatekeeper role and unfair practices by a prominent category of online platforms".
[41] COM (2020) 67 final.

o condivisione di contenuti illeciti. Tuttavia, su queste basi, la proposta di DSA innesta nuovi obblighi per gli *hosting providers* e per le piattaforme *online*, specialmente se di grandi dimensioni.

Allo stato attuale, la proposta di DSA è all'attenzione del Parlamento europeo e del Consiglio ai sensi della procedura legislativa ordinaria (Artt. 289 e 294 TFUE).

2.1 Ambito di applicazione e definizioni rilevanti.

La proposta di DSA mira ad introdurre "un quadro normativo orizzontale per tutte le categorie di contenuti, prodotti, servizi ed attività sui servizi intermediari"[42] che integri le normative settoriali vigenti che continueranno ad applicarsi come *lex specialis* (Considerando 9).

In particolare, il DSA stabilisce norme armonizzate sulla prestazione di servizi intermediari nel mercato interno, quali, in particolare: a) norme sull'esenzione di responsabilità; b) norme relative a specifici obblighi in materia di dovere di diligenza per determinate categorie di prestatori di servizi intermediari; c) norme sull'attuazione e sull'esecuzione, anche in relazione alla cooperazione e al coordinamento tra le autorità competenti.

Tra i contenuti illegali veicolati tramite l'uso dei servizi di intermediazione *online* è menzionata esplicitamente dal Considerando 12 anche la vendita di prodotti non conformi o contraffatti[43]. La Relazione Introduttiva al DSA specifica, inoltre, come la proposta sia basata anche sulla raccomandazione sui contenuti illegali del 2018[44] e sull' "esperienza acquisita nel quadro degli sforzi di autoregolamentazione sostenuti dalla Commissione"[45], tra cui il protocollo d'intesa sulla vendita di merci contraffatte[46].

2.1.1 Ambito di applicazione territoriale.

Tra le novità introdotte dalla proposta rileva l'ambito di applicazione territoriale.

La proposta precisa all'Art. 1(3) che il DSA si applica "ai servizi intermediari prestati a destinatari il cui luogo di stabilimento o di residenza si trova nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi". Il DSA, dunque, sembra ampliare i criteri per determinare l'ambito di applicazione territoriale di tali norme, oltre al luogo di stabilimento dei prestatori dei servizi (*country of origin*) che costituisce il criterio principale del quadro normativo vigente. L'ambito di applicazione territoriale è inteso in maniera dinamica, sulla base di un principio di "collegamento sostanziale", definito dal Considerando 7 ed i cui indici sono indicati dal Considerando 8. Tale collegamento, infatti,

[42] Commissione europea, ***supra*** nota 17, Explanatory memorandum, 4.
[43] I contenuti illegali sono definiti dall'Art. 2(g) come "qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni". La nozione è dunque molto ampia.
[44] C (2018) 1177 final.
[45] Commissione europea, ***supra*** nota 17, Explanatory memorandum, 5.
[46] Commissione europea, ***Memorandum of understanding on the sale of counterfeit goods on the internet***, (2016) https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

può basarsi sul luogo di stabilimento oppure, in mancanza, "sulla base dell'esistenza di un numero considerevole di utenti in uno o più Stati membri" o "dell'orientamento delle attività verso uno o più Stati membri", il quale può essere determinato sulla base di "circostanze pertinenti" (tra cui, ai sensi del Considerando 8, fattori quali "l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione, la possibilità di ordinare prodotti o servizi oppure l'utilizzo di un dominio di primo livello nazionale", [...] "la disponibilità di un'applicazione nell'apposito negozio online (app store) nazionale, dalla fornitura di pubblicità a livello locale o nella lingua usata nello Stato membro in questione o dalla gestione dei rapporti con la clientela, ad esempio la fornitura di assistenza alla clientela nella lingua generalmente parlata in tale Stato membro", mentre "la mera accessibilità tecnica di un sito web dall'Unione non può, di per sé, essere considerata come costitutiva di un collegamento sostanziale con l'Unione").

L'ambito di applicazione territoriale, che ricorda i criteri di applicazione territoriale del GDPR[47], è così individuato al fine di garantire una maggiore efficacia delle norme, oltre a stabilire parità di condizioni nel mercato interno. La relazione al DSA sottolinea come la rilevanza di tale aspetto sia emerso in sede di consultazione specialmente con riferimento alle grandi piattaforme[48].

L'ambito di applicazione territoriale della proposta di DSA è completato dalle norme sull'*enforcement* che istituiscono un quadro multilivello UE/Stati Membri.

L'Articolo 40, infatti, stabilisce che la giurisdizione per l'applicazione del Regolamento (e in particolare l'esecuzione delle norme di cui al Capo III e IV) spetta allo Stato membro in cui è situato lo stabilimento principale del prestatore di servizi, a meno che non sussista la competenza della Commissione europea ai sensi degli Articoli 50 e 51. Lo stabilimento principale è indicato quale luogo in cui il prestatore ha la "sua sede principale o sociale nella quale sono esercitate le principali funzioni finanziarie e il controllo operativo" (Considerando 76). Per i prestatori non stabiliti nell'Unione, ma che "offrono servizi nell'Unione" la giurisdizione è determinata dal luogo in cui il prestatore ha nominato il proprio rappresentante legale. Ove il prestatore ometta di designare un rappresentante legale, tutti gli Stati Membri dovrebbero in linea di principio avere giurisdizione, a condizione che sia rispettato il principio del *ne bis in idem* e che vi sia una opportuna comunicazione tra Stati delle misure adottate nell'esercizio di tale giurisdizione.

Un altro profilo peculiare concerne l'ambito di applicazione degli ordini da parte di autorità giurisdizionali ed amministrative nazionali di contrasto ai contenuti illegali e di richiesta di informazioni (definiti agli Articoli 8 e 9). Oltre a ribadire che tali ordini dovrebbero limitarsi a quanto strettamente necessario per il conseguimento dei relativi obiettivi ed a prevedere che essi sono soggetti alle norme che tutelano la competenza dello Stato membro nel quale è stabilito il prestatore di servizi cui sono rivolti, i Considerando 31 e seguenti menzionano "eventuali deroghe a tale competenza in determinati casi previsti all'articolo 3 della direttiva 2000/31/CE". Inoltre, la proposta afferma che "qualora l'ordine contenente riferimento a informazioni specifiche possa avere effetto oltre il territorio dello Stato membro dell'autorità in questione, quest'ultima dovrebbe inoltre valutare se le informazioni in questione possano costituire contenuti illegali in altri Stati membri interessati e, se del

[47] Regolamento (UE) 2016/679 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), GU (2016) L 119/1.
[48] Commissione europea, ***supra*** nota 17, Explanatory memorandum, 10.

caso, tenere conto delle pertinenti norme del diritto dell'Unione o del diritto internazionale e degli interessi della cortesia internazionale". Tale circostanza appare coerente con la giurisprudenza euro-unitaria[49], seppur un tale assetto potrebbe creare eventuali problemi di raccordo internazionale, per i quali sarebbe necessario ulteriore approfondimento.

2.1.2 Ambito di applicazione soggettivo: le nuove definizioni di "servizi intermediari" e "piattaforme" del DSA

Per quanto concerne l'ambito di applicazione soggettivo del DSA, esso regola la **"prestazione di servizi intermediari"**. Il Considerando 5 chiarisce a tal fine che si tratta di prestatori di determinati servizi della società dell'informazione quali definiti nella Direttiva (UE) 2015/1535, ossia "qualsiasi servizio prestato normalmente dietro retribuzione[50], a distanza, per via elettronica e a richiesta individuale di un destinatario" e in particolare ai servizi intermediari consistenti in servizi noti (e definiti all'Art. 2) come: un servizio di semplice trasporto (***mere conduit***), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire accesso a una rete di comunicazione; un servizio di memorizzazione temporanea (***caching***), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta; un servizio di ***hosting***, consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo.

L'Art. 1(4) stabilisce, inoltre, che il DSA non si applica ai servizi che non sono servizi intermediari né alle prescrizioni imposte in relazione a tali servizi, indipendentemente dal fatto che questi ultimi siano prestati facendo ricorso a servizi intermediari.

A tali tradizionali categorie, si affianca nel DSA una ulteriore nuova qualificazione che innesca una serie di obblighi, la **"piattaforma online",** definita (Art. 2(h)) come un prestatore di servizi di *hosting* che, su richiesta di un destinatario del servizio, non solo memorizza, ma diffonde anche al pubblico tali informazioni[51], come nel caso dei *social network* e dei mercati *online* (Considerando 13). In tale definizione non rientrano, tuttavia, i servizi di *hosting* la cui attività di diffusione al pubblico sia "solo una funzionalità minore e meramente accessoria di un altro servizio e, per ragioni tecniche oggettive, tale funzionalità non può essere utilizzata senza tale altro servizio principale"[52], al fine di evitare l'imposizione di obblighi eccessivamente ampi[53]. Il Considerando 13 fornisce l'esempio delle sezioni

[49] ***Eva Glawischnig-Piesczek c. Facebook, supra*** nota 29.
[50] Sulla nozione di retribuzione è lecito peraltro domandarsi se vi rientri anche l'offerta di dati personali come controprestazione alla luce di quanto stabilito dalla Direttiva 2018/1972/UE che istituisce il codice europeo delle comunicazioni elettroniche e la Direttiva 2019/770/UE relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.
[51] La diffusione al pubblico è definita all'Art. 2 (i) come la "messa a disposizione di un numero potenzialmente illimitato di terzi informazioni su richiesta del destinatario del servizio che le ha fornite". Il concetto dovrebbe tuttavia escludere la diffusione di informazioni all'interno di gruppi chiusi costituiti da un numero limitato di persone predeterminate e i servizi di comunicazione interpersonale, come i servizi di messaggistica o di posta elettronica (Considerando 14).
[52] Sempre che l'integrazione di tale funzionalità non sia un mezzo per eludere l'applicabilità delle norme del regolamento applicabili alle piattaforme online.
[53] La stessa logica è seguita dalla Direttiva sui servizi media audiovisivi 2018/1808 del 14 novembre 2018, GUUE (2018) L 303/69.

relative ai commenti di un quotidiano *online*, ove sia evidente che tale attività sia accessoria al servizio principale rappresentato dalla pubblicazione di notizie sotto la responsabilità editoriale dell'editore.

Nell'ambito della categoria delle piattaforme, inoltre, obblighi specifici sono riservati alle "**piattaforme online di dimensioni molto grandi**" per la gestione dei rischi sistemici, la cui definizione non è fornita all'Art. 2 ma direttamente dall'Art. 25 e che ricomprende le "piattaforme online che prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni", calcolato conformemente a metodologie stabilite dalla Commissione in atti delegati.

Merita sin da ora rilevare come le definizioni di "piattaforma" adottate dalla Proposta DSA non coincidano con le definizioni contenute in altri strumenti normativi, rischiando di creare incoerenze sistematiche. Ad esempio: il Regolamento (UE) 2019/1150 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online ('**Regolamento P2B**') è applicabile ai "servizi di intermediazione online"[54]; l'Art. 17 della Direttiva CDSM disciplina la responsabilità dei "prestatori di servizi di condivisione di contenuti online" per l'utilizzo di contenuti protetti dal diritto d'autore; la Direttiva SMAV impone determinati obblighi per i "servizio di piattaforma per la condivisione di video"; la proposta di DMA si applica ai "servizi di piattaforma di base forniti o offerti dai gatekeeper", ovvero un soggetto che "ha un impatto significativo sul mercato interno; gestisce un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali; detiene una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro".

Senza poter al momento entrare nel dettaglio di tali regole, si segnala che una tale discrepanza di definizioni potrebbe avere un impatto concreto con riferimento all'interazione tra la disciplina orizzontale del DSA e le discipline settoriali vigenti, in quanto l'inquadramento in tali categorie soggettive potrebbe innescare l'applicazione di una *lex specialis* ed escludere l'applicazione del DSA. Potrebbe, inoltre, creare incertezza giuridica o obblighi sproporzionati in capo ad alcune categorie di soggetti.

Per completezza, gli altri soggetti elencati dal DSA sono i "**destinatari del servizio**", ovvero qualsiasi persona fisica o giuridica che utilizza il servizio intermediario in questione (Art. 2(b)), i "**consumatori**" e gli "**operatori commerciali**" e, infine, le Autorità competenti e i "**coordinatori nazionali dei servizi digitali**", oltre al Comitato europeo per i servizi digitali (di seguito il "Comitato", *i.e.* il gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari), di cui si tratterà *infra* nel §2.3 (dedicato a esecuzione ed *enforcement*).

2.2 La responsabilità delle piattaforme: esenzioni e nuovi obblighi.

[54] GUUE (2019) L 186/57.

Nel disciplinare la responsabilità dei servizi di intermediazione, il DSA prevede anzitutto disposizioni sull'esenzione dalla responsabilità dei prestatori di servizi intermediari per le informazioni fornite da terzi che essi trasmettono e memorizzano, compresi contenuti illeciti o contraffattori.

Coerentemente all'approccio della Direttiva e-commerce, il DSA stabilisce il divieto di imporre a tali prestatori obblighi generali di sorveglianza o di accertamento attivo dei fatti ed impone un obbligo in relazione agli ordini delle autorità giudiziarie o amministrative nazionali di contrastare i contenuti illegali e di fornire informazioni. L'unica novità introdotta si riferisce alla *good samaritan clause*, di cui si discuterà più diffusamente *infra.*

Dopo aver delineato tali principi generali, i successivi capi della Proposta delineano un quadro di obblighi specifici di diligenza che si potrebbe definire ***"a geometria variabile"***, basato sul ruolo e sulla dimensione delle varie categorie coinvolte.

Come dimostra la figura di cui sotto, sono previsti, infatti, (i) obblighi applicabili a tutti i prestatori di servizi intermediari, (ii) obblighi aggiuntivi applicabili ai prestatori di servizi di *hosting* (iii) obblighi aggiuntivi applicabili a tutte le piattaforme *online* e, infine, (iv) ulteriori obblighi aggiuntivi a carico delle piattaforme *online* di dimensioni molto grandi per la gestione dei rischi sistemici.

Merita rilevare come, sebbene la proposta DSA si concentri sulla responsabilità dei servizi intermediari e sugli obblighi comportamentali e di diligenza "per un ambiente online trasparente e sicuro", il Considerando 26 sottolinei che "nonostante il ruolo generalmente importante svolto da tali prestatori, il problema dei contenuti e delle attività illegali online non dovrebbe essere affrontato concentrandosi esclusivamente sulla loro responsabilità e sulle loro competenze". Seppur non dettando altri obblighi nei confronti di soggetti diversi dai "servizi intermediari", la Proposta sembra richiamare l'attenzione anche sulla responsabilità di altri soggetti, quali: (i) i destinatari dei servizi per i contenuti illegali che forniscono e che possono diffondere attraverso servizi intermediari, ove le norme applicabili del diritto dell'Unione e nazionale che determinano tale responsabilità lo prevedano; (ii) i moderatori dei gruppi negli ambienti online chiusi, in particolare nel caso di grandi gruppi, affinché contribuiscano a evitare la diffusione di contenuti illegali online, conformemente al diritto applicabile. La Proposta sottolinea, inoltre, la necessità di limitare il coinvolgimento dei soggetti intermediari, rivolgendo richieste ed ordini "al soggetto che dispone della capacità tecnica e operativa per contrastare gli specifici contenuti illegali" come argine "agli eventuali effetti negativi in termini di disponibilità e accessibilità delle informazioni che non sono contenuti illegali".

2.2.1 Esenzioni.

La disciplina delle esenzioni alla responsabilità coincide con quella della Direttiva *e-commerce*. Infatti, la proposta di Regolamento riproduce – con qualche mera modifica formale – il testo degli articoli da 12 a 15 della Direttiva 2000/31/CE, che contestualmente abroga.[55] Pertanto, gli Articoli da 3 a 5

[55] Cfr. Art. 71. È necessario menzionare, inoltre, che il Considerando 19 conferma espressamente l'attualità dell'interpretazione della Corte di giustizia resa in vigenza del precedente quadro normativo.

riproducono le definizioni[56] ed esenzioni del previgente quadro normativo pur facendo in ogni caso salva la possibilità per gli intermediari di essere soggetti destinatari di azioni inibitore.[57]

A tal proposito, il Considerando 17 chiarisce anche che le norme in questione non dovrebbero essere intese come un test per verificare la responsabilità di un prestatore, in quanto tale condizione deve essere determinata in base alle norme del diritto UE o nazionale a ciò preposte. Lo stesso Considerando sottolinea come tali esenzioni abbiano, in ogni caso, portata orizzontale, applicandosi "in relazione a qualsiasi tipo di responsabilità per qualsiasi tipo di contenuto illegale, indipendentemente dall'oggetto preciso o dalla natura esatta di tali leggi".

Nel merito, l'Articolo 3 attiene agli intermediari di semplice trasporto ("*mere conduit*") che svolgono un'attività limitata a trasmettere informazioni fornite da terzi, o nel fornire un accesso alla rete di comunicazione. In tale ipotesi, l'intermediario non è responsabile delle informazioni trasmesse a condizione che egli non dia origine alla trasmissione e non selezioni né modifichi il destinatario dell'informazione od il suo contenuto.

L'Articolo 4 definisce invece l'attività di memorizzazione temporanea ("*caching*") quale attività consistente nel trasmettere informazioni fornite da terzi che l'intermediario memorizza in maniera automatica, intermedia e temporanea al solo scopo di rendere più efficiente la loro comunicazione ad altri soggetti che lo richiedano. In tal caso, l'esonero da responsabilità è condizionato alla circostanza che l'intermediario non modifichi le informazioni; rispetti le condizioni di accesso alle informazioni e le norme sul loro aggiornamento; non interferisca con l'uso lecito della tecnologia e comunque agisca prontamente per rimuovere le informazioni o per disabilitare l'accesso, non appena venga "*effettivamente a conoscenza*" del fatto che le informazioni all'origine della trasmissione sono state rimosse o che l'accesso alle stesse è stato disabilitato, anche per decisione di un'autorità pubblica.

L'Articolo 5, infine, attiene alla categoria di intermediari più rilevante per le piattaforme *online* e che anche in via giurisprudenziale ha creato più dibattito ed incertezze: gli *hosting provider*. È *hosting provider* l'intermediario che memorizza le informazioni fornite da terzi. Questo soggetto non è responsabile delle informazioni memorizzate, a condizione che lo stesso non sia effettivamente a conoscenza delle attività o dei contenuti illegali che ospita e comunque agisca "immediatamente" per rimuovere i contenuti illegali o per disabilitarne l'accesso non appena venga a conoscenza di tali attività o contenuti illegali "o diviene consapevole di tali fatti o circostanze".[58] Lo stesso articolo chiarisce che, per quanto attiene a domande risarcitorie, l'*hosting* è esonerato da responsabilità a condizione che lo stesso non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti.

[56] Per quanto attiene alle definizioni, il Considerando 27 da atto dell'evoluzione tecnologica intervenuta dal 2000, la quale ha reso l'ecosistema online sempre più complesso. Tale complessità imporrebbe che "anche i prestatori di servizi che stabiliscono e agevolano l'architettura logica di base e il corretto funzionamento di Internet, comprese le funzioni tecniche ausiliarie, possono beneficiare delle esenzioni dalla responsabilità stabilite nel presente regolamento, nella misura in cui i loro servizi si qualificano come ***mere conduit, caching o hosting***". Sono in particolare menzionati i servizi di reti locali senza fili, di sistema dei nomi di dominio (DNS), di registro dei nomi di dominio di primo livello, delle autorità di certificazione che rilasciano certificati digitali o reti per la diffusione di contenuti che abilitano o migliorano le funzioni di altri prestatori di servizi intermediari. Accanto a questi intermediari tecnici, sono altresì menzionati i servizi utilizzati per le comunicazioni come il Voice over IP, i servizi di messaggistica e i servizi di posta elettronica basati sul web, in cui la comunicazione avviene tramite un servizio di accesso a Internet ed è chiarito che: "[a]nche tali servizi possono beneficiare delle esenzioni dalla responsabilità, nella misura in cui si qualificano come servizi di ***mere conduit, caching o hosting***".

[57] Considerando 24.

[58] Il Considerando 22 fa espresso riferimento alla necessità che la disabilitazione dell'accesso o la rimozione dei contenuti avvenga nel rispetto del principio della libertà di espressione.

Ancora, l'Articolo 5 individua delle ipotesi in cui l'esonero da responsabilità previsto dal primo paragrafo è escluso. In particolare, tale esonero da responsabilità non si applica nel caso di ruolo attivo del prestatore del servizio, atto a conferirgli la conoscenza o il controllo di tali informazioni (Considerando 18), come nel caso in cui il rapporto tra i terzi ed il prestatore sia invertito, ovvero quando il destinatario del servizio agisce sotto l'autorità o il controllo o la responsabilità editoriale del prestatore.

In ogni caso, l'esonero da responsabilità non si applica in relazione alla responsabilità prevista dalla normativa in materia di protezione dei consumatori per le piattaforme *online* che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, qualora tali piattaforme presentino informazioni o rendano altrimenti possibile l'operazione "in modo tale da indurre un consumatore medio e ragionevolmente informato a ritenere che le informazioni, o il prodotto o il servizio oggetto dell'operazione, siano forniti dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo".

Alla luce di ciò, sebbene lo stesso Regolamento faccia salva la giurisprudenza della Corte di giustizia, non sembra però incorporarla testualmente in quanto il riferimento alle categorie e ai principi elaborati a livello giurisprudenziale sono molto limitati.

Per quanto attiene in particolare alla categoria degli *hosting*, ci si sarebbe augurata una codificazione della distinzione elaborata in via interpretativa tra hosting attivo e passivo; invece, tale richiamo è limitato al Considerando 18. Questo chiarisce in particolare che le esenzioni dalla responsabilità non dovrebbero applicarsi qualora l'intermediario non adotti un comportamento neutro, ovvero puramente tecnico, ma piuttosto "*svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni*".[59] In ogni caso, è chiarito, le esenzioni non dovrebbero applicarsi alle ipotesi in cui le informazioni non siano rese da terzi o dai destinatari del servizio, ma dallo stesso intermediario, o sotto sua responsabilità editoriale (concetto non definito dal DSA).

Il Considerando 22, inoltre, aggiunge che "il prestatore può effettivamente acquisire tale conoscenza o consapevolezza", che esclude il beneficio dell'esenzione di responsabilità, "in particolare mediante indagini volontarie o notifiche inviategli da persone o enti conformemente al presente regolamento, nella misura in cui tali notifiche sono sufficientemente precise e dimostrate da consentire a un operatore economico diligente di individuare ragionevolmente, valutare e, se del caso, contrastare i presunti contenuti illegali".

Infine, l'Articolo 7 riproduce il principio di **assenza di obblighi generali di sorveglianza** e **di accertamento attivo di fatti o circostanze "che indichino la presenza di attività illegali".**

È invece del tutto innovativa – anche se ampiamente richiesta dalla dottrina[60] e dagli stessi *stakeholders* – la norma contenuta all'Articolo 6, rubricato "Indagini volontarie promosse di propria iniziativa e rispetto degli obblighi normativi". Questa costituisce la **c.d. *good-samaritan clause***, che consente agli intermediari di avvalersi dell'esenzione dalla responsabilità prevista agli articoli

[59] Si consideri anche il contenuto dei Considerando 20 e 21. Il Considerando 20 chiarisce che non è neutra la condotta dell'intermediario che collabora con un destinatario dei servizi al fine di commettere attività illegali. Il Considerando 21 aggiunge poi che è neutra una condotta per cui l'intermediario non sia in alcun modo coinvolto nella manipolazione delle informazioni trasmesse, con la sola esclusione di quelle aventi carattere tecnico.

