Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 - Fascicolo n. 1/2025

La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso *Telegram* al Digital Services Act

Anna Vicinanza*

SOMMARIO: 1. Introduzione: il caso *Telegram* e il Digital Services Act. – 2. Dagli Stati Uniti all'Unione europea: la tradizionale immunità degli intermediari digitali per i contenuti dei terzi. – 3. Il Digital Services Act: verso una maggiore responsabilizzazione delle piattaforme digitali. – 4. Responsabilità e obblighi di Telegram nei confronti dei contenuti illegali.

1. *Introduzione: il caso* Telegram *e il Digital Services Act*

Il recente arresto in Francia del proprietario di Telegram, Pavel Durov, per sospetta complicità in attività illegali, quali pedopornografia e traffico di esseri umani, nonché per la mancata collaborazione con le autorità giudiziarie francesi[1], ha suscitato reazioni contrastanti. Da un lato, vi è l'indignazione di chi considera Telegram come un baluardo della libertà di espressione e l'arresto come un tentativo di censura; dall'altro, la soddisfazione di chi spera nella fine di questa zona franca

* Dottoranda in Diritto Europeo presso l'Università di Bologna.
[1] L'insieme dei capi per cui si procede sono stati resi pubblici da un comunicato stampa emesso dalla Procura della repubblica presso il Tribunale di Parigi il 26 agosto 2024, consultabile al seguente indirizzo web: www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf.

di internet[2]. Queste reazioni riflettono la classica tensione tra la protezione della libertà di espressione e le esigenze di contrasto alle attività illegali, una questione centrale nel dibattito sulla regolazione di internet e, più in generale, dei mezzi di comunicazione di massa.

La posizione di Telegram è particolarmente esemplificativa di questa tensione. Infatti, questo servizio di messagistica facilmente accessibile a tutti tramite browser o applicazione possiede alcune caratteristiche che ne fanno al contempo un prezioso mezzo di diffusione di informazioni e un agevolatore di attività illegali. Queste caratteristiche sono: l'esistenza di gruppi a cui possono partecipare un elevato numero di utenti (fino a 200.000 contro, ad esempio, i circa 1.000 di WhatsApp), la semplicità nel trovare i gruppi mediante una funzione di ricerca per parole chiave, la possibilità di criptare i messaggi e l'assenza quasi totale di collaborazione con le autorità giudiziarie e amministrative[3]. Il potenziale di diffusione dei gruppi aperti, unito alle garanzie di anonimato, permettono una più libera circolazione di informazioni, specialmente in contesti autoritari (ad esempio, fin dalle sue origini, Telegram ha respinto richieste di accesso ai dati provenienti del regime russo)[4]. Tuttavia, le medesime funzionalità facilitano l'accesso ad attività illegali, rendendo alla portata di tutti trovare un gruppo che venda armi, droga o condivida contenuti a sfondo sessuale non consensuali o rappresentanti minorenni[5].

Si noti come Telegram, fornendo un servizio di intermediazione digitale, costituisca solo uno strumento di condivisione di contenuti tra gli utenti; e non sia all'origine di alcuno di questi. In questo senso, il suo uso per diffondere contenuti illegali o per esercitare diritti democratici dipende esclusivamente dalla volontà dei suoi utenti. Sulla

[2] D. LELOUP, *Arrestation de Pavel Durov en France: le récit d'une semaine retentissante*, in *Le Monde*, 2024.
[3] P. MOZUR ET AL., *How Telegram Became a Playground for Criminals, Extremists and Terrorists*, in *The New York Times*, 2024 (www.nytimes.com/2024/09/07/technology/telegram-crime-terrorism.html).
[4] *Ibidem*.
[5] Ad esempio, in Italia, dopo un episodio di cronaca relativo ad una violenza sessuale di gruppo, si sono moltiplicate le ricerche ed i gruppi Telegram volti ad ottenere il video della violenza. Tra i molti che riportano la notizia: E. NICOLOSI, *Stupro Palermo, le chat della vergogna: su Telegram scattata la caccia al video della violenza*, in *La Repubblica*, 2023.

scia di questo ragionamento, l'account ufficiale di Telegram ha dichiarato su X (Twitter) successivamente all'arresto di Pavel Durov: «È assurdo sostenere che una piattaforma o il suo proprietario siano responsabili per l'abuso della stessa piattaforma»[6].