[60] Si vedano, di recente, Miriam C. Buiten, Alexandre de Streel, e Martin Peitz, ***Rethinking liability rules for online hosting platforms***, 28 International Journal of Law and Information Technology 139 (2020).

precedenti anche nelle ipotesi in cui svolgano di propria iniziativa indagini o attività volontarie volte ad individuare e rimuovere contenuti illegali o a disabilitarne l'accesso – "purché tali attività siano svolte in buona fede e in modo diligente"[61]. Tale approccio, già presente nel sistema statunitense, mira a non disincentivare i fornitori di servizi *online* ad intraprendere misure proattive tese ad accrescere il loro livello di conoscenza sulle condotte illecite perpetrate sulle loro piattaforme (si veda *infra*).

Da ultimo, la proposta DSA descrive agli Artt. 8 e 9 il contenuto degli ordini nazionali della autorità amministrative o giurisdizionali di contrasto ai contenuti illegali e di richiesta di informazioni rivolti ai prestatori di servizi intermediari, richiamando l'attenzione in particolare sulla necessità che tali ordini siano motivati[62] e rechino informazioni sui mezzi di ricorso a disposizione del prestatore e del destinatario del servizio in questione. Le norme chiariscono l'ambito di applicazione territoriale degli ordini (*supra*, §2.1.1.) ed alcuni meccanismi di informazione e raccordo internazionale tra autorità. Tali disposizioni non pregiudicano le prescrizioni stabilite dal diritto processuale penale nazionale in conformità al diritto dell'Unione.

2.2.2 Obblighi applicabili a tutti i prestatori di servizi intermediari.

Per quanto riguarda gli obblighi imposti a tutti i prestatori di servizi intermediari, la Proposta di DSA prevede alcuni obblighi minimi per consentire trasparenza (i) nei confronti delle autorità e (ii) nei confronti degli utenti e dei destinatari dei servizi digitali.

Gli Artt. 10 e 11, anzitutto, impongono obblighi procedurali per semplificare la comunicazione tra intermediari ed autorità degli Stati membri, la Commissione e il Comitato, come l'obbligo di istituire punti di contatto unici con cui comunicare per via elettronica in via diretta con le autorità e l'obbligo di nomina di un rappresentante legale in uno degli Stati membri per i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che offrono servizi nell'Unione, al fine di facilitare la vigilanza e l'esecuzione del regolamento da parte delle autorità.

Gli Articoli 12 e 13 impongono a tutti i prestatori intermediari obblighi di trasparenza e tutela nei confronti dei propri utenti (destinatari del servizio).

L'Art. 12, a tal fine, disciplina norme sul contenuto, sull'applicazione e sull'esecuzione delle condizioni generali predisposte dai prestatori di servizi intermediari. I servizi intermediari dovranno rendere note le restrizioni che impongono in relazione all'uso dei loro servizi ai destinatari dei servizi. "Tali informazioni riguardano tra l'altro le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana". Tali informazioni devono essere contenute nelle condizioni generali del servizio, redatte in un linguaggio chiaro e privo di ambiguità e sono disponibili al pubblico in un formato facilmente

[61] Considerando 25.

[62] Quanto agli ordini di contrasto ai contenuti illegali, l'ordine deve contenere "la motivazione per cui le informazioni costituiscono contenuti illegali, mediante un riferimento alla specifica disposizione del diritto dell'Unione o nazionale violata; [e] uno o più indirizzi URL (Uniform Resource Locator) esatti e, se necessario, informazioni supplementari che consentano l'identificazione dei contenuti illegali in questione"; quanto agli ordini di fornire informazioni, essi dovranno contenere "una motivazione dell'obiettivo perseguito con la richiesta di tali informazioni e delle ragioni per cui la trasmissione di tali informazioni è un adempimento necessario e proporzionato per accertare il rispetto delle norme dell'Unione o nazionali applicabili da parte dei destinatari dei servizi intermediari, a meno che una simile motivazione non possa essere fornita per motivi connessi ad attività di prevenzione, indagine, accertamento e perseguimento di reati".

accessibile. Così, se un intermediario utilizza procedure automatizzate o umane per la verifica o la moderazione dei contenuti (come procedure per prevenire eventuali contraffazioni) tali modalità dovranno essere rese note ai destinatari del servizio.

L'Art. 12 aggiunge, inoltre, l'obbligo per i prestatori di applicare e far rispettare tali restrizioni "in modo diligente, obiettivo e proporzionato", "tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali applicabili dei destinatari del servizio sanciti dalla Carta". L'Art. 13 aggiunge (per tutti gli intermediari che non siano microimprese o piccole imprese) obblighi di comunicazione trasparente per quanto riguarda la rimozione delle informazioni che siano considerate contenuti illegali o contrari alle condizioni generali dei prestatori e la disabilitazione dell'accesso a tali informazioni, attraverso la pubblicazione di relazioni almeno annuali.

Tali relazioni comprendono, in particolare, informazioni sui seguenti elementi, a seconda dei casi: "a) il numero di ordini ricevuti dalle autorità degli Stati membri, classificati in base al tipo di contenuti illegali in questione, compresi gli ordini emessi a norma degli Articoli 8 e 9, e il tempo medio necessario per intraprendere le azioni indicate in tali ordini; b) il numero di notifiche presentate a norma dell'Articolo 14, classificate in base al tipo di contenuto illegale presunto di cui trattasi, nonché eventuali azioni intraprese in applicazione delle notifiche, specificando se l'azione sia stata avviata in virtù di disposizioni normative oppure delle condizioni generali del prestatore, e il tempo medio necessario per intraprendere l'azione; c) le attività di moderazione dei contenuti avviate di propria iniziativa dai prestatori, compresi il numero e il tipo di misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità delle informazioni fornite dai destinatari del servizio e sulla capacità dei destinatari di fornire informazioni, classificate in base al tipo di motivazione e alle ragioni per l'adozione di tali misure; d) il numero di reclami ricevuti tramite il sistema interno di gestione dei reclami di cui all'Articolo 17, la base di tali reclami, le decisioni adottate in relazione a tali reclami, il tempo medio necessario per adottare tali decisioni e il numero di casi in cui tali decisioni sono state revocate".

Tutti gli intermediari
• Obbligo di istituire punti di contatto unici per tutto il territorio dell'UE. • Obbligo di nomina di un rappresentante legale in uno degli Stati membri per i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che offrono servizi nel suo territorio. • Termini e condizioni d'uso: necessario rispetto dei principi di trasparenza e chiarezza, in particolare con riferimento alle politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana. • Obbligo per i prestatori di applicare e far rispettare tali restrizioni in modo diligente, obiettivo e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte.

2.2.3 Disposizioni aggiuntive applicabili ai prestatori di servizi di hosting, comprese le piattaforme online.

L'Articolo 14 (**Meccanismo di notifica e azione,** altrimenti detto **"*notice and action*"**) è una disposizione centrale all'impianto del DSA, in quanto recepisce le critiche mosse (dalla dottrina, quanto dagli operatori) all'assenza di un sistema armonizzato di *notice and take-down* a livello europeo. [63] Mancando tale armonizzazione nella Direttiva *e-commerce*, infatti, la disciplina di sistemi di *notice and take down/notice and action/notice and stay down* è stata sinora lasciata alla auto-organizzazione delle piattaforme (che si sono sostanzialmente ispirate al *Digital Millennium Copyright Act*, *DMCA*, statunitense), mentre alcuni Stati Membri hanno iniziato a prevedere una disciplina autonoma nazionale per alcune categorie di contenuti[64], con rischio di frammentazione del mercato interno.

Coerentemente, la norma proposta nel DSA dispone che i prestatori di servizi di *hosting* (a prescindere dalle loro dimensioni) devono adottare meccanismi per consentire a qualsiasi persona o ente di notificare la presenza sui servizi di informazioni specifiche che ritengano costituire contenuti illegali. È espressamente chiarito che tali meccanismi devono essere di facile accesso e uso e consentire una gestione elettronica dell'istanza. I prestatori di servizi di *hosting* sono infatti considerati dal DSA come soggetti aventi un ruolo tale da avere un notevole impatto sul contrasto ai contenuti illegali *online* (Considerando 40). I sistemi di notifica devono essere tali da indurre ("facilitare") la presentazione di notifiche sufficientemente precise e adeguatamente motivate, in base alle quali un operatore economico diligente può rilevare l'illegalità dei contenuti in questione.

Il paragrafo secondo specifica anche il contenuto dell'istanza, peraltro attraverso una previsione molto simile al DMCA statunitense relativamente al *copyright*: a) una spiegazione dei motivi per cui l'istante ritiene che le informazioni in questione costituiscano contenuti illegali; b) l'indicazione dell'ubicazione elettronica di tali informazioni (tramite indirizzo URL) oppure eventuali informazioni supplementari che consentano di individuare comunque il contenuto; c) l'identità e i contatti del soggetto notificante, (tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della direttiva 2011/93/UE); d) una dichiarazione che confermi la buona fede dell'istante.

Il paragrafo 3 istituisce una presunzione a carico dell'intermediario, disponendo che le notifiche contenenti gli elementi previsti dal Regolamento permettono di acquisire una "conoscenza o consapevolezza effettiva" dell'attività ai fini dell'Articolo 5, e dunque della responsabilità del fornitore di servizi. Tale disposizione chiarirebbe il problema interpretativo che si è posto sinora relativo alla soglia di conoscenza dell'intermediario in grado di escludere l'esenzione dalla responsabilità prevista dalla Direttiva *e-commerce*. Ricevuta la notifica, il prestatore "senza indebito ritardo" trasmette all'istante la propria decisione fornendo informazioni sulle modalità adottate per la decisione,

[63] Il Considerando 40 fa espresso riferimento alla nozione di "***notice and action***" chiarendo anche alcuni aspetti incerti nella disciplina vigente. Innanzitutto, la possibilità di notificare più contenuti specifici presunti illegali mediante un'unica notifica. In secondo luogo, l'applicabilità di tale obbligo di predisporre meccanismi di notifica anche a soggetti diversi dalle piattaforme, quali i servizi di condivisione e memorizzazione di file, i servizi di web hosting, ai server di annunci e ai ***pastebin***, qualora rivestano il ruolo di hosting. Il Considerando 41 risponde idealmente alle critiche mosse rispetto all'assenza di un meccanismo europeo di notifica chiarendo che "[l]e norme relative a tali meccanismi di notifica e azione dovrebbero essere armonizzate a livello dell'Unione, in modo da consentire il trattamento tempestivo, diligente e obiettivo delle notifiche sulla base di norme uniformi, trasparenti e chiare, che forniscano solide garanzie a tutela dei diritti e degli interessi legittimi di tutte le parti interessate, in particolare dei loro diritti fondamentali garantiti dalla Carta, indipendentemente dallo Stato membro nel quale tali parti sono stabilite o residenti e dal settore del diritto in questione".

[64] Cfr. il Network Enforcement Act tedesco (Netzwerkdurchsetzungsgesetz, NetzDG) a proposito di ***fake news*** sui social network.

sull'eventuale uso di strumenti automatizzati per tali processi di trattamento o decisione, nonché sui mezzi di ricorso disponibili. Per quanto attiene al merito della decisione, i prestatori di servizi di *hosting* devono agire in modo tempestivo, diligente e obiettivo.

Se la norma che istituisce il meccanismo di notifica e azione ha portata sostanzialmente generale, la vera novità del DSA è costituita dall'Articolo 15, che **chiarisce il portato dell'obbligo di motivazione e di comunicazione ai destinatari del servizio della decisione di rimozione e disabilitazione all'accesso ai contenuti illeciti**.

L'obbligo di comunicazione deve essere assolto al più tardi al momento della rimozione o della disabilitazione dell'accesso, fornendo una motivazione chiara e specifica di tale decisione.

Per quanto attiene invece alla motivazione, la stessa deve contenere informazioni chiare, facilmente comprensibili e precise rispetto - almeno - a: la modalità di intervento (rimozione o disabilitazione dell'accesso); la portata territoriale della disabilitazione dell'accesso; gli elementi su cui si basa la decisione ed il suo presupposto (una notifica, o rilevazione automatica); l'eventuale utilizzo di strumenti automatizzati per l'adozione della decisione o per l'individuazione del contenuto; la base giuridica invocata e una spiegazione delle ragioni per cui l'informazione è considerata contenuto illegale in applicazione di tale base giuridica; la clausola delle condizioni generali di servizio invocata in caso l'intervento sia dettato dalla loro violazione e una spiegazione delle ragioni per cui le informazioni sono ritenute incompatibili con tale clausola; informazioni sui mezzi di ricorso a disposizione (sia interni che giudiziali o ADR).

Tali informazioni sono funzionali a consentire al destinatario della decisione di esercitare utilmente il diritto di difesa e contraddittorio a lui garantito, ed esperire eventualmente i mezzi di ricorso previsti dalla legge.

Infine, l'Articolo 15 prevede che le decisioni (senza indicazione dei dati personali) siano **pubblicate** in una banca dati pubblicamente accessibile gestita dalla Commissione.

Merita rilevare già da subito come il DSA non sembra prevedere un corrispondente procedimento di "*notice and stay down*", ovverosia un obbligo di impedire *ex ante* la fornitura di contenuti illeciti già segnalati in modo circostanziato, impedendo così in via preventiva la reiterazione di attività illecite anche senza necessità di nuova notifica (*supra*, § 1 e *infra*, § 3).

Hosting Providers
• Obbligo di istituire punti di contatto unici per tutto il territorio dell'UE. • Obbligo di nomina di un rappresentante legale in uno degli Stati membri per i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che offrono servizi nel suo territorio. • Termini e condizioni d'uso: necessario rispetto dei principi di trasparenza e chiarezza, in particolare con riferimento alle politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana.

- Obbligo per i prestatori di applicare e far rispettare tali restrizioni in modo diligente, obiettivo e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte.
- Obblighi di comunicazione trasparente e motivazione per quanto riguarda la rimozione di contenuti illegali o contrari alle condizioni generali d'uso e la disabilitazione dell'accesso a tali contenuti, attraverso la pubblicazione di relazioni annuali (c.d. obbligo di reporting).
- ***Notice and action***: i prestatori di servizi devono adottare meccanismi per consentire a qualsiasi utente di notificare la presenza di contenuti illegali. I sistemi di notifica devono essere tali da facilitare la presentazione di notifiche sufficientemente precise e adeguatamente motivate.
- Ricevuta la notifica, il prestatore senza indebito ritardo trasmette all'istante la propria decisione fornendo informazioni sulle modalità adottate per la decisione, sull'eventuale uso di strumenti automatizzati per tali processi di trattamento o decisione, nonché sui mezzi di ricorso disponibili.
- Obbligo di notifica, motivazione e pubblicazione delle decisioni.

2.2.4 Disposizioni aggiuntive applicabili alle piattaforme online.

Nella logica della struttura a geometria variabile del DSA impostata dalla Commissione, la sezione 3 aggiunge ulteriori previsioni a carico delle sole piattaforme *online*, ovvero di quei prestatori di servizi di *hosting* che non si limitano a memorizzare le informazioni, ma, su richiesta di un destinatario del servizio, diffondono al pubblico tali informazioni (come i *social network* o le piattaforme di *e-commerce*).

L'Art. 16, a tal proposito, tuttavia, esclude espressamente dall'ambito di applicazione di tale sezione le microimprese e le piccole imprese, per non creare obblighi sproporzionati. Ciò deve ritenersi limitato all'ipotesi in cui - in ragione del loro raggio d'azione e del loro impatto - esse non possano comunque qualificarsi come piattaforme *online* di dimensioni molto grandi. Inoltre, l'esenzione non incide sulla capacità di tali imprese di istituire, su base volontaria, un sistema che rispetti uno o più di tali obblighi (Considerando 43).

Venendo al merito delle disposizioni relative alle piattaforme *online*, l'Articolo 17 (**Sistema interno di gestione dei reclami**) prevede che le piattaforme devono fornire ai destinatari del servizio, per un periodo di almeno sei mesi dalla decisione, l'accesso a un sistema interno di gestione dei reclami efficace, che consenta di presentare – elettronicamente, gratuitamente e facilmente accessibili – reclami contro le decisioni adottate dalla piattaforma e relative alla rimozione o disabilitazione dell'accesso alle informazioni; alla sospensione o cessazione in tutto o in parte della prestazione del servizio ai destinatari; alla sospensione o cessazione dell'account del destinatario.

Le piattaforme gestiscono i reclami presentati attraverso il loro sistema interno in modo tempestivo, diligente e obiettivo e comunicano senza indebito ritardo ai reclamanti la decisione adottata

informandoli della possibilità di ricorrere a strumenti di risoluzione extragiudiziale delle controversie ai sensi dell'Art. 18 e di tutte le altre possibilità di ricorso a loro disposizione.

Infine, è chiarito che le piattaforme provvedono affinché le decisioni sui reclami non siano prese avvalendosi esclusivamente di strumenti automatizzati. Tale norma prende evidentemente in considerazione i limiti delle decisioni algoritmiche laddove vi siano elementi valutativi "di contesto" non interamente automatizzabili.

Sia nella fase di decisione che nella fase di reclamo della decisione, particolare attenzione deve essere data all'impatto che tali decisioni hanno "sui diritti e sui legittimi interessi di tutte le parti interessate in particolare dei loro diritti fondamentali garantiti dalla Carta, indipendentemente dallo Stato membro nel quale tali parti sono stabilite o residenti e dal settore del diritto in questione" (Considerando 41). Questa attenzione risulta particolarmente importante, ma anche particolarmente problematica in sede di attuazione degli obblighi a carico delle piattaforme poste nella condizione di gestire bilanciamenti di interessi particolarmente delicati, che, nel contesto che occupa, sottintendono il rapporto tra i diritti di proprietà industriale considerati e i relativi limiti per consentire le utilizzazioni libere altrui.

Il DSA si premura, inoltre, all'Art. 18 di prevedere regole sulla risoluzione extragiudiziale delle controversie al fine di consentire ai destinatari del servizio ai quali sono rivolte le decisioni di cui all'articolo 17(1), fermo restando il diritto di adire un'autorità giurisdizionale, di scegliere qualunque organismo certificato in conformità al paragrafo 2 ai fini della risoluzione delle controversie inerenti a tali decisioni, compresi i reclami che non è stato possibile risolvere mediante il sistema interno di gestione dei reclami di cui a tale articolo.

Le piattaforme *online* a tal fine si impegnano in buona fede con l'organismo selezionato al fine di risolvere la controversia e sono vincolate dalla decisione adottata da tale organismo. In particolare, ai sensi del comma 3, è previsto che, ove la controversia sia risolta in questa sede favorevolmente per il destinatario del servizio, la piattaforma *online* rimborsa al destinatario i diritti e le altre spese ragionevoli che il destinatario ha sostenuto o deve sostenere in relazione alla risoluzione della controversia. Viceversa, se l'organismo risolve la controversia a favore della piattaforma *online*, il destinatario non è tenuto a rimborsare i diritti e le altre spese alla piattaforma *online*.

Al fine di rendere più rapido ed affidabile il contrasto ai contenuti illegali *online*, le piattaforme *online* attribuiscono priorità nelle proprie procedure di "notifica ed azione" ai cd. **segnalatori attendibili** (***trusted flaggers***). Ai sensi dell'Art. 19, tali soggetti sono qualificati come tali dal coordinatore dei servizi digitali dello Stato membro in cui è stabilito il richiedente, a condizione che quest'ultimo abbia dimostrato di soddisfare tutte le condizioni seguenti: a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) rappresenta interessi collettivi ed è indipendente da qualsiasi piattaforma *online*; c) svolge le proprie attività al fine di presentare le notifiche in modo tempestivo, diligente e obiettivo.

Il Considerando 46 specifica che la qualifica dovrebbe essere preferibilmente riconosciuta a enti, non a persone fisiche, che abbiano "dimostrato, tra l'altro, di disporre di capacità e competenze particolari nella lotta ai contenuti illegali, di rappresentare interessi collettivi e di svolgere le proprie attività in modo diligente e obiettivo". La natura di tali enti può essere pubblica, come ad esempio per i contenuti

terroristici le stesse unità addette alle segnalazioni su Internet delle autorità di contrasto nazionali o l'Europol, oppure organizzazioni non governative e organismi semipubblici (come organizzazioni facenti parte della rete di linee di emergenza per la segnalazione di materiale pedopornografico INHOPE e le organizzazioni impegnate nella notifica dei contenuti razzisti e xenofobi illegali online). Per i diritti di proprietà intellettuale, il Considerando 46 menziona espressamente l'esempio delle organizzazioni del settore e dei titolari dei diritti che abbiano dimostrato di soddisfare le condizioni applicabili.

Una volta riconosciuta tale qualifica, i coordinatori dei servizi digitali comunicano alla Commissione e al Comitato gli enti selezionati, che sono inseriti a cura della Commissione in una banca dati accessibile al pubblico.

Le piattaforme *online* segnalano al coordinatore dei servizi digitali l'eventuale ricezione da parte di un segnalatore attendibile di un numero significativo di notifiche non sufficientemente precise o non adeguatamente motivate ed il coordinatore dei servizi digitali che ha riconosciuto la qualifica di segnalatore attendibile a un ente revoca tale qualifica se accerta, a seguito di un'indagine avviata di propria iniziativa o in base a informazioni ricevute da terzi, comprese le informazioni fornite da una piattaforma online a norma del paragrafo 5 e dopo aver atteso la risposta del segnalatore attendibile, che l'ente non soddisfa più le condizioni di cui al paragrafo 2[65].

Il DSA attribuisce, inoltre, alle piattaforme *online* **l'obbligo di reagire per contrastare abusi dei propri servizi da parte dei destinatari dei servizi o dei segnalanti** (Art. 20). Ferma restando la facoltà di porre in essere altre azioni ai sensi del diritto UE o nazionale applicabile (Considerando 47), dopo aver emesso un avviso preventivo, le piattaforme *online* sono tenute a (i) sospendere per un periodo di tempo ragionevole la prestazione dei loro servizi ai destinatari del servizio che con frequenza forniscono contenuti manifestamente illegali ed a (ii) sospendere altresì periodo di tempo ragionevole il trattamento delle notifiche e dei reclami presentati da persone, enti o reclamanti che con frequenza presentano notifiche o reclami manifestamente infondati.

La valutazione da parte delle piattaforme degli abusi dei destinatari dei servizi e/o dei segnalanti deve avvenire caso per caso, in modo tempestivo, diligente e obiettivo, tenendo in considerazione tutti i fatti e di tutte le circostanze pertinenti che risultano dalle informazioni a disposizione della piattaforma online, inclusi: a) il numero, in termini assoluti, di contenuti manifestamente illegali o di notifiche o reclami manifestamente infondati presentati durante l'anno precedente; b) la relativa proporzione rispetto al numero totale di informazioni fornite o di notifiche presentate nell'anno precedente; c) la gravità degli abusi e delle relative conseguenze; d) l'intenzione del destinatario, della persona, dell'ente o del reclamante.

Le politiche delle piattaforme relative agli abusi devono essere chiaramente e dettagliatamente definite nelle condizioni generali delle stesse.

Al Considerando 47, inoltre, il DSA specifica che tali norme "lasciano impregiudicata l'eventuale possibilità prevista dal diritto dell'Unione o nazionale di considerare responsabili, anche a fini di risarcimento dei danni, le persone che hanno commesso abusi".

[65] Ai sensi del comma 7 "[l]a Commissione, previa consultazione del comitato, può emanare orientamenti per assistere le piattaforme online e i coordinatori dei servizi digitali nell'applicazione dei paragrafi 5 e 6".

Qualora la piattaforma, inoltre, venga a conoscenza di informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, la piattaforma *online* è tenuta ad informare senza indugio le autorità giudiziarie o di contrasto dello Stato membro o degli Stati membri interessati in merito ai propri sospetti, fornendo tutte le informazioni pertinenti disponibili (Art. 21, *infra* §2.4).

Altra norma di fondamentale importanza nel contesto che occupa attiene agli obblighi per le piattaforme di tracciabilità degli operatori commerciali che rispondono al principio del "***know-your-business-customer***" (**KYBC**) (Art. 22). Come chiarisce il Considerando 49, "[a]l fine di contribuire a un ambiente online sicuro, affidabile e trasparente per i consumatori, nonché per altre parti interessate quali operatori commerciali concorrenti e titolari di diritti di proprietà intellettuale, e per dissuadere gli operatori commerciali dalla vendita di prodotti o servizi in violazione delle norme applicabili, le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali dovrebbero provvedere affinché tali operatori commerciali siano tracciabili". Qualora nell'ambito dei propri servizi la piattaforma consenta ai consumatori di concludere contratti a distanza con operatori commerciali, dunque, tale piattaforma è tenuta ad ottenere dagli operatori commerciali determinate informazioni essenziali ai fini della tracciabilità, anche ai fini della promozione di messaggi o dell'offerta di prodotti. Tale prescrizione dovrebbe, inoltre, applicarsi anche agli operatori commerciali che promuovono messaggi riguardanti prodotti o servizi per conto di marchi sulla base dei relativi accordi.

Il DSA, inoltre, richiede che la piattaforma **compia sforzi ragionevoli per stabilire l'attendibilità di tali informazioni** e, se ottiene indicazioni secondo le quali le informazioni di cui al paragrafo 1 ricevute dall'operatore commerciale in questione sono inesatte o incomplete, ne richiede la correzione senza indugio o entro il termine stabilito dal diritto dell'Unione e nazionale, a pena di sospensione della prestazione del suo servizio all'operatore commerciale fino a quando la richiesta non sia stata soddisfatta. Tali informazioni sono conservate in modo sicuro per la durata del rapporto contrattuale con l'operatore commerciale interessato ed in seguito cancellate, divulgate a terzi solo se così richiesto dal diritto applicabile (come nel caso di ordini da parte delle autorità competenti ai sensi dell'art. 9) e (per quanto riguarda solo alcune informazioni) messe a disposizione dei destinatari del servizio in modo chiaro, facilmente accessibile e comprensibile.

La piattaforma *online* progetta e organizza la propria interfaccia *online* in modo da consentire agli operatori commerciali di adempiere i loro obblighi riguardanti le informazioni precontrattuali e quelle in materia di sicurezza dei prodotti a norma del diritto dell'Unione applicabile.

Anche in relazione alle attività richieste alle piattaforme online dalla sezione III, sussiste un obbligo di comunicazione trasparente alle autorità competenti, che si aggiungono, per le piattaforme *online* agli obblighi di comunicazione trasparente applicabili a tutti i prestatori di servizi intermediari ai sensi del DSA (Art. 23 - Obblighi di comunicazione trasparente per i fornitori di piattaforme online). Tali obblighi di comunicazione comprendono anche la pubblicazione e la comunicazione di informazioni sul numero medio mensile di destinatari attivi del servizio nell'Unione, utile ai fini della determinazione della qualifica di "piattaforme online di dimensioni molto grandi", soggette ad obblighi ancora ulteriori descritti nel § successivo.

A chiusura della sezione terza, il DSA prevede per le piattaforme *online* che visualizzano **pubblicità sulle loro interfacce online alcuni obblighi di trasparenza** volti a prevenire eventuali rischi "che variano dalla pubblicità che costituisce di per sé contenuto illegale, al contributo a incentivi finanziari per la pubblicazione o l'amplificazione di attività e contenuti online illegali o comunque dannosi fino alla visualizzazione discriminatoria di pubblicità con ripercussioni sulla parità di trattamento e di opportunità dei cittadini" (Considerando 52). È noto, ad esempio, come in certe circostanze la pubblicità possa costituire violazione della disciplina a tutela dei marchi, capace – ad esempio- di indurre in confusione i consumatori sull'origine dei prodotti o di approfittare o recare pregiudizio ai marchi dotati di reputazione. A questo proposito, l'obbligo di informazione a carico delle piattaforme *online* può consentire ai "destinatari del servizio" di comprendere quando e per conto di chi sono visualizzate pubblicità (Art. 24 e Considerando 52). Ferma restando l'applicazione del GDPR, inoltre, i destinatari del servizio dovrebbero "disporre di informazioni sui principali parametri utilizzati per stabilire che vengono mostrate loro pubblicità specifiche, con spiegazioni rilevanti sulla logica seguita a tal fine, anche quando essa è basata sulla profilazione" (Considerando 52).

Piattaforme Online
• Obbligo di istituire punti di contatto unici per tutto il territorio dell'UE. • Obbligo di nomina di un rappresentante legale in uno degli Stati membri per i prestatori di servizi intermediari che non sono stabiliti nell'Unione ma che offrono servizi nel suo territorio. • Termini e condizioni d'uso: necessario rispetto dei principi di trasparenza e chiarezza, in particolare con riferimento alle politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana. • Obbligo per i prestatori di applicare e far rispettare tali restrizioni in modo diligente, obiettivo e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte. • Obblighi di comunicazione trasparente per quanto riguarda la rimozione di contenuti illegali o contrari alle condizioni generali d'uso e la disabilitazione dell'accesso a tali contenuti, attraverso la pubblicazione di relazioni annuali (c.d. obbligo di reporting). • Notice and action: i prestatori di servizi devono adottare meccanismi per consentire a qualsiasi utente di notificare la presenza di contenuti illegali. I sistemi di notifica devono essere tali da facilitare la presentazione di notifiche sufficientemente precise e adeguatamente motivate. • Ricevuta la notifica, il prestatore senza indebito ritardo trasmette all'istante la propria decisione fornendo informazioni sulle modalità adottate per la decisione, sull'eventuale uso di strumenti automatizzati per tali processi di trattamento o decisione, nonché sui mezzi di ricorso disponibili. • Obbligo di notifica, motivazione e pubblicazione delle decisioni. • Gestione dei reclami: i destinatari del servizio, per un periodo di almeno sei mesi dalla decisione, devono avere accesso a un sistema interno di gestione dei reclami efficace, che consenta di presentare – elettronicamente, gratuitamente e facilmente accessibili – reclami contro le decisioni adottate dalla piattaforma e relative alla rimozione o

disabilitazione dell'accesso alle informazioni; alla sospensione o cessazione in tutto o in parte della prestazione del servizio ai destinatari; alla sospensione o cessazione dell'account del destinatario.

- Obbligo di dare priorità nelle proprie procedure di "notifica ed azione" ai cd. segnalatori attendibili (trusted flaggers).
- Obbligo di reagire per contrastare abusi dei propri servizi da parte dei destinatari dei servizi o dei segnalanti.
- Assessment dei rischi (KYBC): le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali dovrebbero provvedere affinché tali operatori commerciali siano tracciabili e a tal fine sono tenute ad ottenere dagli operatori commerciali determinate informazioni e a compiere sforzi ragionevoli per stabilirne l'attendibilità.
- Obbligo di trasparenza delle fonti di pubblicità.
- Obbligo di riportare reati.

2.2.5 Obblighi supplementari a carico delle piattaforme online di dimensioni molto grandi per la gestione dei rischi sistemici

In linea con l'approccio seguito nella proposta di DMA, il DSA introduce un trattamento differenziato degli operatori *online* sulla base della loro dimensione prevedendo obblighi aggiuntivi per quelle che vengono etichettate come piattaforme "*very large*" (VLOP). Il criterio adoperato per la loro individuazione (un numero medio mensile di utenti nell'Unione pari o superiore a 45 milioni) corrisponde, peraltro, ad uno dei criteri utilizzati nel DMA per definire le piattaforme come *gatekeeper*[66].

La *ratio* di tale approccio è esplicitata al Considerando 56, laddove si sottolinea come le piattaforme di dimensioni molto grandi, i cui servizi sono ottimizzati a beneficio di un modello di *business* spesso basato sui proventi pubblicitari, vengano utilizzate in modo tale da influenzare significativamente la sicurezza e il commercio *online*, nonché la formazione dell'opinione pubblica. In assenza di una regolazione ed un *enforcement* efficaci, tali piattaforme sono in grado di fissare le "regole del gioco" senza identificare e mitigare i rischi ed i danni economici e sociali che esse stesse possono procurare. Per queste ragioni, la proposta di DSA mira a responsabilizzare tali piattaforme prevedendo che le stesse debbano valutare i "rischi sistemici" derivanti dal funzionamento ed utilizzo dei propri servizi, al pari dei potenziali abusi commessi dai destinatari degli stessi servizi, e adottare misure appropriate per ridurre e mitigare tali rischi. Ai fini della presente analisi, si rileva come una delle tre principali categorie di rischi sistemici individuati dal DSA attiene alla disseminazione di contenuti illegali (Considerando 57).

In questa prospettiva, l'Articolo 26 impone alle piattaforme di grandi dimensioni di identificare, analizzare e valutare ogni significativo rischio sistemico con specifico riferimento ai servizi offerti, ed il successivo Articolo 27 richiede che le piattaforme adottino misure di **mitigazione di tali rischi** che siano ragionevole, proporzionate, efficaci e ritagliate sugli specifici rischi sistemici previamente

[66] Cfr. Articolo 25(1) del DSA con l'Articolo 3(2)(b) del DMA.

individuati. Come chiarito al Considerando 58 e all'Art. 27(1), tali misure di attenuazione possono anzitutto comprendere il rafforzamento e l'adeguamento dei sistemi di moderazione dei contenuti, dei loro sistemi algoritmici di raccomandazione e delle loro interfacce online, oppure l'adeguamento dei loro processi decisionali o delle loro condizioni generali. Le piattaforme devono altresì prendere in considerazione l'adozione di misure correttive, quali la soppressione degli introiti pubblicitari per specifici contenuti, o altre azioni, quali il miglioramento della visibilità delle fonti di informazione autorevoli. Infine, le piattaforme possono rafforzare i loro processi interni o la vigilanza sulle loro attività, nonché avviare o aumentare la cooperazione con i segnalatori attendibili e con altre piattaforme, anche attraverso codici di condotta e altre misure di autoregolamentazione, quali i protocolli di crisi.

Ai sensi dell'Articolo 28, data la necessità di garantire la verifica da parte di esperti indipendenti, le piattaforme online di dimensioni molto grandi dovrebbero essere chiamate a rispondere, attraverso audit indipendenti, della loro conformità agli obblighi stabiliti nel DSA e, se del caso, agli impegni supplementari assunti a norma di codici di condotta e protocolli di crisi[67]. Una relazione di audit non positiva obbligherà le piattaforme a tener conto delle raccomandazioni in essa contenute al fine di adottare le misure necessarie per attuarle.

Dal momento che un elemento essenziale delle attività delle piattaforma di dimensioni molto grandi consiste nel modo in cui le informazioni sono messe in ordine di priorità e presentate nella interfaccia *online* per facilitare e ottimizzare l'accesso alle stesse da parte dei destinatari dei servizi (Considerando 62), l'Articolo 29 impone alle suddette piattaforme di specificare nelle condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei sistemi di raccomandazione, nonché adoperarsi affinché i destinatari dispongano di opzioni alternative per i principali parametri, comprese opzioni non basate sulla profilazione del destinatario. I sistemi di raccomandazione possono, infatti, avere effetti significativi sulla capacità dei destinatari di reperire informazioni e interagire con esse *online*, e svolgono un ruolo importante nell'amplificazione di determinati messaggi, nella diffusione virale delle informazioni e nella sollecitazione del comportamento *online* (Considerando 62).

Ulteriore elemento caratterizzate il modello di *business* di numerose piattaforme *very large* che richiede vigilanza pubblica e regolamentare è la presenza di sistemi pubblicitari. A tal proposito, l'Articolo 30 obbliga tali piattaforme a garantire l'accesso del pubblico ai registri della pubblicità visualizzata sulle loro interfacce per facilitare la vigilanza e la ricerca sui rischi emergenti derivanti dalla distribuzione della pubblicità.

Al fine di vigilare sul rispetto degli obblighi appena descritti, il Coordinatore dei servizi digitali del luogo di stabilimento o la Commissione può chiedere l'accesso a dati specifici o la comunicazione di questi ultimi (Articolo 31). Inoltre, dal momento che le indagini condotte da ricercatori sull'evoluzione e sulla gravità dei rischi sistemici sono considerate particolarmente importanti per ridurre le asimmetrie informative e istituire un sistema resiliente di attenuazione dei rischi (Considerando 64), le piattaformi sono tenute a **fornire ai ricercatori abilitati** (***vetted researchers***) **l'accesso ai dati**.

[67] Si vedano anche i Considerando 60 e 61 del DSA.

In considerazione della complessità del funzionamento dei sistemi utilizzati e i rischi sistemici che essi presentano per la società (Considerando 65), le piattaforme di dimensioni molto grandi sono chiamate a designare responsabili della conformità, qualificati a rendere operative le misure e monitorare la conformità al DSA all'interno dell'organizzazione della piattaforma (Articolo 32).

Infine, le altre prescrizioni in materia di trasparenza già previste dal DSA devono essere integrate da obblighi di trasparenza supplementari quali, in particolare, l'obbligo di riferire in merito alle valutazioni dei rischi svolte e alle successive misure adottate (Articolo 33).

Obblighi supplementari a carico delle piattaforme online di dimensioni molto grandi.
• Valutazione di ogni significativo rischio sistemico con specifico riferimento ai servizi offerti. • Adozione delle misure di mitigazione dei rischi sistemici (adeguamento dei sistemi di moderazione dei contenuti o di raccomandazione, limitazione della pubblicità, rafforzamento dei processi interni o della vigilanza, cooperazione con i segnalatori attendibili e con altre piattaforme online). • Audit indipendenti sulla conformità agli obblighi stabiliti nel DSA. • Divulgazione dei parametri utilizzati nei sistemi di raccomandazione e predisposizione di funzionalità che consentano ai destinatari del servizio di selezionare e modificare l'opzione preferita per i sistemi di raccomandazione. • Accesso ai registri della pubblicità visualizzata sulle interfacce. • Accesso ai dati necessari per monitorare e valutare la conformità al DSA. • Designazione dei responsabili della conformità al DSA. • Divulgazione della relazione sui risultati della valutazione del rischio, delle misure di attenuazione dei rischi individuate e attuate, della relazione di audit e della relazione di attuazione dell'audit.

2.2.6 Altre disposizioni relative agli obblighi in materia di dovere di diligenza.

L'Articolo 34 stabilisce che "la Commissione europea sostiene e promuove lo sviluppo e l'attuazione di **norme settoriali volontarie stabilite dai competenti organismi di normazione europei e internazionali**" per regolare alcune particolari fattispecie, ed in particolare: la presentazione elettronica delle notifiche da parte degli utenti e dei segnalatori attendibili; l'elaborazione di interfacce specifiche, (anche tramite interfacce API)[68] per agevolare il rispetto degli obblighi in materia di

[68] Considerando 66. Il medesimo Considerando chiarisce anche che "[t]ali norme potrebbero essere utili in particolare per i prestatori di servizi intermediari relativamente piccoli".

pubblicità di cui agli Articoli 30 e 31; gli audit delle VLOP; l'interoperabilità dei registri della pubblicità; la trasmissione di dati tra intermediari pubblicitari a sostegno degli obblighi di trasparenza.

Il successivo Articolo 35 (**Codici di condotta**) attiene invece all'incoraggiamento ed agevolazione dell'elaborazione di codici di condotta a livello di Unione per contribuire alla corretta applicazione del regolamento. I codici di condotta sono ritenuti, infatti, strumenti idonei ad affrontare le specificità dei diversi tipi di contenuti illegali e ai rischi sistemici. I codici di condotta devono definire chiaramente i propri obiettivi; contenere indicatori chiave di prestazione per misurare il loro conseguimento;[69] tenere conto delle esigenze e degli interessi di tutte le parti interessate, compresi i cittadini, a livello di Unione; garantire che i partecipanti riferiscano periodicamente alla Commissione e ai rispettivi coordinatori dei servizi digitali in merito a tutte le misure adottate e ai relativi risultati. La Commissione e il Comitato valutano se i codici di condotta rispondano alle finalità e monitorano e valutano periodicamente il conseguimento dei loro obiettivi pubblicando le proprie conclusioni.

Il Regolamento dedica particolare attenzione al tema della pubblicità online, anche con riferimento ai codici di condotta. Infatti, l'Articolo 36 stabilisce che, entro un anno dalla entrata in vigore del Regolamento dovranno essere adottati dei codici di condotta sotto gli auspici della Commissione "tra le piattaforme online e altri prestatori di servizi interessati, quali i prestatori di servizi intermediari per la pubblicità online o le organizzazioni che rappresentano i destinatari del servizio, e le organizzazioni della società civile o le autorità competenti, al fine di contribuire a una maggiore trasparenza della pubblicità online al di là di quanto prescritto dagli articoli 24 e 30."

Lo scopo è quello di garantire che i codici di condotta perseguano un'efficace trasmissione delle informazioni, nel pieno rispetto dei diritti di tutte le parti coinvolte, e della concorrenza, trasparenza ed equità della pubblicità online. Tali codici dovrebbero avere almeno ad oggetto: la trasmissione di informazioni detenute dai prestatori di servizi intermediari per la pubblicità online ai destinatari del servizio; la trasmissione di informazioni detenute dai prestatori di servizi intermediari per la pubblicità online ai registri.[70]

Accanto ai codici di condotta, il Regolamento pone altri strumenti volontari, in particolare i **protocolli di crisi** previsti dall'Articolo 37. Questi sono elaborati, su raccomandazione del Comitato, dalla Commissione "per affrontare situazioni di crisi strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica".[71]

Tali protocolli di crisi comprendono una o più delle misure seguenti: "a) la visualizzazione di informazioni ben evidenziate sulla situazione di crisi fornite dalle autorità degli Stati membri o a livello di Unione; b) la garanzia che il punto di contatto sia responsabile della gestione delle crisi; c) ove

[69] Il Considerando 67 specifica che l'attuazione dei codici di condotta dovrebbe essere misurabile e soggetta a controllo pubblico e che, in determinate circostanze, è importante che le piattaforme online di dimensioni molto grandi cooperino all'elaborazione di specifici codici di condotta e vi aderiscano. A tal proposito il successivo Considerando 68 afferma che il fatto che una piattaforma ***online*** rifiuti, senza adeguate spiegazioni, l'invito a partecipare all'applicazione di un tale codice di condotta potrebbe essere preso in considerazione, se del caso, nel determinare se la piattaforma online abbia violato gli obblighi stabiliti dal DSA. Infine, il Considerando 69 ipotizza che le norme sui codici di condotta potrebbero fungere da base per le iniziative di autoregolamentazione già stabilite a livello dell'Unione, tra cui l'impegno per la sicurezza dei prodotti (Product Safety Pledge), il protocollo d'intesa sulla vendita di merci contraffatte, il codice di condotta per lottare contro le forme illegali di incitamento all'odio online nonché il codice di buone pratiche sulla disinformazione.

[70] Come precisa il Considerando 70, "[i]l coinvolgimento di un'ampia gamma di portatori di interessi dovrebbe far sì che tali codici di condotta siano largamente sostenuti, tecnicamente solidi, efficaci e tali da offrire la massima facilità d'uso per garantire che siano conseguiti gli obiettivi degli obblighi di trasparenza".

[71] Il Considerando 71 aggiunge che "[n]elle circostanze straordinarie possono rientrare gli eventi imprevedibili, quali i terremoti, gli uragani, le pandemie e le altre gravi minacce per la salute pubblica a carattere transfrontaliero, le guerre e gli atti di terrorismo, in cui, ad esempio, le piattaforme online possono essere utilizzate in modo improprio per la rapida diffusione di contenuti illegali o disinformazione o in cui sorge la necessità di divulgare velocemente informazioni affidabili."

opportuno, l'adeguamento delle risorse destinate a garantire il rispetto degli obblighi di cui agli articoli 14, 17, 19, 20 e 27 alle esigenze create dalla situazione di crisi." Inoltre definiscono chiaramente gli elementi seguenti: i parametri specifici per determinare la circostanza eccezionale oggetto del protocollo; gli obiettivi del protocollo; il ruolo dei partecipanti; le misure che devono mettere essere in atto durante l'attivazione del protocollo di crisi; le condizioni in cui deve essere attivato il protocollo; criteri per la determinazione del periodo di crisi (che deve comunque essere strettamente limitato a quanto necessario per far fronte alle specifiche circostanze eccezionali); le garanzie a tutela dell'esercizio dei diritti fondamentali ed in particolare la libertà di espressione e di informazione e il diritto alla non discriminazione; una procedura per comunicare pubblicamente l'esito della gestione della crisi.

2.3 Attuazione, cooperazione, sanzioni ed esecuzione

Il capo IV del DSA è dedicato all'attuazione del DSA, alla cooperazione transnazionale tra Autorità nazionali e sovranazionali ed alle sanzioni previste in caso di violazione degli obblighi imposti dal DSA.

La Sezione 1 del Capo IV attiene alla individuazione e disciplina delle autorità competenti e dei Coordinatori nazionali dei servizi digitali.

Ai sensi dell'Articolo 38 (**Autorità competenti e Coordinatore dei Servizi Digitali** (**CSD**) è fatto obbligo agli Stati membri di designare, entro due mesi dall'entrata in vigore del DSA, una o più autorità competenti per l'*enforcement* del Regolamento. Una delle autorità competenti così individuate è designata CSD, il quale è responsabile di tutte le questioni relative all'*enforcement* del DSA nello Stato Membro, a meno che quest'ultimo non deleghi determinati compiti o settori specifici ad altre autorità.[72] In tale ipotesi, l'autorità designata CSD è comunque responsabile di garantire il coordinamento a livello nazionale in relazione alle questioni attinenti al DSA al fine di garantire un'applicazione coerente del Regolamento.

Tale coerenza è anche garantita a livello europeo, tramite uno scambio regolare tra i singoli CSD, con il Comitato e con la Commissione. Una tale struttura desta anzitutto una riflessione sull'opportunità di designare un unico coordinatore nazionale competente per illeciti di così varia natura. Per quanto specificamente concernente la tutela online di diritti di proprietà industriale, è lecito chiedersi quale possa essere il coordinamento interno tra diversi enti con competenze diverse.