Per verificare la fondatezza di questa affermazione è tuttavia necessaria un'analisi più approfondita. Nonostante l'arresto di Pavel Durov sia basato sul diritto penale francese, è utile analizzare la posizione di Telegram alla luce delle regole europee sulla responsabilità delle piattaforme. In particolare, verranno esaminate le disposizioni rilevanti del recente Digital Services Act ("DSA")[7], in quanto tra gli obiettivi di questo regolamento troviamo proprio la volontà di combattere l'esistenza di zone franche online (secondo le parole di Ursula Von der Leyen «what is illegal offline, should be illegal online»[8]) e bilanciare diritti fondamentali e sicurezza[9].

Prima di procedere all'analisi normativa, è bene fare alcune precisazioni di natura terminologica, in quanto la disciplina europea dei fornitori di servizi internet (*internet services providers* o «ISPs») varia a seconda della tipologia di servizio informatico prestato. Dato che le classificazioni utilizzate sono di natura tecnica e non immediatamente intuibili, si è tentato di schematizzarle mediante un diagramma a centri concentrici per una più agevole comprensione (Figura 1).

---

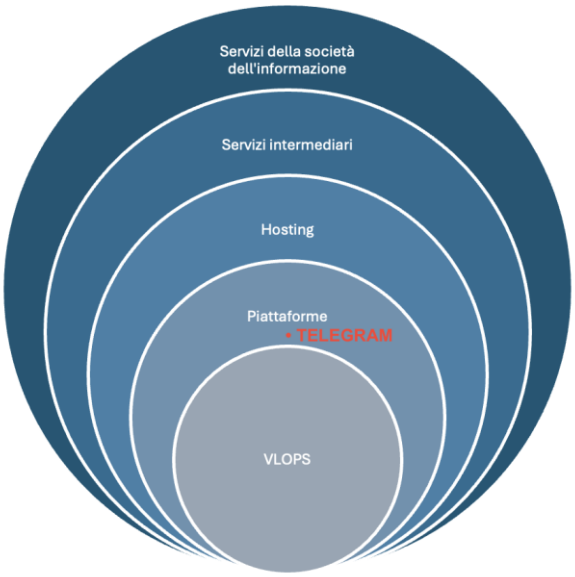
[6] Il post è disponibile su X al seguente link: www.x.com/telegram/status/1827787345367834772.

[7] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), PE/30/2022/REV/1.

[8] V. comunicato stampa della Commissione europea, del 23 aprile 2022: *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment*(www.ec.europa.eu/commission/presscorner/detail/en/ip_22_2545).

[9] Il considerando n. 9 del Digital Services Act afferma che l'obiettivo del regolamento è la creazione di un ambiente online sicuro, in cui siano tutelati i diritti fondamentali e sia promossa l'innovazione, il tutto contrastando la diffusione di contenuti illegali e dannosi.

Figura 1. Le categorie di fornitori di servizi internet secondo la regolamentazione europea e la classificazione di Telegram



L'insieme più ampio si riferisce alla macrocategoria degli *internet services providers*, la cui denominazione normativa è generalmente quella di «servizi della società dell'informazione»[10]. Un sotto-insieme di questi è rappresentato dai «fornitori di servizi intermediari» o, semplicemente, «intermediari»[11]. A loro volta questi si dividono in tre tipologie: servizi di «mere conduit», di «caching» e di «hosting»[12]. Tra i fornitori di servizi di *hosting*, ossia di memorizzazione di informazioni, vi sono i servizi di «piattaforma» o, più semplicemente, le «piattaforme digitali». Rispetto alla generalità dei servizi di *hosting*, le piattaforme si caratterizzano in quanto la loro funzione principale è

[10] I servizi della società dell'informazione sono definiti dalla direttiva 98/34/CE, così come modificata dalla direttiva 98/48/CE, come: «servizi forniti a distanza, mediante apparecchiature elettroniche, per l'elaborazione e l'archiviazione di dati e su richiesta individuale di un destinatario». Secondo il diciottesimo considerando, tale definizione «include i servizi non remunerati, nella misura in cui costituiscono un'attività economica, quali gli strumenti che consentono la ricerca e l'accesso ai dati o la trasmissione di informazioni attraverso una rete di comunicazione». È a questi soggetti che si applica la direttiva sul commercio elettronico (v. *infra*)

[11] A questi si applica la sezione 4 della direttiva sul commercio elettronico e il DSA (v. pag. 4).