L'Articolo 39 (Prescrizioni relative ai CSD) definisce alcune caratteristiche che il CSD deve avere per rispondere alle esigenze del Regolamento e che sembrerebbero *prima facie* condurre tutte verso la qualificazione del CSD quale un'autorità indipendente. In particolare, il CDS deve assolvere ai propri

[72] L'Art. 38(2) specifica: "Se uno Stato membro designa più di un'autorità competente oltre al CSD, tale Stato membro provvede affinché i rispettivi compiti di tali autorità e del CSD siano chiaramente definiti e affinché essi cooperino strettamente ed efficacemente nello svolgimento dei loro compiti. Lo Stato membro interessato comunica alla Commissione e al Comitato il nome delle altre autorità competenti e i compiti assegnati a ciascuna di esse".

compiti in modo imparziale, trasparente e tempestivo, disponendo di risorse tecniche, finanziarie e umane adeguate. Ancora, il CDS deve garantire un esercizio del potere indipendente, senza influenza esterna, diretta o indiretta, pubblica o privata.

L'Articolo 40 pone le **norme di giurisdizione, a meno che non vi sia competenza diretta della Commissione europea**. In particolare, è competente il CSD dello Stato membro in cui è situato lo stabilimento principale del prestatore di servizi intermediari. Un intermediario che presta servizi in UE pur non essendovi stabilito è soggetto alla giurisdizione dello Stato membro in cui risiede o è stabilito il suo rappresentante legale. Nell'ipotesi in cui non è stato nominato tale rappresentante, allora tutti gli Stati membri hanno giurisdizione. In tale ipotesi, quando uno Stato membro decide di esercitare la giurisdizione, ne informa tutti gli altri Stati membri a garanzia del principio del ne bis in idem.

I **poteri dei CSD** sono definiti dall'Articolo 41 e devono consistere almeno nei seguenti poteri di indagine (nei limiti della propria giurisdizione): a) il potere di imporre ai prestatori, a qualsiasi persona che agisca per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale e che possa ragionevolmente essere a conoscenza di informazioni relative a una presunta violazione del Regolamento, comprese le organizzazioni che effettuano gli audit, di fornire tali informazioni entro un termine ragionevole; b) il potere di effettuare ispezioni in loco presso i locali commerciali, o di chiedere ad altre autorità pubbliche di procedere in tal senso, al fine di esaminare, sequestrare, prendere o ottenere copie di informazioni relative a una presunta violazione in qualsiasi forma, indipendentemente dal supporto di conservazione; c) il potere di chiedere a qualsiasi membro del personale o rappresentante di tali prestatori o persone di fornire spiegazioni in merito a qualsiasi informazione relativa a una presunta violazione e di registrarne le risposte.

I CSD dispongono anche di poteri di esecuzione nei confronti dei prestatori di servizi intermediari soggetti alla giurisdizione del loro Stato membro ed almeno del: a) potere di accettare gli impegni offerti da tali prestatori in relazione alla loro conformità al presente Regolamento e di rendere tali impegni vincolanti; b) potere di ordinare la cessazione delle violazioni e, ove opportuno, di imporre misure correttive proporzionate alla violazione e necessarie per far cessare effettivamente la stessa; c) potere di imporre sanzioni pecuniarie; d) potere di imporre penalità di mora; e) potere di adottare misure cautelari.

Ancora, ove necessario per far cessare una violazione che causi un danno grave (e qualora siano stati esauriti tutti gli altri poteri e la violazione persiste), il CSD deve avere anche il potere di adottare le misure seguenti: a) imporre all'organo di gestione dei prestatori, entro un termine ragionevole, di esaminare la situazione, di adottare e presentare un piano di azione che definisca le misure necessarie per far cessare la violazione, di provvedere affinché il prestatore adotti tali misure e di riferire sulle misure adottate; b) se il CSD ritiene che il prestatore non si sia sufficientemente conformato agli obblighi di cui alla lettera a) e che la violazione persista, causi un danno grave e integri un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, chiedere alle autorità giudiziarie competenti di tale Stato membro di ordinare la restrizione temporanea dell'accesso dei destinatari del servizio interessati dalla violazione o, unicamente qualora ciò non sia tecnicamente fattibile, la restrizione dell'accesso all'interfaccia online del prestatore di servizi intermediari sulla quale ha luogo la violazione.

In tale seconda ipotesi, tranne qualora il CSD agisca su richiesta della Commissione, prima di trasmettere la richiesta all'autorità giudiziaria, invita le parti interessate a presentare osservazioni scritte entro un termine non inferiore a due settimane, descrivendo le misure che intende richiedere e identificando il destinatario o i destinatari previsti di tali misure. Il prestatore, il destinatario o i destinatari previsti e i terzi che dimostrino di avere un interesse legittimo sono autorizzati a partecipare al procedimento dinanzi all'autorità giudiziaria competente. Le misure disposte devono essere proporzionate alla natura, alla gravità, alla reiterazione e alla durata della violazione e non devono limitare indebitamente l'accesso alle informazioni lecite da parte dei destinatari dei servizi interessati.

Tali restrizioni all'accesso sono disposte per un periodo di quattro settimane, fatta salva la possibilità, tramite autorizzazione dell'autorità giudiziaria competente, di prorogare tale termine di ulteriori periodi della stessa durata, nel rispetto di un numero massimo di proroghe stabilito da tale autorità giudiziaria. La proroga può essere ammessa solo nell'ipotesi in cui siano soddisfatte entrambe le condizioni seguenti: a) il prestatore ha omesso di adottare le misure necessarie per porre fine alla violazione; b) la restrizione temporanea non limita indebitamente l'accesso dei destinatari del servizio alle informazioni lecite, tenuto conto del numero di destinatari interessati e dell'eventuale esistenza di alternative adeguate e facilmente accessibili (proporzionalità). Nell'ipotesi in cui la proroga non può essere disposta pur al ricorrere di entrambe le condizioni, il CSD deve presentare una nuova richiesta all'autorità giudiziaria competente.

Le misure adottate dai CSD devono essere effettive, dissuasive e proporzionate, tenuto conto, in particolare, della natura, della gravità, della reiterazione e della durata della violazione o presunta violazione cui si riferiscono tali misure, nonché, ove opportuno, della capacità economica, tecnica e operativa del prestatore di servizi intermediari interessato. In ogni caso, l'esercizio dei poteri deve avvenire nel rispetto del dei diritti fondamentali ed in particolare del diritto al rispetto della vita privata e ai diritti della difesa, e fatto salvo il diritto di tutte le parti coinvolte a un ricorso giurisdizionale effettivo.

Per quanto attiene alle **sanzioni,** l'Articolo 42 lascia discrezionalità agli Stati membri per la previsione delle norme relative alle sanzioni da applicare ai prestatori di servizi sottoposti alla relativa giurisdizione in caso di violazione del Regolamento. Tali misure, che devono comunque essere effettive, proporzionate e dissuasive, devono essere notificate alla Commissione, anche in caso di successiva modifica.

In ogni caso, l'importo massimo delle sanzioni irrogate in caso di inosservanza degli obblighi stabiliti dal Regolamento non può superare il 6% del reddito o del fatturato annuo del prestatore di servizi intermediari interessato. Invece, le sanzioni in caso di comunicazione di informazioni inesatte, incomplete o fuorvianti, di mancata risposta o rettifica di informazioni inesatte, incomplete o fuorvianti e di inosservanza dell'obbligo di sottoporsi a un'ispezione in loco non possono superare l'1% del reddito o del fatturato annuo del prestatore interessato. Per quanto attiene, infine, alle penalità di mora, l'importo massimo giornaliero non può superare il 5% del fatturato giornaliero medio del prestatore di servizi intermediari interessato nell'esercizio finanziario precedente, calcolato a decorrere dalla data specificata nella decisione in questione.

Ai destinatari del servizio, gli utenti, l'Articolo 43 - **Diritto di presentare un reclamo** – riconosce espressamente il diritto di presentare un reclamo nei confronti dei prestatori di servizi intermediari in ipotesi di violazione del Regolamento. Tale reclamo può essere promosso presso il CSD dello Stato membro in cui il destinatario risiede o è stabilito. Il CSD dello Stato del destinatario valuta il reclamo e lo trasmette al CSD del luogo di stabilimento del fornitore di servizi che a sua volta può trasmetterlo all'autorità compente eventualmente designata.

L'Articolo 44 impone ai CSD di elaborare una **relazione annuale** sulle attività svolte che deve essere pubblica e comunicata alla Commissione e al Comitato. Tale relazione ha un contenuto minimo individuato dal medesimo articolo e consistente almeno nell'indicazione di: a) il numero e l'oggetto degli ordini di contrastare contenuti illegali e degli ordini di fornire informazioni emessi da qualsiasi autorità giudiziaria o amministrativa nazionale dello Stato membro del CSD; b) il seguito dato a tali ordini. Nell'ipotesi in cui lo Stato membro abbia designato più autorità competenti, l'autorità designata CSD elabora un'unica relazione riguardante le attività di tutte le autorità coinvolte.

Il Regolamento disciplina anche un particolare sistema di collaborazione tra CSD. L'Articolo 45 (Cooperazione transfrontaliera tra CSD) prevede a tal proposito che il CSD che abbia motivo di sospettare che un prestatore di servizi, non soggetto alla propria giurisdizione, abbia violato il DSA chiede al CSD del luogo di stabilimento dell'intermediario di valutare la questione e di adottare le misure necessarie.

Se la condotta asseritamente violativa ha coinvolto almeno tre Stati membri, il Comitato raccomanda al CSD del luogo di stabilimento di valutare la questione e di adottare le necessarie. La richiesta o la raccomandazione di intervento deve almeno specificare: a) il punto di contatto del prestatore di servizi intermediari; b) una descrizione dei fatti rilevanti, delle norme interessate e dei motivi per cui il CSD che ha inviato la richiesta o il Comitato sospetta che il fornitore abbia violato il Regolamento; c) qualsiasi altra informazione pertinente.

Se il CSD del luogo di stabilimento ritiene di non avere informazioni sufficienti per dare seguito alla richiesta o alla raccomandazione e ha motivo di ritenere che il CSD segnalante possa fornire informazioni supplementari, può richiederle.

Il CSD destinatario della segnalazione comunica al CSD segnalante, senza indebito ritardo e in ogni caso entro due mesi dal ricevimento della richiesta o della raccomandazione, la sua valutazione, e una spiegazione delle adottate. Qualora il CSD segnalante non riceva tale comunicazione o non concordi con la valutazione o le misure adottate, lo stesso può deferire la questione alla Commissione, fornendo tutte le informazioni pertinenti.

La Commissione valuta la questione entro tre mesi dal deferimento della stessa, previa consultazione del CSD del luogo di stabilimento e del Comitato, salvo qualora la questione sia stata deferita dal Comitato stesso. Se la Commissione giunge alla conclusione, che la valutazione o le misure del CSD non sono opportune, chiede al CSD del luogo di stabilimento di valutare ulteriormente la questione e di adottare le misure di indagine o di esecuzione necessarie per garantire il rispetto del Regolamento e di riferire in merito a dette misure entro due mesi.

Oltre a questo complesso sistema di interazione, l'Articolo 46 prevede anche la possibilità di svolgere indagini congiunte, che possono essere coordinate con il sostegno del Comitato, in relazione ai

prestatori di servizi intermediari che operano in più Stati membri. Tali indagini non pregiudicano i compiti e i poteri dei singoli CSD partecipanti, che, inoltre mettono i risultati delle indagini congiunte a disposizione degli altri CSD, della Commissione e del Comitato. Se ha motivo di sospettare che una VLOP abbia violato il DSA, il CSD del luogo di stabilimento può chiedere alla Commissione di adottare le misure di indagine e di esecuzione necessarie per garantire il rispetto del Regolamento. Tale richiesta contiene tutte le informazioni di cui All'articolo 45(2) ed espone i motivi alla base della richiesta di intervento della Commissione.

La Sezione 2 del Capo IV è dedicata alla **disciplina del Comitato istituito, ai sensi dell'Articolo 47, quale gruppo consultivo indipendente di coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari**. Il Comitato fornisce consulenza ai CSD e alla Commissione per conseguire gli obiettivi seguenti: a) contribuire all'applicazione coerente del Regolamento e alla cooperazione efficace dei CSD e della Commissione; b) coordinare e contribuire agli orientamenti e all'analisi della Commissione, dei CSD e di altre autorità competenti sulle questioni emergenti in relazione alle materie disciplinate dal DSA; c) assistere i CSD e la Commissione nella vigilanza sulle piattaforme online di dimensioni molto grandi.

Ai sensi dell'Articolo 48, il Comitato è composto dai CSD (rappresentati da funzionari di alto livello) dei singoli Stati Membri. Solo ove previsto dal diritto nazionale, altre autorità competenti per l'*enforcement* del DSA insieme al CSD possono partecipare al Comitato in forma permanente od occasionale per singole riunioni e limitatamente alle questioni di loro pertinenza.

Nel Comitato ciascuno Stato membro dispone di un solo voto mentre la Commissione non ha diritto di voto. Il Comitato adotta i propri atti a maggioranza semplice. La Commissione presiede il Comitato, convoca le riunioni e prepara l'ordine del giorno conformemente al proprio regolamento interno. Il Comitato può invitare esperti e osservatori a partecipare alle proprie riunioni e può cooperare con altre istituzioni e altri organi, organismi e gruppi consultivi dell'UE mettendo a disposizione del pubblico i risultati di tale cooperazione.

I compiti del Comitato sono definiti dall'Articolo 49 e consistono in particolare nel: a) sostenere il coordinamento delle indagini congiunte; b) assistere le autorità competenti nell'analisi delle relazioni e dei risultati degli audit delle VLOP; c) fornire pareri, raccomandazioni o consulenze ai CSD in conformità al DSA; d) raccomandare alla Commissione l'adozione delle misure e, su sua richiesta adottare pareri sui progetti di misure della Commissione riguardanti le VLOP; e) sostenere e promuovere l'elaborazione e l'attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei, nonché l'individuazione di questioni emergenti in materia.

I pareri del Comitato non sono vincolanti, ma i CSD che ritengano di non aderire agli stessi devono motivare tale scelta nell'ambito delle relazioni annuali previste dal Regolamento o al momento di adottare le decisioni pertinenti, a seconda dei casi.

La Sezione 3 del Capo IV specifica **le norme sulla vigilanza, indagini, esecuzione e monitoraggio in relazione alle piattaforme online di dimensioni molto grandi.** In particolare, i CSD possono avvalersi di sistema di vigilanza rafforzata in presenza di una violazione del Regolamento compiuta da piattaforma *online* di dimensioni molto grandi. Nel caso in cui vi sia il sospetto che un tale soggetto abbia violato le disposizioni del DSA, la Commissione, di propria iniziativa, o il Comitato, di propria

iniziativa o su richiesta di almeno tre coordinatori dei servizi digitali del luogo di destinazione, può raccomandare al coordinatore dei servizi digitali del luogo di stabilimento di indagare sulla presunta violazione in modo che tale coordinatore dei servizi digitali possa adottare una simile decisione entro un periodo di tempo ragionevole (Art. 50). Si apre, così, una interlocuzione tra piattaforma *online* di dimensioni molto grandi e CSD del luogo di stabilimento per far cessare o porre rimedio alla violazione, in cui il CSD tiene nella massima considerazione i pareri e le raccomandazioni della Commissione e del comitato. Se nutre preoccupazioni quanto all'idoneità delle misure a far cessare o a porre rimedio alla violazione, il CSD del luogo di stabilimento può chiedere alla piattaforma online di dimensioni molto grandi interessata di sottoporsi a un audit indipendente supplementare, a spese della piattaforma interessata, che consenta di valutare l'efficacia di tali misure nel far cessare o porre rimedio alla violazione. A seguito di tale interlocuzione il CDS comunica il proprio parere finale alla Commissione al comitato e alla piattaforma online di dimensioni molto grandi interessata.

Ai sensi dell'Art. 51, la Commissione può avviare un procedimento in vista della possibile adozione di decisioni sanzionatorie o di non conformità, su raccomandazione del Comitato o di propria iniziativa previa consultazione del Comitato, in caso di sospetto di violazione di una delle disposizioni del regolamento da parte di una piattaforma online di dimensioni molto grandi e (a) mancata attivazione del CSD competente; (b) richiesta di intervento da parte del CSD o (c) in caso di accertamento della responsabilità.

Gli Artt. 50 e 51 prevedono alcuni meccanismi specifici di coordinamento tra CSD e Commissione.

Per svolgere i compiti ad essa assegnati, la Commissione dispone di poteri simili a quelli previsti per i procedimenti avviati in caso di violazioni *antitrust*. Può inviare, infatti, richieste di informazioni, ha poteri di audizione, di raccolta di dichiarazioni e di ispezioni in loco ai sensi degli Artt. 52, 53 e 54. La Commissione può altresì applicare misure provvisorie in caso di urgenza dovuta al rischio di danni gravi per i destinatari del servizio (Art. 55) e può decidere di rendere vincolanti gli impegni eventualmente presentati dalla piattaforma online di dimensioni molto grandi volti a garantire la conformità alle pertinenti disposizioni del regolamento (Art. 56). La Commissione, inoltre, dispone di poteri di monitoraggio sull'effettiva attuazione e osservanza del regolamento da parte della piattaforma online di dimensioni molto grandi interessata. A tal fine, la Commissione, avvalendosi di esperti e revisori esterni indipendenti, può anche ordinare a tale piattaforma di fornire accesso ai suoi algoritmi e alle sue banche dati e di fornire spiegazioni al riguardo (Art. 57).

Nel caso in cui la VLOP interessata non rispetti a) le pertinenti disposizioni del DSA, b) le misure provvisorie eventualmente ordinate a norma dell'Articolo 55 o c) gli impegni resi eventualmente vincolanti a norma dell'Articolo 56, la Commissione adotta una decisione di non conformità, preceduta da constatazioni preliminari in cui si presume vi possa essere un contraddittorio tra piattaforma e Commissione. Nella decisione di non conformità (Art. 58), la Commissione ordina alla VLOP interessata di adottare le misure necessarie per garantire il rispetto della decisione di non conformità entro un termine ragionevole e di fornire informazioni sulle misure che la piattaforma intende adottare per conformarsi alla decisione. Le misure poi effettivamente adottate devono essere comunicate alla Commissione che, qualora giudichi le condizioni non soddisfatte, chiude il procedimento tramite decisione.

L'Articolo 59 stabilisce le sanzioni pecuniarie applicabili alle VLOP che siano soggetto di una decisione adottata ai sensi dell'Articolo 58. In tale ipotesi, la Commissione può infliggere sanzioni pecuniarie non superiori al 6% del fatturato totale realizzato nell'esercizio precedente. Tale sanzione può essere comminata qualora sia constatato che (intenzionalmente o per negligenza): a) siano state violate le disposizioni del Regolamento; b) non sia stata rispetta una decisione attinente misure provvisorie; oppure c) si sia verificata l'inottemperanza ad una misura volontaria resa vincolante con decisione della Commissione. La sanzione è diversa, ovvero non superiore all'1% del fatturato totale dell'esercizio precedente, qualora, intenzionalmente o per negligenza, la piattaforma: i) fornisca informazioni inesatte, incomplete o fuorvianti in risposta a una richiesta di informazioni o - se le informazioni sono richieste mediante decisione - non rispondano alla richiesta entro il termine stabilito; ii) ometta di rettificare, entro il termine fissato dalla Commissione, le informazioni inesatte, incomplete o fuorvianti fornite, oppure ometta o rifiuti di fornire informazioni complete; iii) rifiuti di sottoporsi ad un'ispezione in loco.

Singolarmente, il paragrafo 3 prevede che solo prima di adottare una decisione a norma del paragrafo 2, la Commissione comunica le proprie constatazioni preliminari alla piattaforma online di dimensioni molto grandi interessata.

Infine, è chiarito che, nel determinare l'importo della sanzione pecuniaria, vari elementi concorrono alla determinazione della sanzione da parte della Commissione, ed in particolare della natura, della gravità, della durata e della reiterazione della violazione e, per le sanzioni relative alle informazioni e alle ispezioni, del ritardo causato al procedimento.

La proposta di DSA prevede anche la possibilità, per la Commissione, di irrogare penalità di mora giornaliere ai sensi dell'Articolo 60. Tali penalità non possono essere superiori al 5 % del fatturato giornaliero medio dell'esercizio precedente, calcolate a decorrere dalla data stabilita nella decisione, e possono essere inflitte solo al fine di costringere a: a) fornire informazioni corrette e complete in risposta a una richiesta di informazioni; b) sottoporsi a un'ispezione in loco; c) conformarsi a una decisione che dispone misure provvisorie; d) rispettare gli impegni resi giuridicamente vincolanti; e) conformarsi a una decisione adottata a norma dell'Articolo 58(1).

Qualora la VLOP si sia conformata all'obbligo per il cui adempimento è stata inflitta la penalità di mora, la Commissione può fissare l'importo definitivo di quest'ultima in una misura inferiore a quella che risulta dalla decisione originaria.

Ai sensi dell'Articolo 61, i poteri sanzionatori conferiti alla Commissione sono soggetti ad un termine di prescrizione di cinque anni che decorre dal giorno in cui è stata commessa la violazione. Tuttavia, in caso di violazioni continuate o reiterate, tale termine inizia a decorrere dal giorno in cui cessa la violazione. Il termine prescrizionale è interrotto da qualsiasi azione intrapresa dalla Commissione o dal CSD ai fini dell'indagine o del procedimento ed in particolare: a) la trasmissione di richieste di informazioni; b) ispezioni in loco; c) l'avvio di un procedimento da parte della Commissione. Ogni interruzione fa decorrere nuovamente il termine di prescrizione fino ad un massimo pari al doppio del termine di prescrizione fatto salvo il termine sospensivo determinato dalla proposizione di un giudizio innanzi alla Corte di giustizia dell'Unione europea.

Stesso termine quinquennale si applica anche, ai sensi dell'Articolo 62, all'esecuzione delle decisioni da parte della Commissione. Tale termine inizia a decorrere dal giorno in cui la decisione diventa definitiva ma può essere interrotto: a) dalla notifica di una decisione che modifica l'importo iniziale della sanzione pecuniaria o della penalità di mora, oppure respinge una domanda intesa ad ottenere una tale modifica; b) da qualsiasi azione della Commissione, o di uno Stato membro che agisca su richiesta della Commissione, volta a dare esecuzione al pagamento della sanzione. Il termine è, invece, sospeso: a) per la durata del termine fissato per il pagamento; b) qualora l'esecuzione del pagamento stessa sia sospesa in virtù di una decisione della Corte di giustizia dell'Unione europea.

L'Articolo 63 garantisce il rispetto del principio del contradditorio procedimentale ed in particolare riconosce all'interessato il diritto di essere ascoltati e di avere accesso al fascicolo. In particolare, è sancito il principio per cui la Commissione può basare le proprie decisioni solo sulle obiezioni in merito alle quali le parti interessate sono state poste in condizione di esprimersi. È infatti stabilito che, prima di adottare una decisione a norma dell'Articolo 58(1) o degli Articoli 59 e 60, la Commissione dà alla VLOP interessata la possibilità di essere ascoltate in merito alle constatazioni preliminari (comprese le questioni sulle quali la Commissione ha sollevato obiezioni) e alle misure che la Commissione intende adottare alla luce delle constatazioni preliminari. In tali ipotesi, possono essere presentate osservazioni sulle constatazioni preliminari della Commissione entro un termine ragionevole fissato nelle stesse constatazioni preliminari, che non può essere comunque inferiore a 14 giorni.

Anche il diritto di difesa delle parti interessate è pienamente riconosciuto e garantito, in particolare tramite il diritto di accesso al fascicolo detenuto dalla Commissione alle condizioni previste per una divulgazione negoziata, fermo restando il legittimo interesse alla protezione dei segreti commerciali. Il diritto di accesso al fascicolo non si estende alle informazioni riservate e ai documenti interni della Commissione o delle autorità degli Stati membri. In particolare, il diritto di accesso non si estende alla corrispondenza tra la Commissione e tali autorità. È altresì chiarito che le informazioni raccolte in seguito a richiesta possono essere utilizzate esclusivamente ai fini del presente regolamento.

L'Articolo 64 prevede anche un regime di pubblicità delle decisioni adottate dalla Commissione che ne impone la pubblicazione con l'indicazione dei nomi delle parti, il contenuto essenziale, comprese eventuali sanzioni irrogate.

Ai sensi dell'Articolo 65, qualora siano stati esauriti tutti i poteri previsti per far cessare una violazione e quest'ultima persista causando un danno grave, la Commissione può chiedere al CSD del luogo di stabilimento della piattaforma online di dimensioni molto grandi interessata, di restringerne l'accesso o adottare un diverso piano di azione ai sensi dell'Articolo 41(3). Prima di inviare tale richiesta al Coordinatore dei servizi digitali, la Commissione invita le parti interessate a presentare osservazioni scritte entro un termine non inferiore a due settimane, descrivendo le misure che intende richiedere e identificando il destinatario o i destinatari previsti di tali misure. Ove necessario, la Commissione, di propria iniziativa, può presentare osservazioni scritte all'autorità giudiziaria competente e previa autorizzazione della stessa, anche formulare osservazioni orali.

L'articolo 66, infine, aggiunge che, rispetto alle modalità pratiche per lo svolgimento del procedimento a norma degli Articoli 54 e 57 e delle audizioni previste dall'Articolo 63, nonché per la divulgazione negoziata di informazioni di cui all'Articolo 63, la Commissione può adottare atti di esecuzione secondo procedura consultiva pubblicando un progetto di tali misure e invitando tutte le parti

interessate a presentare osservazioni entro il termine ivi stabilito, che non può essere inferiore a un mese.

La Sezione 4 del Capo IV reca, infine, le disposizioni comuni in materia di esecuzione. Ai sensi dell'Articolo 67, la Commissione istituisce e mantiene un sistema affidabile e sicuro di condivisione delle informazioni a sostegno delle comunicazioni tra i CSD, la Commissione e il Comitato.

2.4 Osservazioni preliminari sulla compliance normativa al DSA per le diverse tipologie di piattaforme

Rispetto al quadro vigente, la proposta di Regolamento DSA introduce una serie di obblighi comportamentali e di *due diligence* "a geometria variabile" per i servizi *online* di differenti tipologie e dimensioni.

La proposta si caratterizza così per indirizzarsi a soggetti specifici, pur aspirando ad una regolazione trasversale "per tutte le categorie di contenuti, prodotti, servizi ed attività sui servizi intermediari", in cui rientra anche la contraffazione di diritti di proprietà industriale.

Il sistema creato dal DSA non può che concentrare l'attenzione sulle definizioni dei soggetti regolati, che, tuttavia, come già anticipato nel §2.1.2, non coincidono perfettamente con altre discipline settoriali vigenti, rischiando di creare incertezza giuridica o obblighi sproporzionati di *compliance* in capo ad alcune categorie di soggetti distinti per tipologia e dimensione. Sembra crearsi in sostanza una regolazione "asimmetrica" di obblighi comportamentali e di *due diligence*, la cui vigilanza e attuazione è demandata alla Commissione e ad autorità competenti designate da ciascun Stato membro. A tal proposito l'esclusione espressa di microimprese e piccole imprese dall'ambito di applicazione di alcune norme (e.g. Art. 16) non previene, tuttavia, rischi elusivi di *compliance* dovuti al fatto che l'applicazione del DSA è innescata dalla dimensione e dalla tipologia dei servizi piuttosto che dalla natura illecita delle condotte.

Ancora, con riferimento alla sovrapposizione e intersezione con altre fonti normative settoriali (e.g. Digital Markets Act, Direttiva AVMS, Direttiva Copyright, come anche le disciplina che qualificano l'illiceità delle condotte da prevenire o reprimere) si rileva sin da ora il rischio di problemi di coordinamento sia sotto il profilo del merito delle discipline applicabili, sia sul versante dell'*enforcement* in relazione all'individuazione dell'autorità competente (o delle autorità competenti) ad applicare determinate disposizioni del DSA che sottintendono illeciti qualificati da fonti nazionali.

Venendo al contenuto degli obblighi comportamentali imposti a vari soggetti, quelli relativi ai soggetti qualificati come piattaforme online (*supra* §2.2.4) e come piattaforme online di dimensioni molto grandi per la gestione dei rischi sistemici (*supra* §2.2.5) suscitano alcune osservazioni preliminari sulla *compliance* normativa.

Si tratta, infatti, di obblighi sia procedurali che di comunicazione alle autorità preposte, secondo un modello che ricorda, da un lato, la regolazione dei servizi finanziari e, dall'altro lato, l'approccio di prevenzione del rischio, attraverso misure volontarie e controlli ex ante ed ex post, adottato dal GDPR.

In particolare, per quanto riguarda le piattaforme online sono imposti obblighi comportamentali e di comunicazione trasparente con le autorità preposte alla vigilanza. Tra tali obblighi, l'Art. 21 prescrive anche un obbligo di comunicazione in caso di sospetto che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone.

Il Considerando 48 spiega, infatti, come "una piattaforma online può in alcuni casi venire a conoscenza, ad esempio attraverso una notifica di una parte notificante o mediante proprie misure volontarie, di informazioni relative a determinate attività di un destinatario del servizio, quali la fornitura di determinati tipi di contenuti illegali, che giustifichino ragionevolmente, considerato l'insieme delle circostanze pertinenti di cui la piattaforma online è a conoscenza, il sospetto che il destinatario possa aver commesso, potenzialmente stia commettendo o probabilmente commetterà un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, quali i reati di cui alla direttiva 2011/93/UE del Parlamento europeo e del Consiglio".

In tali casi la piattaforma *online* è tenuta a informare senza ritardo le autorità di contrasto competenti, fornendo tutte le pertinenti informazioni a sua disposizione, compresi ove opportuno i contenuti in questione e una illustrazione delle ragioni alla base del proprio sospetto.

L'indeterminatezza della norma in questione, il cui contenuto non è chiarito neppure dal "considerando" dedicato, suscita da subito alcune perplessità sulla portata dell'obbligo gravante sulle piattaforme che potrebbe renderne difficoltosa l'osservanza, considerata anche la portata transnazionale del precetto. Il Considerando 48 si limita, infatti, a sottolineare come il DSA non fornisca "la base giuridica per la profilazione dei destinatari dei servizi al fine dell'eventuale individuazione di reati da parte delle piattaforme online" e come "nell'informare le autorità di contrasto, le piattaforme online dovrebbero inoltre rispettare le altre norme applicabili del diritto dell'Unione o nazionale in materia di tutela dei diritti e delle libertà delle persone".

In secondo luogo, nel DSA non è specificato cosa si intenda per "gravità" del reato in questione, "gravità" che potrebbe peraltro variare in relazione all'ordinamento nazionale considerato.

In terzo luogo, non risultano delineati con precisione né il perimetro di applicazione degli obblighi di cui si tratta né il richiamo al fatto che le gravi ipotesi di reato considerate devono comportare una "minaccia alla vita" o alla "sicurezza delle persone".

La locuzione adoperata – minaccia – fa pensare a condotte che possano determinare tanto la lesione effettiva quanto l'esposizione a pericolo dei beni in questione. Il riferimento alla vita presenta contorni più definiti ma rischia di circoscrivere molto la portata applicativa delle previsioni in questione, dovendosi a rigore limitare alle sole condotte incidenti su siffatto bene e dunque escludere sia oggettività giuridiche contigue (es. integrità fisica) sia beni giuridici di sicura pertinenza personale (reputazione, libertà morale etc.), estranei tuttavia a quest'ultimo ambito di tutela. Per contro, l'espressione sicurezza delle persone non evoca alcun bene giuridico tradizionale e fatica ad assolvere una funzione classificatoria. Ciò è dimostrato dalle ipotesi di reato richiamate a titolo esemplificativo,

pedopornografia etc., che sono riconducibili alla protezione della libertà sessuale del minore. Si tratta allora di concetto malleabile che non offre una guida sicura alla piattaforma e che si rivela suscettibile di essere riempito di contenuti variegati negli accertamenti *ex post* demandati alle Autorità di settore. A rigore entrambe le categorie menzionate non dovrebbero includere i reati di contraffazione che sicuramente non comportano una minaccia alla vita, ma che pare difficile annoverare altresì tra quelli in grado di determinare quantomeno un pericolo per la sicurezza delle persone, se si eccettuano casi quali ad esempio talune figure di contraffazione alimentare o relative a medicinali etc. (es. 440 c.p.).

Infine, la norma fa riferimento a presupposti dell'obbligo variabili e anch'essi di non agevole individuazione. Anzitutto la notifica in capo alla piattaforma riguarda tanto casi in cui il reato è commesso quanto ipotesi in cui è *in itinere* o si ritiene sarà commesso. In secondo luogo, l'obbligo scatta allorché sussistano, a seguito di notificazioni ricevute o misure volontarie attuate dalla piattaforma, elementi che, sulla base di quanto a conoscenza della piattaforma, giustifichino ragionevolmente il "sospetto che sia stato commesso, si stia commettendo o probabilmente sarà commesso" uno dei reati delle categorie sopra elencate. Si tratta tuttavia di un giudizio prognostico di difficile accertamento, dai contorni particolarmente labili soprattutto laddove si fa riferimento al sospetto che in futuro sarà commesso in reato.

Bisogna peraltro tenere a mente, nel valutare la conformità di tali obblighi ai principi di fondo del nostro ordinamento, la natura sostanzialmente afflittiva delle relative sanzioni (amministrative) che, come d'altronde già da più parti evidenziato rispetto alla disciplina prevista su altri versanti dal GDPR, induce a ricondurre tali disposizioni alla nozione fluida di 'materia penale' elaborata dalla Corte EDU, con tutti i corollari in punto di necessaria prevedibilità del precetto, fermo restando che in questo caso bisognerà attendere la normativa interna di attuazione.

Gli obblighi in questione ripropongono il tema da tempo dibattuto della responsabilità penale del provider – e qui in genere delle piattaforme – in relazione a reati commessi on line. La questione non riguarda comunque l'ipotesi di omessa notifica della commissione di un reato, atteso che in questo caso non è configurabile rispetto al 'controllore' né un possibile concorso criminoso né una responsabilità c.d. omissiva impropria ex art. 40 c.p., a norma del quale non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo. Entrambe le clausole generali di incriminazione presuppongono difatti che non sia intervenuta la consumazione del reato.

Il tema potrebbe porsi rispetto agli altri casi, in particolare, a quello in cui la piattaforma possa 'ragionevolmente sospettare' che un reato sia in corso di realizzazione. A questo riguardo, va peraltro evidenziato che, supponendo il reato oggetto di impedimento come doloso, si dovrebbe in ogni caso dimostrare che il responsabile della piattaforma o comunque il soggetto preposto al controllo versi quantomeno in dolo eventuale (si sia cioè rappresentato la possibilità che il reato fosse in esecuzione e avesse consapevolmente omesso di attivarsi). Si tratta dunque, come si può constatare, di uno standard probatorio ben diverso e più stringente di quello posto dal DSA.

Peraltro, va considerato come le stesse pertinenti previsioni del DSA non pongano in capo alla piattaforma l'obbligo di impedire la realizzazione del reato, bensì quello di comunicare senza indugio all'Autorità competente 'le ragioni del sospetto'. Questa scelta normativa dovrebbe essere valorizzata nel senso di ritenere inesigibile una condotta impeditiva da parte del responsabile della piattaforma o del soggetto preposto al controllo e di ritenere pertanto l'assenza in capo a quest'ultimo dei correlativi

poteri di 'blocco' della vicenda criminosa. Deve peraltro segnalarsi come nella materia del contrasto alla pedopornografia il legislatore con la legge n. 269 del 1998 abbia introdotto all'Art. 14 *ter* obblighi di comunicazione da parte dei fornitori dei servizi resi attraverso reti di comunicazione elettronica, accostabili a quelli oggi previsti, e vi siano stati settori della dottrina inclini a desumere da siffatti obblighi vere e proprie posizioni di garanzia *ex* Art. 40 cpv. gravanti sulle piattaforme.

A questo riguardo può essere interessante rilevare che, oltre al profilo della possibile sovrapposizione tra gli obblighi di cui discutiamo, la figura risulta decisamente meglio delineata. Intanto, è chiaro l'ambito di applicazione – la lotta alla pedopornografia su internet – e, in secondo luogo, i menzionati obblighi ricorrono allorché i soggetti di cui sopra vengano a conoscenza di «imprese o soggetti che, a qualunque titolo, diffondono, distribuiscono o fanno commercio, anche in via telematica, di materiale pedopornografico».

Per quanto riguarda le piattaforme di "dimensioni molto grandi", ad esse sono richieste azioni e procedure volte a prevenire i "rischi sistemici" derivanti dal funzionamento ed utilizzo dei propri servizi e ad adottare misure appropriate per ridurre e mitigare tali rischi (cfr. § 2.2.5).

La *compliance* normativa è completata da obblighi di *due diligence* e dalla previsione di alcune misure di auto o co-regolazione come codici di condotta e protocolli di crisi (cfr. §2.2.6).

2.5 Osservazioni preliminari sul possibile impatto del DSA sui titolari dei diritti di proprietà industriale

Dall'analisi sinora svolta possono essere delineate alcune preliminari osservazioni sul possibile impatto che la nuova normativa avrebbe sui titolari dei diritti di proprietà industriale.

La normativa attualmente in vigore non affronta in maniera diretta la tutela dei diritti di proprietà industriale, presentando un quadro di più ampio respiro avente ad oggetto la responsabilità dei prestatori intermediari. All'interno di questa cornice, nel prevedere che un *hosting provider* sia tenuto ad agire prontamente per rimuovere i contenuti illegali o per disabilitarne l'accesso non appena al corrente di tali fatti, la Direttiva sul commercio elettronico non introduce tuttavia una procedura armonizzata di *notice and takedown*. Di conseguenza, i titolari dei diritti, al fine di tutelare i propri interessi, sono chiamati o ad adire le autorità competenti o a segnalare la violazione direttamente alla piattaforma interessata sulla base della procedura di *notice* che quest'ultima ha adottato.

Tale sistema ha generato incertezze ed incongruenze più volte denunciate in letteratura, nonché numerose decisioni giurisprudenziali, a livello sia nazionale sia europeo, con esiti talvolta contrastanti. Le suddette criticità sono state evidenziate e recepite nella proposta del Regolamento DSA, il quale a tal riguardo interviene introducendo, in particolare, un meccanismo uniforme di notificazione dei contenuti illegali (Articolo 14 e Considerando 40 e 41). Secondo l'attuale formulazione dell'Articolo 14, ai titolari dei diritti sarà richiesto di presentare notifiche sufficientemente precise e

adeguatamente motivate sulla presenza di contenuti illeciti, con particolare riferimento ad alcuni elementi (una spiegazione dei motivi per cui la persona o l'ente ritiene che le informazioni in questione costituiscano contenuti illegali; una chiara indicazione dell'ubicazione elettronica di tali informazioni, in particolare l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale; il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la notifica; una dichiarazione con cui la persona o l'ente che presenta la notifica conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute). Infine, le suddette notifiche non devono essere abusive in quanto manifestamente infondate, a pena di sospensione dal servizio (Articolo 20).

Riguardo ai tempi di decisione in merito alle notifiche presentate, la proposta di DSA non fornisce al momento una indicazione precisa limitandosi a stabilire che le decisioni sulle eventuali rimozioni devono esse assunte in modo tempestivo, diligente ed obiettivo (Articolo 14).

Uno degli obiettivi dichiarati dal DSA è proprio quello di consentire facile accesso ed uso a tale meccanismo, attraverso la presentazione di notifiche esclusivamente tramite via elettronica (Articolo 14). In questo contesto, i titolari dei diritti beneficeranno di una maggiore facilità nella segnalazione delle violazioni dei diritti di proprietà industriale.

Una ulteriore semplificazione dei meccanismi di notificazione viene realizzata tramite l'introduzione della figura dei *trusted flaggers*, le cui notifiche sono trattate e decise in via prioritaria e senza indugio. I titolari dei diritti potrebbero beneficiarne sia qualora venissero designati essi stessi come segnalatori attendibili sia qualora tale qualifica venisse riconosciuta in forma collettiva alle organizzazioni di settore.

Nel complesso, i vantaggi derivanti dalla semplificazione delle procedure di notifica e dalla possibilità che le stesse siano presentate in forma collettiva da associazioni di categoria saranno comparativamente più significativi per le piccole e medie imprese.

Accanto al meccanismo di notificazione, la proposta di DSA interviene su altri aspetti rilevanti per i titolari dei diritti e idonei ad avere un impatto diretto su questi ultimi. In termini di *compliance*, si segnala in particolare la previsione di cui all'Articolo 22 alla luce della quale tutti gli operatori commerciali (tra cui i titolari dei diritti) sono tenuti a fornire alle piattaforme le informazioni necessarie alla tracciabilità degli stessi. In ogni caso, le informazioni richieste non appaiono particolarmente gravose per gli operatori commerciali e, allo stato, sono limitate solo ad alcune categorie di piattaforme (*marketplaces*). Infine, i titolari dei diritti potrebbero essere altresì coinvolti nell'elaborazione di codici di condotta laddove emerga un rischio sistemico o sfide specifiche connesse alla lotta ai diversi tipi di contenuti illegali (Articolo 35).

3. Il dibattito con gli Stakeholders

Al netto di un generale consenso sulla proposta di DSA, la consultazione pubblica ha fatto emergere alcune criticità, richieste di modifica o di maggior chiarezza, anche con riferimento specifico alla tutela dei diritti di proprietà industriale nell'ambito della proposta[73]. I riscontri degli *stakeholders* che hanno contribuito alla consultazione pubblica risentono inevitabilmente dal ruolo dagli stessi svolto quali rappresentanti dei titolari dei diritti piuttosto che degli intermediari *online.*

Non mancano, tuttavia, criticità trasversali, sollevate da alcuni portatori di interesse che appartengono ad entrambe le suddette categorie.

A tal riguardo, si segnalano i rilievi sollevati con riferimento ad alcune definizioni, la cui assenza o scarsa chiarezza possono minare la certezza giuridica e, dunque, la corretta applicazione del DSA. In particolare, perplessità si palesano con riferimento alla mancata definizione di "contenuto illegale" che, per scelta legislativa, viene rimessa agli Stati Membri in sede di recepimento: tale scelta potrebbe condurre a definizioni differenti tra i vari Paesi a scapito dell'armonizzazione della disciplina nel mercato interno. Inoltre, alcuni dubbi emergono sulle conseguenze inattese di una regolamentazione asimmetrica che, anziché essere centrata sulle condotte illecite, ruota attorno alla dimensione degli operatori: il rischio, infatti, è di incentivare il proliferare di attività illegali presso gli intermediari che, in ragione della loro dimensione, sono soggetti ad obblighi e sorveglianza meno stringenti. Infine, si manifesta l'opportunità di chiarire i concetti di "conoscenza effettiva" e di "ruolo attivo", essenziali ai fini della esenzione di responsabilità degli intermediari.

Sul versante dei titolari dei diritti, si riportano le seguenti principali criticità. I rilievi più ricorrenti riguardano il trattamento delle violazioni ripetute (c.d. "repeating infringer policy"). Si lamenta, in particolare, la mancata introduzione di un meccanismo di *stay down* che imporrebbe agli *hosting providers* di impedire la nuova visualizzazione di un contenuto illegale già rimosso: tale obbligo viene considerato fondamentale per assicurare l'effettività delle misure di *notice and action,* nonché compatibile con il divieto di monitoraggio generale in quanto rappresenterebbe una previsione specifica e proporzionata. Allo stesso tempo, si richiede che, per i trasgressori recidivi (*repeat infringers*), sia prevista non solo la sospensione ma altresì la possibilità di una esclusione permanente. Infine, pur apprezzando l'introduzione di procedure di *notice and action/takedown* più accessibili, si segnala l'opportunità di includere i consumatori finali tra i destinatari dell'obbligo di informazione.

Ulteriori rilievi riguardano la tracciabilità degli operatori commerciali e la definizione di "segnalatori attendibili". Con riferimento al primo aspetto, gran parte degli *stakeholders* che rappresentano i titolari

[73] Le posizioni espresse dagli ***stakeholders*** sono rinvenibili al seguente link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services/feedback?p_id=16748286.

dei diritti richiedono che, affinché il principio KYBC sia implementato in modo effettivo, sarebbe necessario estenderlo a tutti gli intermediari *online* (anziché ai soli *marketplace*) e ai venditori privati. Con la medesima *ratio*, si segnala l'opportunità di estendere gli obblighi di *due diligence* a tutti gli intermediari, indipendentemente dalla loro dimensione. Per quanto concerne, invece, i *trusted flaggers*, si raccomanda di includere nella relativa categoria anche i singoli titolari dei diritti e non solo le loro organizzazioni rappresentative: nei casi di contraffazione, infatti, i *brand owners* sono i soggetti meglio posizionati per confermare l'autenticità dei prodotti e rendere così il processo di rimozione più veloce e snello in termini di oneri burocratici.

Sul versante degli intermediari, le criticità rilevate sono naturalmente spesso diametralmente opposte a quelle evidenziate dai titolari dei diritti. Si segnala, innanzitutto, la necessità di salvaguardare il rispetto del principio del divieto di monitoraggio generale che inevitabilmente verrebbe compromesso dall'eventuale introduzione di obblighi di *stay down*.

Si contestano, inoltre, i contorni troppo ampi della definizione di piattaforme *online*, la quale non tiene conto dei diversi modelli di business e, in particolare, non distingue le piattaforme di transazione (come i *marketplaces*) dalle altre tipologie. Ne consegue, ad esempio, che apparentemente la definizione di piattaforme *online* includerebbe anche i fornitori di servizi *cloud*, i quali, tuttavia, nella maggior parte dei casi non hanno accesso né controllo sui contenuti illegali e su come i propri utenti utilizzano i servizi, sicché sarebbe ingiustificato applicare loro gli obblighi aggiuntivi previsti per le piattaforme *online*.

Le perplessità riguardo ad un trattamento differenziato basato solamente sulla dimensione degli operatori emergono anche riguardo alla definizione delle VLOP, dove si rileva come altri fattori, quali il modello di business, la finalità del servizio offerto e l'eventuale prevalenza di contenuti illegali su quest'ultimo, meriterebbero considerazione.

Si segnala, altresì, una apparente contraddizione riguardo la posizione dei servizi di comunicazione interpersonale (messaggi di posta elettronica o servizi di messaggistica privata), i quali mentre dal Considerando 14 sono esclusi dall'ambito di applicazione del DSA, nel successivo Considerando 27 vengono indicati tra i servizi che possono beneficiare delle esenzioni dalla responsabilità, nella misura in cui si qualificano come servizi di *mere conduit*, *caching* o *hosting*.