[12] Così come definiti in precedenza dagli artt. 12, 13 e 14 della direttiva sul commercio elettronico e, adesso, dagli artt. 4, 5 e 6 del DSA.

di consentire la diffusione di contenuti al pubblico[13]. Il preambolo del DSA precisa che, alla luce di questo criterio distintivo, i servizi di messaggistica non sono inclusi nella definizione di piattaforme, salvo per ciò che concerne i gruppi pubblici o i canali aperti[14]. Infine, il DSA ha introdotto una nuova categoria di piattaforme definite secondo dei requisiti dimensionali, ossia le «Piattaforme online di dimensioni molto grandi» o, secondo l'acronimo inglese, «VLOPs»[15]. Ne consegue che tutte le piattaforme digitali rientrano anche nella definizione di *hosting*, di intermediari e di ISPs, ma solo alcune sono classificate ulteriormente quali VLOPs[16].

Telegram, fornendo un servizio di messaggistica, è sicuramente qualificabile quale *hosting provider*[17]. Inoltre, può essere classificabile come piattaforma, precisamente nella misura in cui permette la diffusione di informazioni al pubblico sia mediante gruppi pubblici che mediante canali aperti[18]. Non rientra invece nella categoria VLOP, in quanto la Commissione europea non lo ha per ora designato come tale (v. *infra*, p. 13).

Al fine di comprendere meglio l'attuale quadro in materia di responsabilità delle piattaforme per i contenuti illegali, si illustrerà brevemente la sua genesi storica (par. 2), per poi descrivere le principali novità addotte dal DSA (par. 3). Infine, si analizzerà la posizione di Telegram in base alle norme attualmente vigenti (par. 4).

2. *Dagli Stati Uniti all'Unione europea: la tradizionale immunità degli intermediari digitali per i contenuti dei terzi*

[13] Definite dall'art. 1 lett. (i) del DSA come servizi di memorizzazione di informazioni che diffondono, su richiesta del destinatario, informazioni al pubblico.
[14] Considerando n. 14 del DSA.
[15] V. nota n. 42.
[16] La disciplina europea degli ISPs prevede ulteriori categorizzazioni, ma si è scelto di soffermarsi su quelle più pertinenti alla questione in esame.
[17] J. VAN HOBOKEN ET AL., *Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report*, Publications Office of the European Union, 2019, p. 12.
[18] I primi permettono l'iscrizione a massimo 200.000 persone, tutte abilitate alla pubblicazione (www.telegram.org/tour/groups/it?ln=a); i secondi invece ad un numero indeterminato di persone, ma solo gli amministratori del canale possono pubblicare contenuti (www.telegram.org/faq_channels/it).

La tradizionale regolamentazione occidentale degli intermediari digitali prevede una generale immunità in favore di questi per i contenuti trasmessi per conto di terzi. Questa soluzione, adottata negli Stati Uniti, nell'Unione europea, e in molti altri ordinamenti, adotta una prospettiva favorevole alla libertà di espressione mediante la creazione di c.d. *safe harbour*[19].