Infine, si pone l'attenzione sul potenziale impatto negativo degli obblighi di *due diligence*: si chiede, per un verso, che, a fronte di obblighi particolarmente dettagliati, venga invece garantita una certa flessibilità, oltre che una proporzionalità tra gli stessi e le sanzioni previste per il loro mancato rispetto, e, per altro verso, che dagli stessi vengano esentate le imprese di medie dimensioni (oltre che le micro e piccole imprese) al fine di non gravarle da oneri eccessivi che potrebbero precluderne la competitività sul mercato.

4. Il dibattito istituzionale: punti critici e proposte di modifica

La proposta di DSA è attualmente all'attenzione del Consiglio dell'Unione europea e del Parlamento europeo ai sensi della procedura legislativa ordinaria (cfr. *supra* §2). Dai lavori preliminari delle suddette istituzioni emergono spunti interessanti che è opportuno richiamare al fine di individuare aree di intervento per possibili modifiche.

Anzitutto, dai documenti esaminati emerge, allo stato, un sostegno generale rispetto agli obiettivi ed all'impostazione della proposta della Commissione.

In particolare, **in seno al Consiglio**, alcuni Stati membri hanno sollevato interrogativi sull'**ambito di applicazione** della proposta, con specifico riferimento all'interazione tra quest'ultima e la legislazione vigente dell'Unione.[74] Inoltre, sebbene gli Stati membri abbiano espresso il loro impegno a preservare i principi fondamentali della direttiva sul commercio elettronico, con particolare riferimento al principio del paese di origine, alcuni di essi hanno manifestato l'esigenza di un maggiore coinvolgimento del paese di destinazione, nonché una migliore cooperazione transfrontaliera tra coordinatori dei servizi digitali, indagini congiunte e richieste di intervento della Commissione. In questo contesto, peraltro, diversi Stati membri hanno espresso preoccupazioni e dubbi sulla portata e sull'efficacia degli ordini nazionali di contrasto ai contenuti illegali e di richiesta di informazioni rivolti ai prestatori di servizi intermediari di cui agli Articoli 8 e 9 della proposta: le perplessità riguardano, in particolare, le condizioni in base alle quali le autorità giudiziarie o amministrative nazionali possono emettere tali ordini, anche a livello transfrontaliero ed il relativo impatto sul principio del Paese di origine.

Infine, ai fini dell'applicazione del DSA, sono stati sollevati quesiti anche in merito al funzionamento pratico del sistema di vigilanza a più livelli, il quale prevede distinti poteri e requisiti per i coordinatori dei servizi digitali e le autorità competenti, per il Comitato e la Commissione: a destare preoccupazione è soprattutto l'impatto di tale sistema di vigilanza sulla struttura amministrativa nazionale esistente.

Per quanto concerne la **responsabilità delle piattaforme**, l'approccio asimmetrico della proposta ha riscosso consensi. In particolare, la previsione di un obbligo in capo alle piattaforme di grandi dimensioni di valutare ogni significativo rischio sistemico con riferimento ai servizi offerti ha ricevuto ampio sostegno, sebbene alcuni Stati membri abbiano comunque evidenziato la necessità di rafforzare la protezione dei diritti fondamentali, in particolare la libertà di espressione. Lo stesso dicasi per l'obbligo di tracciabilità degli operatori commerciali di cui all'Articolo 22: alcuni Stati membri hanno anzi suggerito di ampliare la sua portata al fine di includere anche altri tipi di prestatori di servizi

[74] Le relazioni sullo stato di avanzamento dei lavori del Consiglio dell'Unione europea sono disponibili all'indirizzo internet https://eur-lex.europa.eu/procedure/EN/2020_361.

intermediari e di estenderlo alle microimprese e alle piccole imprese. Più in generale, alcuni Stati membri hanno suggerito di adattare la definizione di microimprese e piccole imprese all'ambiente digitale articolandola, perciò, su un approccio basato sul rischio, anziché esclusivamente sui criteri delle dimensioni e del fatturato: infatti se, da una parte, per evitale oneri sproporzionati tali imprese sono esentate dall'ambito di applicazione di taluni obblighi della proposta di DSA, dall'altra parte si rileva come una siffatta esenzione potrebbe minare l'efficacia delle misure di contrasto alla diffusione di contenuti illegali.

Alcuni Stati Membri hanno, inoltre, sottolineato l'importanza delle misure di *stay down* nella lotta alla contraffazione e, pertanto, hanno chiesto di chiarire la possibilità delle autorità nazionali di emettere "ordini di non ripubblicazione", che obbligherebbero le piattaforme online a prevenire la ricomparsa di contenuti dichiarati illegali e di conseguenza rimossi.

Un'ulteriore questione sollevata da alcuni Stati membri è l'opportunità di una estensione dello *status* di segnalatori attendibili a tutti gli enti che presentano notifiche, dimostrano di possedere competenze e un elevato grado di precisione quando segnalano contenuti illegali, senza la necessità di rappresentare interessi collettivi.

Alcuni Stati membri hanno espresso anche la necessità di un riesame della *good-samaritan clause* di cui all'Articolo 6, interrogandosi sulla possibilità che l'esenzione derivante dalle indagini volontarie contro i contenuti illegali sia sufficiente per favorire un'azione significativa da parte del fornitore di servizi o se, invece, siano necessarie ulteriori garanzie per prevenire eventuali abusi.

Infine, un'altra questione attiene alla protezione dei segreti commerciali dei prestatori di servizi "in relazione all'accesso ai dati e alle indagini".

Alcuni dei rilievi critici e degli spunti emersi nell'ambito sia della consultazione degli *stakeholders* sia dei lavori del Consiglio trovano eco nel report rilasciato dal **Committee on the Internal Market and Consumer Protection (IMCO) del Parlamento europeo**.[75]

Riguardo all'impianto generale, la *rapporteur* Christel Schaldemose esprime forte perplessità rispetto all'**approccio *one size fits all*** della proposta di DSA: l'assenza di una distinzione delle piattaforme alla luce dei loro diversi modelli di business si traduce nella mancanza di una adeguata valorizzazione del ruolo particolare svolto dai *marketplaces*, per i quali invece la *rapporteur* suggerisce l'introduzione di una apposita disposizione con requisiti più stringenti ai fini dell'esenzione da responsabilità con la finalità di rafforzare la tutela dei consumatori ed uniformare il rispetto delle regole per tutte le imprese che operano *online*. L'IMCO, infatti, propone ulteriori obblighi di *due diligence* per gli *online marketplaces* (i.e. i servizi che consentono ai consumatori di concludere contratti a distanza con i venditori) al fine di beneficiare delle esenzioni di responsabilità (*cfr.* Art. 5, proposta di modifica n. 73). In particolare, IMCO propone di introdurre obblighi di *due diligence* in capo agli intermediari nel caso in cui imprese di Paesi terzi si servano dei relativi servizi per raggiungere i consumatori.

[75] Il testo è disponibile all'indirizzo internet https://www.europarl.europa.eu/doceo/document/IMCO-PR-693594_EN.pdf?redirect. Cfr. anche i report dei Committee associati (per quanto di competenza) Civil Liberties, Justice and Home Affairs (LIBE), the Committee for Industry, Research and Energy (ITRE) and the Legal Affairs Committee (JURI).

IMCO propone altresì di introdurre la possibilità per i consumatori di richiedere forme di risarcimento nei confronti degli intermediari, che a loro volta potranno rivalersi sui venditori.

Allo stesso modo, viene proposto di rafforzare l'obbligo di tracciabilità degli operatori commerciali sia estendendo il suo campo di applicazione a tutti gli intermediari sia introducendo specifiche disposizioni per i *marketplaces* che consentano il tracciamento non solo dei *traders* ma anche dei prodotti e servizi venduti tramite la piattaforma (cfr. proposte Artt. 13b e 22).

Anche l'IMCO mostra dubbi significativi rispetto al trattamento privilegiato riservato alle microimprese e piccole imprese e propone che a queste siano applicati tutti gli obblighi aggiuntivi previsti per le piattaforme online, con la sola eccezione degli obblighi di comunicazione trasparente di cui all'Articolo 23[76].

Ulteriori modifiche sono, inoltre, proposte con riferimento ai criteri per determinare l'ambito di applicazione del Regolamento (cfr. modifiche suggerite per gli Artt. 1 e 2), all'identificazione delle autorità competenti (con particolare riferimento all'obbligo di notifica di sospetto di reato - *cfr.* emendamento 61) ed alla possibilità di rafforzare i poteri del coordinatore dei servizi digitali e della Commissione, con particolare riferimento alla possibilità di chiedere all'autorità giudiziaria competente eventuali restrizioni all'accesso all'interfaccia online del prestatore di servizi intermediari che abbia ripetutamente violato gli obblighi del Regolamento.

L'IMCO ha inoltre insistito sul rafforzamento degli obblighi di trasparenza a tutela dei consumatori, specialmente in caso di uso di algoritmi da parte degli intermediari.

Di particolare interesse risultano, infine, le proposte di emendamenti relative al meccanismo di rimozione dei contenuti illeciti. La *rapporteur*, infatti, ritiene necessario definire, all'interno del DSA, una cornice regolamentare che definisca in modo chiaro e preciso procedure, tempi e garanzie per il **sistema di *notice and takedown*** al fine di assicurare sia l'applicazione uniforme in tutti gli Stati membri sia la rimozione tempestiva dei contenuti illeciti. Più nello specifico, il report dell'IMCO individua due scadenze temporali differenti per la rimozione dei contenuti sulla base dell'impatto di questi ultimi sulla sicurezza e salute pubblica e dei consumatori: per essere esentata da ogni responsabilità, una piattaforma sarebbe tenuta a rimuovere entro 24 ore tutti quei contenuti illeciti che possono arrecare un danno significativo, laddove invece il termine ordinario per gli altri contenuti sarebbe di sette giorni (cfr. le proposte di modifica all' Art. 5). Scadenze temporali sono altresì proposte per i sistemi interni di gestione dei reclami.

Inoltre, per quanto concerne le violazioni ripetute, il report suggerisce di prevedere che l'obbligo di sospensione degli utenti da parte delle piattaforme in caso di abusi di cui all'Articolo 20 non sia circoscritto alle ipotesi di contenuti manifestamente illegali.

Altra proposta avanzata dall'IMCO è quella di prevedere eventuali obblighi di *stay down* dei contenuti già soggetti a *take down*, specialmente sugli *online marketplaces* (cfr. proposte di modifica all'Art. 14, proposta n. 96).

[76] È da segnalare, tuttavia, che l'opinione del DRAFT ITRE, invece, suggerisce l'estensione di alcune esenzioni eccessivamente gravose per le micro e le piccole imprese, https://www.europarl.europa.eu/doceo/document/ITRE-PA-693552_EN.pdf

La riflessione aperta dalle proposte dell'IMCO in tema di *notice and takedown* appare particolarmente tempestiva ed opportuna alla luce delle Linee guida (faticosamente) licenziate dalla Commissione europea sull'interpretazione dell'**Articolo 17 della Direttiva CDSM**[77] e, dunque, in vista di quel coordinamento necessario, invocato da più parti, del DSA con le altre normative europee vigenti. Sebbene non siano vincolanti, le suddette Linee guida, infatti, prevedono che, nell'ambito dei *best efforts* richiesti per impedire la circolazione di materiali protetti, le piattaforme siano tenute ad adottare soluzioni tecnologiche che consentano il riconoscimento e l'eventuale blocco, a valle di una rapida analisi *ex ante*, di quei contenuti identificati dai titolari dei diritti come manifestamente illeciti, con ciò intendendosi quei contenuti che possono arrecare un danno economico significativo. Viceversa, il caricamento di materiali non manifestamente illegali dovrebbe essere consentito in linea di principio e soggetto alla tradizionale procedura di *notice and takedown*, basata dunque su un'analisi *ex post* del contenuto, previo invio di segnalazione da parte dell'avente diritto. I medesimi presupposti si applicano anche alla procedura di *notice and stay down.*

In sede di discussione nazionale si segnala anche il Documento approvato dalla Commissione IX della Camera dei Deputati sulla proposta di Regolamento DSA, il quale esprime parere favorevole sulla proposta, formulando altresì alcune osservazioni[78].

[77] Commissione europea, ***Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market***, COM (2021) 288 final.
[78] Testo disponibile nel Bollettino delle Giunte e delle Commissioni Parlamentari Trasporti, poste e telecomunicazioni (IX) – All. 4, https://www.camera.it/leg18/824?tipo=A&anno=2021&mese=06&giorno=23&view=&commissione=09# e sulla piattaforma IPEX (Platform for EU Interparliamentary Exchanges) https://secure.ipex.eu/IPEXL-WEB/document/COM-2020-0825/itcam

5. Le principali questioni oggetto del dibattito rilevanti per l'*enforcement* dei diritti di proprietà industriale *online* e l'impatto sugli *stakeholders*

A valle dell'analisi dettagliata delle principali disposizioni della proposta di DSA e dei rilievi emersi nell'ambito sia della consultazione degli *stakeholders* sia dei lavori in seno al Consiglio dell'Unione europea ed al Parlamento europeo, è possibile individuare le questioni più rilevanti per l'*enforcement* dei diritti di proprietà industriale *online* ed avanzare alcune proposte di modifica e di integrazione dell'attuale proposta alla luce dell'impatto che le stesse possono avere sui diversi *stakeholders* interessati, con particolare riferimento alla situazione nazionale.

5.1 Obblighi di *stay down*, rischi di blocco eccessivo e ambito soggettivo dei *trusted flaggers*

Nell'ambito delle disposizioni relative alla responsabilità delle piattaforme, quella concernente il sistema di *notice and take down (meccanismo di notifica e azione)* e la possibile introduzione di obblighi di notifica e blocco permanente (*notice and stay down*) è sicuramente la più attenzionata e dibattuta. In particolare, la necessità che le piattaforme digitali siano chiamate a prevenire *ex ante* la messa in rete di contenuti contraffatti, e non semplicemente di rimuovere *ex post* gli stessi, è ovviamente posta con forza dai titolari dei diritti quale elemento imprescindibile per assicurare una effettiva tutela anche alla luce della disponibilità di diversi strumenti informatici che consentono di rilevare automaticamente la messa in rete di determinati contenuti. Si fa, al riguardo, riferimento a strumenti di riconoscimento automatico di contenuto (*automatic content recognition*) che si basano su diverse tecniche, quali l'hash numerico (*hashing*), la marcatura numerica (*watermarking*) e l'impronta digitale (*fingerprinting*). Allo stesso tempo, non possono essere sottaciute le preoccupazioni da più parti sollevate riguardo alla compatibilità di una tale misura con alcune libertà e diritti fondamentali ed al rischio di abusi derivanti da un blocco eccessivo di contenuti.

Come abbiamo già avuto modo di segnalare, a nostro avviso tale riflessione non può prescindere dal coordinamento con la tutela del diritto d'autore online, recentemente riformata dalla Direttiva CDSM[79].

L'Articolo 17 della suddetta Direttiva prevede un nuovo regime di responsabilità applicabile ai prestatori di servizi di condivisione online, stabilendo obblighi di sorveglianza di fatto dei contenuti che gli utenti dei loro servizi mettono in rete, al fine di prevenire il caricamento delle opere e dei materiali protetti che i titolari dei diritti non desiderano rendere accessibili su tali servizi. Sebbene la versione finale della direttiva 2019/790 non contenga riferimenti espressi agli strumenti di riconoscimento automatico di contenuto, non imponendo, dunque, formalmente l'adozione di misure o di tecniche specifiche, tale sorveglianza preventiva assumerà di norma la forma di un filtraggio di tali contenuti, realizzato con l'ausilio di strumenti informatici utili alle piattaforme per evitare le menzionate responsabilità. Riguardo l'applicazione della suddetta disposizione, la Commissione europea ha recentemente pubblicato i suoi orientamenti sottolineando che i titolari dei diritti dovrebbero avere la possibilità di riservare (*earmark*) i materiali la cui messa in rete non autorizzata sia idonea a causare loro un danno economico significativo e che i prestatori di servizi di condivisione online non adempierebbero ai loro obblighi di *best efforts* qualora consentissero la messa in rete di contenuti che riproducono questi stessi materiali nonostante siffatte riserve[80].

È altresì utile richiamare le riflessioni, al riguardo, svolte dall'Avvocato generale Øe nelle conclusioni davanti alla Corte di giustizia chiamata a pronunciarsi sul ricorso presentato dalla Polonia[81]. Øe segnala, infatti, che gli orientamenti della Commissione non definiscono la nozione di danno economico significativo né contengono criteri che limitino in maniera oggettiva il meccanismo di riserva a taluni casi particolari. L'Avvocato generale rileva, inoltre, come, se il meccanismo delineato dovesse essere inteso nel senso che i prestatori dovrebbero bloccare *ex ante* taluni contenuti dietro la mera allegazione di un rischio di danno economico importante da parte dei titolari dei diritti quand'anche tali contenuti non fossero manifestamente contraffatti, ciò non risulterebbe in linea con l'esigenza di assicurare garanzie sufficienti a salvaguardare il giusto equilibrio fra i diversi interessi in gioco.

In sintesi, secondo l'Avvocato Generale, se i titolari non possono esigere il rischio zero quanto ad eventuali violazioni dei loro diritti e non si possa richiedere che i prestatori intermedi procedano a valutazioni autonome della legalità dei contenuti, dall'altra parte il diritto fondamentale alla libertà di espressione non osta a tutti i tipi di obbligo di sorveglianza. Al fine di ridurre al minimo il rischio di blocco eccessivo, un prestatore intermedio dovrebbe essere unicamente tenuto a filtrare e a bloccare contenuti la cui illiceità sia stata previamente accertata da un giudice o, altrimenti, informazioni il cui carattere illecito sia di immediata evidenza, vale a dire manifesto, senza, segnatamente, che ne sia necessaria la contestualizzazione. Le misure di filtraggio che i prestatori di servizi di condivisione sono tenuti ad attuare devono, dunque, limitarsi, secondo Øe, ai contenuti che sono «identici» o «equivalenti» alle opere e agli altri materiali protetti identificati dai titolari dei diritti.

[79] La necessità di coordinamento tra i due testi normativi è stata recentemente sottolineata da più posizioni. Cfr. Documento approvato dalla Commissione IX della Camera dei Deputati sulla proposta di Regolamento DSA (nota 82) e il Report dell'European Audiovisual Observatory, Unravelling the Digital Sevices Act Package, Strasburgo, Ottobre 2021.
[80] Commissione europea, ***supra*** nota 77.
[81] Conclusioni dell'Avvocato generale Øe, ***supra*** nota 33.

Tali riflessioni, sebbene svolte nel contesto del diritto d'autore e del giusto equilibrio tra la tutela di quest'ultimo e il diritto fondamentale alla libertà di espressione, si rivelano utili anche in questa sede, con riferimento ad altre privative industriali. Del resto, come già segnalato, se non tutte le preoccupazioni emerse in ambito di diritto d'autore con riferimento alle possibili limitazioni alla libertà di espressione siano applicabili anche al contesto dei marchi e dei brevetti, è altrettanto vero che in quest'ultimo contesto occorra comunque assicurare il giusto equilibrio con la libertà di concorrenza ed il principio di libera circolazione nel mercato interno, sicché, come stabilito dalla Corte in *eBay*, un obbligo di sorveglianza non possa avere l'oggetto o l'effetto di imporre un divieto generale e permanente di messa in vendita, in un mercato, di prodotti contrassegnati da alcuni marchi o protetti da brevetti.

Dunque, da una parte la recente evoluzione della tutela del diritto d'autore *online* consente di prevedere anche per la proprietà intellettuale interessata dal DSA l'introduzione di strumenti di *notice and stay down*, dall'altra parte per un regime di responsabilità come quello delineato dal DSA si pone la medesima esigenza avvertita per la Direttiva CDSM di prevedere garanzie sufficienti per ridurre al minimo i rischi di blocco eccessivo e definire un contesto normativo che fissi regole chiare e precise disciplinanti la portata e l'applicazione delle misure di filtraggio attuate dalle piattaforme.

In quest'ottica, in parallelo con l'interpretazione della Direttiva CDSM fornita dagli orientamenti della Commissione e con i rilievi in tema sollevati dall'Avvocato Generale Øe, **si potrebbe ipotizzare la previsione a carico di tutte piattaforme di un obbligo rimuovere (e inibire l'accesso) a quei prodotti la cui illiceità sia stata previamente accertata da un giudice o che risultino manifestamente illeciti e idonei a determinare un danno significativo in quanto eventualmente segnalati come tali dai *trusted flaggers*, senza che alle piattaforme sia richiesta una valutazione autonoma.** Tale previsione andrebbe accompagnata da una **chiara definizione di danno significativo**, la quale risulterebbe necessaria anche ai fini della procedura di *notice and take down*, laddove si decidesse di accogliere la proposta avanzata dall'IMCO relativamente alle scadenze temporali per la rimozione dei contenuti sulla base dell'impatto di questi ultimi sulla sicurezza e salute pubblica e dei consumatori.

Si ricorda, inoltre, come nell'ordinamento italiano siano già presenti alcuni meccanismi di notifica e azione, *stay down* e misure per le violazioni reiterate nell'ambito del procedimento che prevede la competenza amministrativa in materia di tutela del diritto d'autore online dell'Autorità per le Garanzie nelle Comunicazioni (Agcom), ai sensi del Regolamento in Materia di Tutela del Diritto d'autore sulle reti di Comunicazione Elettronica e Procedure Attuative ai sensi del Decreto Legislativo 9 Aprile 2003, N. 70 (come da ultimo modificato dalla Delibera n. 233/21/CONS). Il Regolamento è considerato una *best practice* a livello internazionale.

Strettamente collegata alla procedura di *notice and take down* nonché alla previsione di un obbligo di *stay down* è altresì **la definizione dell'ambito soggettivo dei *trusted flaggers*.** In termini generali, proprio in ragione del ruolo che i segnalatori attendibili sono chiamati a svolgere nel DSA, si avverte l'esigenza di circoscrivere attentamente il perimetro dei soggetti che ambiscono a conseguire tale status, definendo criteri chiari, oggettivi e stringenti al fine di evitare un eccessivo allargamento della categoria. **E, tuttavia, l'esclusione *tout court* dei titolari di diritti di proprietà industriale dal novero dei *trusted flaggers* non sarebbe forse ragionevole**. Esattamente come la Commissione europea riconosce nella Direttiva CDSM ai titolari dei diritti di *earmark* i materiali la cui messa in rete non

autorizzata sia idonea a causare loro un danno economico significativo, mal si comprenderebbe, infatti, il motivo per il quale, nei casi di contraffazione, la medesima possibilità non debba essere prevista per i *brand owners o i patent owners*, i quali sono certamente portatori di un interesse meritevole di tutela da parte del DSA. Tale inclusione potrebbe eventualmente essere prevista in presenza di specifiche circostanze.

5.2 La *good samaritan clause* ed i meccanismi di incentivo per l'autoregolazione

In stretta correlazione con la responsabilizzazione delle piattaforme si pone la discussione del meccanismo cd "*good samaritan clause*" che estende il beneficio dell'esenzione da responsabilità alle ipotesi in cui gli intermediari intraprendano volontariamente misure proattive tese ad accrescere il loro livello di conoscenza sulle condotte illecite perpetrate sulle loro piattaforme. Se tali iniziative sono svolte in buona fede, nonostante possono accrescere il livello di conoscenza degli illeciti, scatta il meccanismo dell'esenzione di responsabilità.

Tale clausola trae origine da una protezione garantita negli Stati Uniti dalla Section 230 (47 U.S.C. § 230) e dalla Section 230(c), avente lo scopo di evitare la responsabilizzazione degli intermediari per misure volontarie adottate in buona fede su alcuni contenuti, nonostante –talvolta- l'inefficacia delle misure adottate[82]. Se trasposta nell'ordinamento euro-unitario, tuttavia, una simile clausola assume connotati diversi in relazione al sistema dei *safe-harbours* della Direttiva e-commerce, la cui impostazione – interpretata peraltro dalle Corti- è mantenuta dal DSA.

L'art. 6 del DSA potrebbe avere un impatto positivo sulle piattaforme non disincentivando una autoregolazione volontaria, volta ad una prevenzione ulteriore delle condotte illecite. Gli intermediari sarebbero così incentivati a sviluppare misure volontarie proattive senza essere considerati necessariamente "attivi" e dunque responsabilizzati. Anche i titolari dei diritti potrebbero beneficiare di tale meccanismo.

Tale esenzione di responsabilità nell'ordinamento euro-unitario potrebbe, tuttavia, rendere immuni da responsabilità condotte da parte degli intermediari – sebbene in buona fede- inefficaci (in quanto le azioni non assicurano un effettivo *enforcement*[83]) oppure potrebbe incentivare una autoregolazione privata "sproporzionata" in contrasto con la libertà di espressione degli utenti, con la libera

[82] Si ricorda come nelle condizioni generali di contratto di molti intermediari che gli utenti sottoscrivono per utilizzare i relativi servizi, vi siano clausole che obbligano al rispetto dei diritti di proprietà intellettuale di terzi. La eventuale contraffazione rappresenta, infatti, anche inadempimento contrattuale nei confronti della piattaforma. Tale meccanismo è spiegato in alcuni casi giurisprudenziali statunitensi. Cfr. Demand for Jury Trial, US Northern District Court of California, Case No. 3:21-cv-3036, ***Facebook, Inc., a Delaware corporation, and Gucci America, Inc., v. Natalia Kokhtenko***, 26.4.2021, §28 https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-03036/Facebook_Inc._et_al_v._Kokhtenko/1/.

[83] Cfr. in particolare le osservazioni del BEUC, ***The Digital Services Act proposal***, (2021) https://www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf.

circolazione di beni e servizi e con la libertà di concorrenza, con impatto negativo anche per gli interessi dei titolari dei diritti, dei consumatori e delle imprese.

Dubbi sono stati avanzati, infatti, da un lato, sulla concreta operatività della clausola all'interno del DSA al fine di favorire un'azione realmente significativa da parte del fornitore di servizi (ossia un'azione che non serva soltanto ad esentare formalmente l'intermediario da responsabilità) e, dall'altro lato, sulla necessità di circoscrivere la portata della clausola e/o inserire eventuali ulteriori garanzie per prevenire abusi nei confronti degli utenti delle piattaforme che potrebbero essere ingiustamente discriminati da tali condotte volontarie[84].

Ai fini di una maggiore operatività della previsione, la clausola potrebbe specificare più precisamente le azioni volontarie da non disincentivare (e.g. termini e condizioni più stringenti, azioni investigative volte allo specifico scopo di identificare e rimuovere contenuti illeciti, nello specifico ove l'illiceità sia già stata in precedenza accertata)**, accompagnando tale elencazione alla indicazione di misure di salvaguardia come la supervisione umana in caso di controlli algoritmici o maggiore tracciabilità.**

Nelle more della discussione per l'approvazione del DSA è da riscontrare, inoltre, una maggiore tendenza da parte delle piattaforme a collaborare virtuosamente con i titolari dei diritti di proprietà industriale e con le associazioni di categoria per prevenire o contrastare la contraffazione mediante i canali *online*[85].

Ne sono un esempio alcune cause congiunte intentate da piattaforme e titolari dei diritti contro utenti delle piattaforme che usano tali canali per pubblicizzare e vendere merci contraffatte, in tal modo contravvenendo altresì ai termini di servizio ed alle condizioni d'uso degli intermediari che prescrivono agli utenti il rispetto dei diritti di proprietà intellettuale di terzi (e.g. la causa di Gucci e Facebook davanti al Tribunale distrettuale nord della California nei confronti di un utente[86] oppure le cause congiunte di Amazon con Valentino e Ferragamo[87]). Le piattaforme (specialmente di maggiori dimensioni) stanno, inoltre, istituendo unità dedicate alle investigazioni volontarie ed alle segnalazioni alle autorità nazionali di condotte di contraffazione. Si segnalano, in particolare, in ambito di tutela dei marchi e dei modelli di utilità, le importanti iniziative avviate da alcune piattaforme per eliminare o quantomeno ridurre il numero di prodotti contraffatti, anche tramite sistemi automatizzati e segnalazioni.

Sebbene tali iniziative siano virtuose nell'ottica della tutela *online* della proprietà industriale, emerge tuttavia una possibile preoccupazione per la tutela della concorrenza, in quanto l'implementazione di tali sistemi – agevolata dalla *good samaritan clause* – richiede l'investimento di risorse ingenti, portando forse nel lungo periodo ad un ulteriore rafforzamento del potere di mercato delle (grandi)

[84] Cfr. rapporteur for the Culture and Education (CULT) committee of the European Parliament, Sabine Verheyen (EPP, Germany). Cfr. Anche il report LIBE (amendment 36, https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf) che suggerisce finanche la cancellazione dell'articolo, in quanto le imprese private non avrebbero i requisiti di indipendenza, ***accountability*** e qualifiche dei pubblici ufficiali e non dovrebbero essere incentivati ad un ***enforcement*** privato dei diritti, che potrebbe avere impatti significativi sui diritti fondamentali. Secondo tale report, tale clausola non sarebbe neanche necessaria in quanto nel diritto dell'Unione e nella relativa interpretazione ad opera della Corte di Giustizia i ***providers*** non sono ritenuti responsabili per il solo fatto di compiere indagini volontarie.

[85] Cfr. in tema anche l'esperienza maturata nell'ambito del Memorandum of Understanding on the sale of counterfeit goods on the internet. Si veda il Report della Commissione SWD (2020) 166 final/2, p. 15-16 e C(2018) 1177, §18-20

[86] ***Supra*** nota 82.

[87] ***Amazon, Inc. and Valentino S.p.A., v. Kaitlyn Pan Group, LLC and Hao Pan,*** 2:20-cv-00934 (W.D. Wash.) .

piattaforme a cui i titolari dei diritti saranno più inclini ad affidarsi rispetto a concorrenti che non offrano simili servizi (e dunque innalzando le barriere all'ingresso nei relativi mercati).

Amazon – Brand Protection Program[88]

Il Brand Protection Program di Amazon intende identificare e bloccare eventuali prodotti contraffatti circolanti sulla piattaforma.

L'approccio utilizzato dall'azienda per la gestione dell'anticontraffazione si compone di tre principali strategie.

La prima viene indicata con la nomenclatura "***Robust proactive controls***" e si basa sull'utilizzo di una combinazione di strumenti di machine learning e di esperienza investigativa umana, al fine di bloccare i malintenzionati prima di una loro eventuale pubblicazione di inserzioni o prodotti di vendita. In particolare, coloro che desiderano divenire dei partner di vendita dell'azienda devono obbligatoriamente fornire un documento di identità con foto rilasciato dal Governo nonché dettagliare ulteriori informazioni sulla loro identità, posizione geografica, conto bancario, posizione contributiva al sistema erariale, carta di credito e molto altro. Partendo da queste informazioni, i sistemi proprietari di Amazon verificano la veridicità dei dati forniti con lo scopo di identificare e bloccare potenziali rischi, prima che si verifichino fattivamente. Tale sistema di accertamento conta inoltre di strumenti di controllo live tramite video e di verifica fisica dell'indirizzo fornito. Nel 2020, questo meccanismo a più fasi di controllo ha permesso di bloccare più di 6 milioni di tentativi di creare falsi account di vendita.

La seconda strategia adottata nell'ambito del programma Brand Protection, indicata come "***Powerful tools for brands***" si basa sull'offrire alle imprese degli strumenti efficaci per la gestione e tutela dei loro marchi, denominati rispettivamente ***Brand Registry***, ***Transparency***, e ***Project Zero.***

Il servizio gratuito ***Brand Registry,*** lanciato nel 2007, è teso ad offrire ai proprietari dei vari brand un insieme di strumenti che possano aiutare nella gestione e protezione dei loro marchi e, in generale, dei loro diritti di proprietà intellettuale, garantendo un maggior controllo sui contenuti riportati nelle pagine descrittive di dettaglio dei loro prodotti.

Un altro servizio complementare è il programma ***Transparency***, che prevede l'applicazione di un codice 2D univoco ai prodotti dell'azienda venditrice che viene verificato da Amazon prima di spedirlo al cliente, al fine di assicurarne l'autenticità.

Infine, ***Project Zero*** ambisce ad azzerare le contraffazioni sulla piattaforma.

Secondo l'azienda, il raggiungimento di questo obiettivo può essere perseguito attraverso le protezioni automatizzate di Amazon nei confronti di inserzioni di prodotti sospetti prima della pubblicazione, tramite i meccanismi del machine learning che prevedono un miglioramento continuo e un incremento nella precisione delle operazioni, ma anche attraverso la concessione ai brand di rimuovere direttamente loro stessi le inserzioni violanti i diritti della proprietà intellettuale dalla "vetrina" Amazon e mediante l'utilizzo del sopramenzionato codice 2D (sebbene non obbligatorio ma consigliato dato gli ottimi risultati).

Inoltre, nell'ambito di tale strategia di sostegno dei brand, Amazon ha istituito un ***IP Accelerator***, con target le piccole e medie imprese. In particolare, si prepone l'obiettivo di rendere più semplice e conveniente per le imprese proteggere i loro prodotti tramite gli strumenti di tutela della proprietà intellettuale. Per far ciò, l'azienda si pone come

[88] https://brandservices.amazon.com/; https://brandservices.amazon.com/progressreport

ponte tra gli imprenditori e alcuni studi legali specializzati in proprietà intellettuale, garantendo tariffe competitive definite ex ante.
Per concludere, l'azienda persegue una terza strategia complementare nell'ambito del ***Brand Protection Program*** denominata "***Holding counterfeiters accountable***". In questo ambito, è stata istituita un'unità ad hoc denominata ***Amazon Counterfeit Crimes Unit***, volta a riportare casi di contraffazione alle Autorità competenti, realizzare indagini indipendenti o in cooperazione con i brand, e perseguire contenziosi civili nei confronti dei contraffattori.

Alibaba – IP Protection Platform[89]

Nel perseguimento dei suoi obiettivi di protezione della proprietà intellettuale, tra i vari strumenti ideati ed utilizzati da Alibaba, l'azienda ha sviluppato una piattaforma ad hoc denominata Alibaba Intellectual Property Protection Platform (IPP), proposta come un meccanismo di risoluzione delle dispute inerenti alla proprietà intellettuale messa a dispozione delle aziende venditrici sulle diffenti piattaforme Alibaba (Taobao.com, Tmall.com, Tmall.hk, 1688.com, Aliexpress.com and Alibaba.com). In particolare, la piattaforma web permette di elaborare reclami per violazione della proprietà intellettuale, avanzati dai venditori, chiamati, in primis, a presentare i loro documenti di identità e i loro diritti di proprietà intellettuale. Una volta che questi ultimi sono verificati, le aziende coinvolte possono inviare richieste di rimozione per elenchi di prodotti sospetti di violazione dei sopracitati diritti che verranno prontamente rimossi. Il giudizio finale su tali prodotti, in termini di rimozione definitiva o ripristino, verrà definito dalla piattaforma anche sulla base di eventuali contronotifiche avanzate dalla controparte interessata.
È evidente, dunque, che le imprese iscritte alla Alibaba IPP Platform possono ottenere diversi benefici grazie alla trasversalità dell'utilizzo di tale sistema per le diverse piattaforme Alibaba e alla possibilità di usare un sistema web efficace ed efficiente per monitorare e gestire le attività connesse alla protezione della proprietà intellettuale.

Ebay – Verified Rights Owner Program[90]

Al fine di rendere Ebay un sistema di acquisto e vendita sicuro, la piattaforma ha sviluppato il programma Verified Rights Owner (VeRO). Tale sistema permette ai proprietari di diritti della proprietà intellettuale di segnare eventuali inserzioni che potrebbero violare i loro diritti. In particolare, le infrazioni segnalabili possono riguardare violazione dei diritti della proprietà intellettuale del venditore, contraffazione/replicazione di prodotti, uso non autorizzato di contenuti protetti all'interno di un elenco di prodotti o nella pagina di un prodotto specifico.
Coloro accusati della violazione sono chiamati a rivolgersi direttamente al proprietario che li ha segnalati, tranne in casi eccezionali di impossibilità dell'interazione in cui saranno gli addetti del programma VeRO ad intervenire come intermediari per connettere le due parti coinvolte. Inoltre, la piattaforma, ricevuta la notifica tramite il sistema VeRO di una presumibile violazione, rimuove il prima possibile l'inserizione incriminata.

[89] https://ipp.alibabagroup.com/
[90] https://pages.ebay.com/seller-center/listing-and-marketing/verified-rights-owner-program.html

Oltre alle funzioni sopraelencate, i proprietari di diritti della proprietà intellettuale che operano sulla piattaforma possono volontariamente creare una pagina al fine di condividere con la community Ebay informazioni sui loro diritti di proprietà. Tra queste informazioni, oltre ad un elenco degli stessi diritti, possono indicarsi quali potrebbero essere le eventuali conseguenze di una violazione di questi, eventualmente con lo scopo dissuadere malintenzionati e di ridurne le possibilità.
Giova sottolineare che i riceventi di multipli richiami di violazione VeRO possono andare incontro a diverse conseguenze, tra cui potenzialmente anche la sospensione da Ebay stesso. Tuttavia, diversamente dai sistemi implementati da altre piattaforme, questo programma non prevede una verifica ulteriore da parte di specifici team deputati al controllo. Infatti, il sito web afferma di non poter esprimire giudizi sui diritti della proprietà intellettuale di terze parti, e pertanto, richiede esplicitamente di risolvere eventuali dispute successive alla rimozione delle inserzioni incriminate contattando direttamente la controparte coinvolta che ha segnalato la violazione.

5.3 Obblighi di tracciabilità degli utenti professionali e dei prodotti che circolano sulle piattaforme

Nel corso delle consultazioni pubbliche che hanno preceduto l'adozione della proposta da parte della Commissione del *Digital Services Act*, diverse categorie di rispondenti (in particolare associazioni di consumatori e di categoria, autorità nazionali e venditori *online*) hanno segnalato la necessità di introdurre una speciale responsabilità per gli *online marketplace*.

I c.d. *online marketplace*, sono definiti da diverse fonti del diritto dell'UE, tutte tendenzialmente incentrate sulla possibilità per gli utenti di concludere, tramite questi servizi, contratti a distanza.[91] Ebbene, l'applicazione dell'articolo 14 della Direttiva E-commerce, come confermata dalla stessa Corte di giustizia,[92] non è sembrata negli anni sufficiente a risolvere una serie di problemi attienenti alla sicurezza ed autenticità dei prodotti (illeciti o difettosi) permanendo ad oggi il dubbio relativo allo *status* giuridico degli *online marketplace* in questa catena di valore e responsabilità, soprattutto nei casi in cui i prodotti illeciti possano raggiungere il mercato unico europeo solo per il tramite di questi servizi di intermediazione.[93]

Tra le diverse proposte avanzate in fase di consultazione, ha raccolto particolare consenso l'adozione di una norma che imponga agli *online marketplace* di verificare l'identità dei venditori che utilizzano i propri servizi, a tutela del mercato, della correttezza e della sicurezza delle transazioni commerciali.

[91] Commission Staff Working Document, ***supra*** nota 2, ANNEX 2, menziona: Regolamento (EU) 2019/1148 relativo all'immissione sul mercato e all'uso di precursori di esplosivi; Direttiva (EU) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("Direttiva NIS"); Regolamento (EU) 524/2013 relativo alla risoluzione delle controversie online dei consumatori; Direttiva 2019/2161, per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori che definisce, all'art. 3: "***n) "mercato online": un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori***". Cfr anche Art. 20 della Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 87/357/CEE del Consiglio e la direttiva 2001/95/CE del Parlamento europeo e del Consiglio - COM (2021) 346 final.

[92] ***eBay, supra*** nota 16.

[93] Commission Staff Working Document, ***supra*** nota 2, ANNEX 2, p. 163 e ss..

Questo principio, che ha preso il nome di KYBC, nella discussione originaria sembrava poter assumere diverse forme: un obbligo di informare i consumatori che hanno acquistato un prodotto falso; applicare misure efficaci per contrastare i trasgressori recidivi; implementare un sistema proattivo di gestione dei rischi; offrire una serie chiara di obblighi di trasparenza e rendicontazione; consultare le informazioni sui prodotti richiamati e pericolosi su RAPEX; e alcuni hanno anche proposto l'implementazione di misure proattive per impedire che prodotti illegali siano disponibili online.[94]

Dunque, all'esito della valutazione di impatto, la Commissione ha proposto un obbligo per le piattaforme *online* che consentano ai consumatori di concludere contratti a distanza con operatori commerciali, di raccogliere informazioni accurate e aggiornate circa i venditori che operano sui propri servizi (*cfr. supra*). Questo consentirebbe ai consumatori di effettuare scelte di consumo più consapevoli ed al contempo scoraggerebbe i venditori dall'offrire prodotti illeciti o difettosi agevolando anche le attività di *enforcement* delle preposte autorità.[95]

Coerentemente, la Commissione ha individuato tra i benefici diretti conseguenti l'introduzione di questa norma l'incremento della trasparenza delle transazioni e tra i beneficiari diretti i titolari dei diritti, le imprese, i consumatori e le autorità nazionali.[96]

Il testo dell'Articolo 22 - *Tracciabilità degli operatori commerciali (supra)* - proposto dalla Commissione prevede, appunto che, qualora una piattaforma *online* consenta ai consumatori di concludere contratti a distanza con operatori commerciali, la stessa provveda affinché sia impossibile pubblicizzare o offrire prodotti o servizi a consumatori situati nell'UE senza aver prima condiviso con la piattaforma una serie di informazioni, dettagliate dal medesimo articolo, che consentono una precisa individuazione del soggetto venditore. Il Considerando 49 aggiunge che: "*tale prescrizione dovrebbe applicarsi anche agli operatori commerciali che promuovono messaggi riguardanti prodotti o servizi per conto di marchi sulla base dei relativi accordi*".

In principio, tali informazioni dovrebbero essere limitate al minimo sufficiente per il perseguimento dello scopo, tuttavia, le proposte di emendamento provenienti dalla discussione parlamentare (di seguito dettagliati) sembrano tendere a modificare la lista delle informazioni che la piattaforma avrebbe l'obbligo di raccogliere.[97]

Ancora, la piattaforma non può limitarsi a chiedere e ricevere le dette informazioni, ma deve anche compiere "*sforzi ragionevoli*" per stabilire se le informazioni relative al nome, l'indirizzo, il numero di telefono e l'indirizzo di posta elettronica dell'operatore commerciale, nonché quelle relative all'iscrizione dell'operatore in un registro delle imprese o analogo registro pubblico, siano attendibili: "*avvalendosi di qualsiasi banca dati o interfaccia online ufficiale liberamente accessibile messa a disposizione da uno Stato membro o dall'Unione o chiedendo all'operatore commerciale di fornire documenti giustificativi provenienti da fonti affidabili*".

A tal proposito, il Considerando 50 suggerisce, per un'applicazione efficace e proporzionata dell'obbligo in parola, il ricorso ai registri delle imprese nazionali e il sistema di scambio di

[94] Id. p. 25.
[95] Considerando 49.
[96] Regulatory Scrutiny Board Opinion, ***Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC {COM (2020) 825} {SWD(2020) 348}{SWD(2020) 349}***, 6.11.2020 - SEC(2020) 432.
[97] Commission Staff Working Document, ***supra*** nota 2, PART 1/2, p. 64, para. 250.

informazioni sull'IVA, oppure ad uno scambio di documenti giustificativi affidabili, quali copie di documenti di identità, estratti conto, certificati relativi alla società e certificati del registro delle imprese, aggiungendo anche che possono essere utilizzate altre fonti purché offrano un livello di affidabilità "analogo". Inoltre, il medesimo Considerando chiarisce che le piattaforme interessate non dovrebbero comunque essere tenute a intraprendere attività di accertamento che si rivelino eccessive o costose né che si traducano in verifiche *in loco*. D'altra parte, si aggiunge, l'accertamento di tali informazioni da parte delle piattaforme non può valere a costituire una garanzia dell'affidabilità delle informazioni nei confronti dei terzi.[98]

Nel caso in cui le informazioni raccolte si rivelino inesatte o incomplete, la piattaforma deve chiederne la correzione senza indugio e qualora il venditore non soddisfi tale richiesta, la prestazione del servizio di *marketplace* deve essere sospesa.

Le informazioni così raccolte - che devono in ogni caso essere conservate dalla piattaforma per tutta la durata del contratto con l'operatore commerciale - devono poi essere messe a disposizione degli utenti in modo chiaro, facilmente accessibile e comprensibile (con la sola esclusione dei dettagli relativi ai documenti di identificazione e delle coordinate bancarie dell'operatore commerciale) e possono essere divulgate nella loro completezza solo nel rispetto del diritto applicabile o su ordine delle autorità preposte.

È anche fatto obbligo alle piattaforme di progettare e organizzare la propria interfaccia in modo da consentire agli operatori commerciali di adempiere ai propri obblighi riguardanti le informazioni precontrattuali ed in materia di sicurezza dei prodotti.

Invece appare implicito, e pure necessario per le piattaforme, un obbligo di adeguare le interfacce al fine di consentire l'assolvimento degli obblighi di comunicazione previsti dall'articolo 22, in quanto le piattaforme devono garantire che, non solo sia possibile una completa trasmissione delle informazioni previste dalla legge, ma che soprattutto la fruizione dei servizi di *marketplace* sia impossibile per i venditori che non abbiano correttamente adempiuto.[99]

La commentata formulazione dell'articolo 22 è già oggetto di dibattito in seno al Parlamento europeo; infatti, le diverse commissioni che si sono espresse hanno formulato proposte divergenti di seguito brevemente riassunte (in ordine cronologico).

La Commissione LIBE,[100] in ragione del rischio di *data breaches* e *identity theft*, suggerisce di non imporre la conservazione e pubblicazione di dati strettamente personali dell'operatore commerciale come fotografia, data di nascita e firma, non essendo questi elementi utili alla verifica della identità.

La Commissione ITRE[101] propone di limitare l'obbligo di comunicazione delle informazioni ai soli venditori professionisti e comunque di rimuovere il conto bancario dall'elenco delle informazioni da ottenere.