La normativa statunitense si basa sulla Sezione 230 del Telecommunication Decency Act del 1996, che si articola in due principi fondamentali. Anzitutto, i fornitori di un servizio informatico interattivo[20] non devono essere considerati come editori («publisher») o diffusori («speaker») di informazioni fornite da altri. In secondo luogo, si esclude la responsabilità civile[21] del fornitore che intraprenda in buona fede azioni volontarie per limitare l'accesso a materiale osceno, indecente, lascivo, turpe, eccessivamente violento, molesto, o in altro modo deplorevole («objectionable»). Dunque, la prima parte della Sezione 230 esclude che i fornitori di servizi informatici interattivi possano incorrere in una responsabilità primaria (come autore o *speaker*) o secondaria (come editore)[22] per i contenuti forniti da terzi; mentre la seconda parte (c.d. «Protezione del Buon Samaritano») rafforza la loro immunità, che permane anche qualora il fornitore eserciti una forma di controllo sui contenuti mediante attività di moderazione. L'obiettivo di queste norme era favorire lo sviluppo di Internet come spazio libero e aperto[23], in cui ognuno potesse

[19] G. SARTOR, *The secondary liability of online intermediaries*, in E. BROGI, P. L. PARCU (eds.), *Research Handbook on EU Media Law and Policy*, Cheltenham, 2022, p. 3.

[20] Come si può notare la normativa statunitense non adotta la stessa terminologia di quella europea. Tuttavia, la nozione di "servizio interattivo" rimanda alla possibilità per i destinatari del servizio di caricare i propri contenuti e ciò rappresenta la caratteristica principale dei servizi di intermediazione digitale.

[21] La Sezione 230 non si applica in ambito penale e della proprietà intellettuale (quest'ultimo regolato dal Digital Millennium Copyright Act in maniera più simile a quanto avviene nell'UE, v. G. SARTOR, *op. cit.*, p. 152). Al contrario, come si vedrà in seguito, l'immunità prevista dal diritto UE si applica a qualsiasi tipo di responsabilità.

[22] A. BERTOLINI ET AL., *Liability of online platforms* (fasc. PE 656.318), European Parliamentary Research Service, 2021, p. 26.

[23] F. PASQUALE, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, in *University of Maryland Francis King Carey School of Law*, n. 24, 2016, p. 494.

condividere contenuti, consentendo al contempo ai fornitori dei servizi informatici di intervenire responsabilmente per limitare l'accesso pubblico ai contenuti più problematici, in una prospettiva di auto-regolazione[24]. L'immunità era inoltre motivata dai dubbi circa la fattibilità tecnica di un controllo pervasivo sui contenuti, considerato che i rischi di fallimento a questo riguardo avrebbero potuto scoraggiare l'ingresso di attori economici nel mercato e frenare l'innovazione[25].

Diversa è la disciplina introdotta nell'Unione europea dalla direttiva sul Commercio Elettronico («ECD») del 2001[26]: questa, pur avendo istituito una forma di immunità, ne ha definito i contorni in maniera differente. Le norme sulla responsabilità degli intermediari digitali sono contenute all'interno della sezione 4 della direttiva, che si applica solo a quei servizi della società dell'informazione classificabili come «intermediari». Il considerando n. 42 della direttiva precisa che l'attività intermediaria è di ordine «meramente tecnico, automatico e passivo», il che significa che il fornitore non conosce né controlla le informazioni trasmesse[27].

---

[24] G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022, p. 42.

[25] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, London, 2018, p. 32.

[26] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico").

[27] Emerge così la delicata questione della definizione del carattere «passivo» o «neutro» dell'attività di intermediazione, che costituisce il presupposto all'applicazione delle regole di esenzione della responsabilità. Essa è analizzata in: A. Bertolini et al., *op. cit.*, p. 29; J. Van Hoboken et al., *op. cit.*, p. 31; M. Maroni, E. Brogi, *Freedom of expression and the rule of law: the debate in the context of online platform regulation*, in E. Brogi, P. L. Parcu (eds.) *op. cit.*, p. 184, Inoltre, la qualifica di intermediario è stato oggetto di diverse pronunce della Corte di giustizia, in particolare rispetto alla qualificazione dell'attività di prioritizzazione dei contenuti effettuata da alcune piattaforme online (e.g. Corte giust. 23 marzo 2010, C-236/08 a C-238/08, *Google France*; 12 luglio 2011, C-324/09, *L'Oréal e a.*). Si noti, tuttavia, che non tutti sono concordi sull'applicabilità del considerando n. 42 anche agli intermediari di tipo "hosting" (v. conclusioni dell'Avv. gen. Jääskinen, del 9 dicembre 2010, C-324/09, *L'Oréal e a.*, punti 130-168). Tale tematica, seppure di notevole importanza per quanto riguarda l'attuale panorama delle piattaforme, non sarà ulteriormente approfondita in quanto estranea alla vicenda di Telegram che ci occupa.