[98] Considerando 50.
[99] Regulatory Scrutiny Board Opinion, ***supra*** nota 94.
[100] Committee on Civil Liberties, Justice and Home Affairs, ***Draft Opinion on the proposal for a regulation of the European Parliament and of the Council Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC,*** Rapporteur for opinion: Patrick Breyer, 2020/0361(COD) 19.05.2021.
[101] Committee on Industry, Research and Energy, ***Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC***, Rapporteur for opinion: Henna Virkkunen, 2020/0361(COD) 27.5.2021.

La Commissione IMCO[102] propone di: (i) estendere a tutti i fornitori di servizi intermediari l'obbligo di tracciare gli utenti professionisti; (ii) aggiungere un obbligo per i *marketplace* di identificare il tipo di prodotti e servizi che il professionista intende offrire; (iii) introdurre la previsione da parte della Commissione europea di un elenco di fonti di informazione; (iv) prevedere che i consumatori possano chiedere un risarcimento al *marketplace* per i danni subiti; (v) introdurre un obbligo di adottare misure finalizzate a garantire che i prodotti commercializzati siano sicuri.

La Commissione CULT[103] sostiene: (i) l'estensione dell'obbligo in parola a tutti i fornitori di servizi di intermediazione ma limitatamente a clienti professionisti; (ii) l'estensione della durata del periodo di conservazione dei dati ai cinque anni successivi alla scadenza del contratto; (iii) l'introduzione di idonee sanzioni pecuniarie per il mancato rispetto delle prescrizioni.

Infine, la Commissione JURI[104] propone l'eliminazione dell'obbligo di cancellare le informazioni sul commerciante dopo la scadenza o risoluzione del contratto e l'introduzione di una serie di obblighi: (i) di fornire informazioni relative ai prodotti offerti per impedire la diffusione di prodotti illegali e contraffatti, in questo caso anche sulla base delle informazioni fornite dal titolare dei diritti; (ii) di richiedere agli operatori commerciali di intraprendere azioni correttive per i prodotti pericolosi anche tramite il ritiro del prodotto e la comunicazione al pubblico dei rischi di conformità (entro 48 ore); (iii) di sospendere l'*account* di operatori commerciali recidivi; (iv) di segnalare alle autorità gli operatori che non si conformano alle prescrizioni normative; (v) di consentire ai consumatori di chiedere un risarcimento al *marketplace* per i danni subiti.

A fronte di tale discussione, per i fini che qui rilevano, la proposta di obblighi di tracciabilità ha sicuramente impatto positivo per i consumatori che possono più agevolmente avere informazioni sulla riconducibilità di beni e servizi ad un determinato soggetto. Una tale norma potrebbe incentivare altresì la collaborazione virtuosa con titolari dei diritti, consentendo un controllo della filiera a beneficio dei consumatori (ad esempio con l'ausilio dei sistemi *blockchain*). In questa ottica, si segnala, dunque, come l'ambito soggettivo delle disposizioni KYBC possa estendersi anche oltre gli *online marketplaces*, tenendo in considerazione i servizi dove più frequentemente sono perpetrate condotte illecite (*e.g.* CDN).

Dall'altro lato, l'obbligo di tracciabilità potrebbe aggravare, invece, gli obblighi di *compliance* delle piattaforme, specialmente per gli oneri di verifica, e degli stessi utenti delle piattaforme (operatori commerciali) circa gli obblighi di informazione.

Pertanto, sarebbe opportuno specificare meglio l'ambito ed il contenuto degli obblighi di informazione e verifica, anche attraverso la promozione di standard e codici di condotta[105].

Merita, infine, particolare attenzione per l'*enforcement* dei diritti di proprietà industriale la **possibilità di tracciamento dei prodotti**, avanzata da IMCO. Ai sensi dell'emendamento proposto sub art. 22 (fa),

[102] Committee on the Internal Market and Consumer Protection, ***Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC***, Rapporteur: Christel Schaldemose, 2020/0361(COD) 28.5.2021.
[103] Committee on Culture and Education, ***Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC***, Rapporteur for opinion: Sabine Verheyen, 2020/0361(COD) 21.6.2021.
[104] Committee on Legal Affairs, ***Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC***, Rapporteur for opinion: Geoffroy Didier, 2020/0361(COD) 22.6.2021.
[105] Cfr. in tema anche l'esperienza maturata nell'ambito del Memorandum of Understanding on the sale of counterfeit goods on the internet. Si veda il Report della Commissione SWD(2020) 166 final/2

gli utenti commerciali sarebbero tenuti a fornire informazioni sui prodotti e servizi commercializzati, al fine di identificare in modo "inequivocabile" tali prodotti, e sulla *compliance* degli stessi al diritto dell'Unione. **A tal fine, anche il rispetto dei diritti di proprietà industriale potrebbe essere una delle informazioni necessarie da richiedere ai venditori.**

5.4 *Compliance* normativa, approccio basato sul rischio ed obblighi per le microimprese e le piccole imprese

Una ulteriore questione di particolare rilevanza consiste nella possibilità di una adeguata *compliance* normativa al DSA da parte delle imprese in materia di tutela *online* dei diritti di proprietà industriale. L'approccio basato sul rischio e a geometria variabile è generalmente apprezzato da tutti i portatori di interesse, sebbene si sia già segnalata l'opportunità di coordinare le definizioni dei soggetti regolati con quelle di altre fonti settoriali interferenti con il DSA (Digital Markets Act, Direttiva AVMS, Direttiva Copyright, come anche la disciplina che qualifica l'illiceità delle condotte da prevenire o reprimere), al fine di assicurare un quadro di riferimento preciso e di non imporre obblighi sproporzionati di *compliance* in capo alle imprese che gestiscono servizi di intermediazione. Ancora, un coordinamento potrebbe rendersi necessario per evitare problemi di interferenza delle discipline applicabili, oltre che incertezze sull'*enforcement* in relazione all'individuazione dell'autorità competente (nonché per evitare rischi di *bis in idem*).

L'attuale formulazione, inoltre, prevede l'esclusione delle micro e delle piccole imprese dagli obblighi previsti per le piattaforme *online* (come vorrebbe l'art. 16 della proposta di DSA della Commissione). Come già anticipato, tale aspetto potrebbe essere rimeditato, privilegiando un approccio basato sul rischio di diffusione di contenuti illeciti anziché su criteri quali dimensioni e fatturato delle imprese. L'esclusione potrebbe essere limitata a obblighi che di fatto impongano oneri sproporzionati di *compliance* che non sono ragionevolmente esigibili da imprese di siffatte dimensioni (e.g. Art. 23). L'esclusione non appare invece persuasiva, ad esempio, rispetto agli obblighi di tracciabilità degli operatori commerciali (ai sensi dell'Art. 22), considerando la finalità perseguita dal DSA di contrasto all'illegalità online specialmente per quanto riguarda le attività di contraffazione.

Quanto all'obbligo di cui all'Art. 21 della proposta della Commissione - che prevede la comunicazione da parte della piattaforma online in caso di sospetto di commissione di un reato grave che comporta una minaccia per la vita o la sicurezza delle persone - non si possono non reiterare le perplessità in precedenza espresse circa la formulazione della norma. Tali perplessità sono confermate dai numerosi rilievi formulati dalla Commissione LIBE.

Si sottolinea in particolare come **la formulazione della norma dovrebbe essere rivista così da indicare in modo più preciso la portata dell'obbligo gravante sulle piattaforme**. La norma non specifica cosa si intenda per "gravità del reato" né chiarisce quali siano le ipotesi che comportino una "minaccia alla vita" o alla "sicurezza delle persone", così rendendo difficoltoso per gli intermediari identificare quali

siano i reati per cui vige un obbligo di comunicazione (e.g. i reati di contraffazione). **In tale ottica, la norma dovrebbe circoscrivere gli obblighi di comunicazione e delimitare con chiarezza le informazioni richieste al provider, per soddisfare la finalità di un più efficace contrasto all'illegalità *online*, senza tuttavia appesantire gli oneri di comunicazione e indagine preventiva degli intermediari, essendo sempre possibile per le autorità competenti richiedere informazioni maggiormente dettagliate[106].**

È utile segnalare che un simile obbligo di *reporting* è previsto anche dall'Art. 14.5 del recente Regolamento (UE) 2021/784 del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici online che richiede al "prestatore di servizi di hosting" di "informare immediatamente l'autorità competente per l'indagine e il perseguimento di reati negli Stati membri interessati" qualora sia "a conoscenza contenuti terroristici che comportano una minaccia imminente per la vita". Si può notare come tali ipotesi siano limitate alle ipotesi di "minaccia imminente per la vita" e non anche per la "sicurezza delle persone" e come l'obbligo sia innescato dalla "conoscenza" (e non dal mero sospetto) di contenuti terroristici (la cui definizione è chiaramente fornita dal Regolamento) che comportino una imminente minaccia per la vista delle persone. Il considerando n. 41 del predetto Regolamento, infatti, che "al fine di garantire la proporzionalità, tale obbligo dovrebbe essere limitato ai reati di terrorismo quali definiti all'Articolo 3, paragrafo 1, della direttiva (UE) 2017/541" e che "tale obbligo di informare non dovrebbe imporre ai prestatori di servizi di hosting l'obbligo di cercare attivamente prove di una tale minaccia imminente per la vita o un presunto reato di terrorismo". La definizione del precetto in questo caso è maggiormente legata alla individuazione del perimetro dell'obbligo di segnalazione (contenuti terroristici) e del presupposto di operatività.

Inoltre, la norma privilegia la tempestività della comunicazione da parte del provider piuttosto che il contenuto o il dettaglio della stessa ed identifica le autorità competenti a ricevere tali informazioni (sulla base della competenza giurisdizionale, o, in caso di dubbio, all'Europol).

A tal fine, per la corrispondente norma del DSA (Art. 21) potrebbe essere auspicata una riformulazione che valorizzi una maggior determinatezza del contenuto e dei presupposti degli obblighi di comunicazione, unitamente alla definizione di reato grave, eventualmente attraverso meccanismi in continuo aggiornamento, superando la mera esemplificazione del cons. 48. Si segnala a tal proposito che la commissione LIBE del PE suggerisce la seguente modifica al DSA: "*where an online platform becomes aware of any information giving rise* ***to a suspicion that a serious criminal offence involving a threat to the life of persons is imminent*** *it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide the information that gave rise to it*"[107]. La limitazione alla "minaccia alla vita delle persone" sembrerebbe peraltro escludere da tale profilo i reati di contraffazione; la formulazione, tuttavia, presenta profili di indeterminatezza tali per cui potrebbe comunque residuare la rilevanza di forme anticipate di tutela riconducibili alla salute pubblica (potendosi per questa via recuperare anche talune figure criminose rilevanti anche sotto il profilo qui preso in esame).

[106] Cfr. anche il draft proposto dalla Commissione LIBE del PE. European Parliament, LIBE draft opinion on Digital Services Act, 19 May 2021, amendment n. 86, https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf.
[107] Cfr. Amendment 86 draft proposto dalla Commissione LIBE.

Infine, se le pertinenti previsioni del DSA non pongono espressamente in capo alla piattaforma un obbligo generale di impedire la realizzazione del reato - bensì quello di comunicare senza indugio all'Autorità competente 'le ragioni del sospetto'- **tale scelta normativa dovrebbe essere valorizzata nel senso di ritenere inesigibile una condotta impeditiva da parte del responsabile della piattaforma o del soggetto preposto al controllo e di ritenere pertanto l'assenza in capo a quest'ultimo dei correlativi poteri di 'blocco' della vicenda criminosa**. La responsabilità penale del *provider* ex art. 40 c.p. dovrebbe ritenersi incompatibile, peraltro, con il divieto di imposizione di obblighi di controllo preventivi, anche per evitare rischi di *overenforcement* a discapito della libertà di espressione, della libera circolazione di beni e servizi e della libertà di concorrenza.

6. Raccomandazioni preliminari di policy

Come segnalato in premessa, nel momento in cui il presente Report è stato elaborato il processo di approvazione del DSA non è stato completato, essendo attualmente all'attenzione del Consiglio dell'Unione europea e del Parlamento europeo. Pertanto, il lavoro di analisi svolto ha come riferimento la proposta originaria formulata dalla Commissione europea.

In quest'ottica, **le conclusioni preliminari dello studio riguardano alcune raccomandazioni di *policy* relative alle questioni più rilevanti e critiche emerse con riferimento alla lotta contro la contraffazione dei diritti di proprietà industriale perpetuata online. Tali conclusioni, illustrate ed argomentate in modo più esteso al precedente §5, hanno la finalità di fornire un contributo al dibattito pubblico in corso nelle sedi istituzionali**.

Obblighi di sorveglianza e procedure di "notifica e azione"

Nell'ambito delle disposizioni relative alla responsabilità delle piattaforme, è opportuno che, rispetto alla previsione di un sistema di *notice and action* e alla possibile introduzione di obblighi di blocco permanente di alcuni contenuti (*stay down*), rilevanti per la tutela dei diritti di proprietà industriale *online*, si garantisca il coordinamento con la tutela del diritto d'autore *online* (con particolare riferimento all'Articolo 17 della nuova Direttiva CDSM) e si assicuri il giusto equilibrio con la libertà di espressione, la libertà di concorrenza ed il principio di libera circolazione nel mercato interno.

Ambito soggettivo dei *trusted flaggers*

Dato il ruolo che i segnalatori attendibili sono chiamati a svolgere nel DSA, è opportuno definire criteri chiari, oggettivi e stringenti al fine di circoscrivere attentamente il perimetro dei soggetti che ambiscono a conseguire tale status. Al contempo, potrebbe essere considerata l'inclusione dei titolari di diritti di proprietà industriale dal novero dei *trusted flaggers* in presenza di specifiche circostanze.

Good samaritan clause

Ai fini di una maggiore operatività della previsione che estende il beneficio dell'esenzione da responsabilità alle ipotesi in cui gli intermediari intraprendano volontariamente misure proattive tese ad accrescere il loro livello di conoscenza sulle condotte illecite perpetrate sulle loro piattaforme, sarebbe opportuno che la *good samaritan clause* specificasse in maniera più precisa le azioni volontarie da non disincentivare (*e.g.* termini e condizioni più stringenti, azioni investigative volte allo

specifico scopo di identificare e rimuovere contenuti illeciti, ad es. ove l'illiceità sia già stata in precedenza accertata), accompagnando tale elencazione alla indicazione di misure di salvaguardia come – ad esempio- la supervisione umana in caso di controlli algoritmici. Appare necessario, infatti, favorire azioni significative da parte del fornitore di servizi, da un lato, e circoscrivere la portata della clausola e/o inserire eventuali ulteriori garanzie per prevenire abusi nei confronti degli utenti delle piattaforme, dall'altro lato.

Obblighi di *compliance*

Al fine di evitare obblighi sproporzionati di *compliance* in capo alle imprese che gestiscono servizi di intermediazione, assicurando al contempo la finalità di contrasto all'illegalità *online* secondo un approccio basato sul rischio, la formulazione di alcune disposizioni potrebbe essere rimeditata. In particolare, l'Articolo 21 della proposta del DSA (che prevede la comunicazione da parte della piattaforma online in caso di sospetto di commissione di un reato grave che comporta una minaccia per la vita o la sicurezza delle persone) necessita di una definizione più precisa della portata dell'obbligo gravante sulle piattaforme.

Nella medesima ottica, sarebbe opportuno specificare meglio portata soggettiva e contenuto degli obblighi di informazione e verifica nell'ambito delle norme sulla tracciabilità degli operatori commerciali (KYBC), anche attraverso la promozione di standard e codici di condotta, seppur mantenedo inalterata la *ratio* della norma dato l'evidente impatto positivo su consumatori e titolari dei diritti. Si segnala, peraltro, come possa essere ragionevole una estensione dell'ambito soggettivo delle disposizioni KYBC anche oltre gli *online marketplaces*, tenendo in considerazione i servizi dove più frequentemente sono perpetrate condotte illecite. Inoltre, l'esclusione delle micro e delle piccole imprese dagli obblighi previsti per le piattaforme *online* potrebbe essere rimeditata. Potrebbe essere opportuno mantenere tale esclusione per obblighi che di fatto impongano oneri sproporzionati di *compliance* che non sono ragionevolmente esigibili da imprese di siffatte dimensioni, mentre ridimensionarla rispetto ad altri obblighi (come, ad esempio, l'obbligo di tracciabilità ai sensi dell'Art.22), considerando la finalità perseguita dal DSA di contrasto all'illegalità *online* specialmente per quanto riguarda le attività di contraffazione.

Necessità di coordinamento con altri plessi normativi a livello europeo e nazionale

A fronte dei diversi plessi normativi in vigore o in via di approvazione incidenti sui servizi digitali, si segnala in generale l'opportunità di un maggior coordinamento della disciplina orizzontle del DSA con altre fonti settoriali interferenti (ad esempio, proposta "Digital Markets Act", "Direttiva sui Servizi Media Audiovisivi", nuova Direttiva Diritto d'Autore nel Mercato Unico Digitale, Regolamento 2019/1150 "*Platform to Business*"), al fine di assicurare un quadro di riferimento preciso, non aggravare eccessivamente la *compliance* normativa delle imprese e non creare frammentazione ed incertezza giuridica circa l'ambito di applicazione delle diverse normative. In questo senso, un aspetto molto rilevante è la definizione dell'ambito soggettivo di applicabilità delle nuove norme. Infatti, si rileva come le definizioni dei prestatori dei servizi intermediari adottate dalla Proposta DSA non coincidano con le definizioni contenute in altri strumenti normativi, in particolare: (i) il Regolamento P2B è

applicabile ai "servizi di intermediazione online"; (ii) l'Art. 17 della Direttiva CDSM disciplina la responsabilità dei "prestatori di servizi di condivisione di contenuti online" per l'utilizzo di contenuti protetti dal diritto d'autore; (iii) la Direttiva SMAV impone determinati obblighi per i "servizio di piattaforma per la condivisione di video"; (iv) la proposta di DMA si applica ai "servizi di piattaforma di base forniti o offerti dai gatekeeper", ovvero un soggetto che "ha un impatto significativo sul mercato interno; gestisce un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali; detiene una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro".

Allo stesso modo, si è già sottolineata la necessità di coordinamento del DSA con la tutela *online* del diritto d'autore prevista dall'Art. 17 Direttiva CDSM e dalle disposizioni nazionali rilevanti in merito (ad esempio, il Regolamento AGCOM in Materia di Tutela del Diritto d'autore sulle reti di Comunicazione Elettronica e Procedure Attuative ai sensi del Decreto Legislativo 9 Aprile 2003, N. 70 (come da ultimo modificato dalla Delibera n. 233/21/CONS).

Infine, nella formulazione di alcuni obblighi specifici potrebbe essere utile adottare la tecnica normativa seguita da altre disposizioni contenute in fonti normative dirette a contrastare condotte illecite perpetrate *online*. Ad esempio, l'art. 21 della proposta DSA (che prevede la comunicazione da parte della piattaforma online in caso di sospetto di commissione di un reato grave che comporta una minaccia per la vita o la sicurezza delle persone) dovrebbe circoscrivere con maggiore precisione la portata degli obblighi di comunicazione, in modo simile alla tecnica usata dall'Art. 14.5 del Regolamento (UE) 2021/784 del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici *online*.

Autorità competenti per l'*enforcement* del DSA

Una questione ancora aperta è rappresentata dall'attribuzione a livello eurounitario e nazionale di competenze per l'*enforcement* del DSA. Al momento la proposta DSA non fornisce indicazioni sui soggetti chiamati a ricoprire il ruolo di autorità competenti per l'applicazione e l'esecuzione del DSA in ambito nazionale, lasciando la relativa designazione agli Stati Membri (Capo IV, sez. I DSA).

In particolare, gli Stati Membri dovranno designare una delle autorità competenti come "coordinatore dei servizi digitali" (Art. 38). Rispetto a tale scelta si possono ipotizzare diverse soluzioni, quali ad esempio la creazione di una nuova Autorità *ad hoc*, oppure l'attribuzione di tale ruolo ad una delle autorità esistenti nell'ordinamento interno. Nel dibattito nazionale si segnala il documento finale approvato dalla IX Commissione (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati sulla proposta DSA. Nell'esprimere una valutazione favorevole sulla proposta, la Commissione osserva come risulti "opportuna una precisazione circa l'assetto delle competenze di applicazione del regolamento, con particolare riguardo al coordinamento tra autorità nazionali, *Digital services coordinator* e Commissione europea, in particolare con riferimento al regime di supervisione e ai poteri di *enforcement* nei confronti delle piattaforme *on line* molto grandi; circa la concreta applicazione del regolamento sul piano nazionale, appare opportuno indicare l'Autorità per le

garanzie nelle comunicazioni quale organismo di diritto interno più idoneo a svolgere le funzioni di *Digital services coordinator*".

A tal proposito si ricorda che ad AGCOM sono già attribuite una serie di competenze per l'*enforcement* di altre normative sui servizi digitali interferenti con il DSA. In particolare, la legge 30 dicembre 2020, n. 178 (legge di Bilancio 2021) designa AGCOM per l'attuazone del Regolamento (UE) 2019/1150 (Platform to Business), mentre il Decreto legislativo di attuazione della direttiva (UE) 2019/790 (Diritto d'autore nel mercato Unico Digitale) estende le competenze dell'Autorità nell'ambito della tutela del diritto d'autore *online* (in aggiunta alle competenze già attribuite dall'art. 182-bis L. 633/1941, Art.32-bis TUSMAR, D.Lgs 70/2003). Ulteriori competenze sono attribuite dal Decreto Legislativo di Attuazione della direttiva (UE) 2018/1808 (Direttiva servizi di media audiovisivi).

Infine, nelle more della discussione interistituzionale sul testo finale del DSA non può essere esclusa l'ipotesi di una competenza esclusiva della Commissione con riferimento all'*enforcement* nei confronti di alcune categorie di piattaforme. In particolare, parallelamente alla competenza esclusiva della Commissione nei confronti dei "*gatekeepers*" soggetti al DMA, alla Commissione potrebbe essere attribuito lo stesso ruolo nei confronti delle piattaforme di dimensioni molto grandi ("VLOP") ai sensi del DSA.

Considerate l'incertezza ancora esistente sull'assetto delle competenze di applicazione del Regolamento e la tendenza all'accentramento delle competenze di *enforcement* in capo al coordinatore nazionale ed eventualmente persino alla Commissione europea, in ragione delle dimensioni e del ruolo delle piattaforme coinvolte, allo stato di avanzamento dell'*iter* di approvazione della proposta è prematuro ipotizzare eventuali forme di coordinamento con altre autorità competenti che potrebbero essere designate a livello interno. Pertanto, l'eventuale ripartizione di competenze andrà esaminata a valle delle soluzioni finali adottate dal DSA.

Infine, si segnala che gli Artt. 8 e 9 del DSA potrebbero avere un impatto sull'ordinamento nazionale, in quanto tali disposizioni prevedono per le autorità giudiziarie o amministrative nazionali il potere di imporre ordini di contrasto ai contenuti illegali e di fornire informazioni nei confronti dei prestatori di servizi intermediari. Il DSA chiarisce che tali ordini potrebbero avere effetto oltre il territorio dello Stato membro dell'autorità in questione.

Coordinatrice Scientifica
Prof.ssa Maria Isabella Leone

Prof. Giuseppe Colangelo
Prof. Antonio Gullo
Dott.ssa Silvia Scalzini

Luiss
Business
School

Villa Blanc
Via Nomentana 216
00162 Roma
T +39 06 852251
businessschool@luiss.it