Il regime di responsabilità degli intermediari di tipo *hosting* nell'ordinamento UE prima dell'entrata in vigore del DSA può essere così riassunto: *(A)* questi non sono responsabili per i contenuti illegali trasmessi dagli utenti salvo il caso in cui ne vengano a conoscenza, spontaneamente o su segnalazione, e non si attivino[28]; *(B)* gli Stati membri non possono imporre obblighi generali di sorveglianza sulle attività illegali degli utenti, ma possono emettere ordini di inibire specifici contenuti o di fornire determinate informazioni relative ad attività illecite.

Per quanto riguarda il punto *(A),* ossia le condizioni di immunità, esse variano a seconda della tipologia di servizio intermediario prestato, ossia di *mere conduit* (art. 12 ECD), *caching* (art. 13) o *hosting* (art. 14). Dato che Telegram e le piattaforme digitali rientrano nell'ultima categoria[29], l'analisi si concentra sull'articolo 14 della direttiva. In particolare, l'esenzione di responsabilità degli *hosting providers* è condizionata al fatto che essi *(i)* non siano al corrente del fatto che l'attività o l'informazione in questione sia illecita e – per quanto attiene ad azioni risarcitorie – non siano al corrente di fatti o circostanze che rendano manifesta l'illegalità; e, *(ii)* non appena al corrente di tale illegalità, agiscano immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. A questo punto si possono notare diverse differenze con il regime di immunità previsto dal diritto statunitense: nell'ordinamento dell'Unione non solo l'ambito di applicazione dell'immunità è definito in maniera più stringente (si applica solo agli intermediari) ma, inoltre, prevede alcune eccezioni (*i.e.*, la conoscenza dell'illegalità). Per questo motivo, l'immunità europea è stata definita *condizionata*[30].

Relativamente al punto *(B)*, il divieto di imporre agli intermediari un generale obbligo di monitoraggio sulle informazioni trasmesse o memorizzate, e/o di ricercare attivamente fatti o circostanze illecite, è sancito dall'articolo 15. D'altro canto, invece, il terzo paragrafo

[28] G. MORGESE, *Proposta di Digital Services Act e rimozione dei contenuti illegali online*, in P. MANZINI, G. CONTALDI, G. CAGGIANO (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, p. 32.
[29] V. nota n. 18.
[30] R. MACKINNON ET AL., *Fostering Freedom Online: The Role of Internet Intermediaries*, Paris, 2015, p. 50.

dell'articolo 14 menziona la possibilità, per un organo giurisdizionale o un'autorità amministrativa, di esigere che il fornitore ponga fine ad un'attività illecita o la impedisca, in conformità agli ordinamenti giuridici degli Stati membri[31]. Ne consegue che gli intermediari non hanno un generale obbligo di sorveglianza sui contenuti trasmessi per conto di terzi, ma possono essere obbligati ad agire nei confronti di contenuti specificatamente individuati dalle autorità nazionali competenti. Inoltre, il paragrafo successivo precisa che gli Stati membri possono di stabilire in capo ai fornitori un obbligo di informazione relativamente a presunte attività illecite dei propri utenti (qualora ne vengano a conoscenza) o di comunicare, a richiesta, informazioni che consentano l'identificazione di determinati utenti.

La possibilità per le autorità nazionali di emettere ordini di rimozione di determinati contenuti illegali è stata oggetto di alcune pronunce da parte della Corte di giustizia. Questa, oltre a definire i confini tra ordini di rimozione specifici (autorizzati) e obblighi generalizzati di sorveglianza (vietati)[32], si è altresì pronunciata sul legame intercorrente tra ricezione di un ordine di rimozione e conoscenza del contenuto illegale. Essa sottolinea come un ordine di rimozione di un contenuto illegale indirizzato ad un fornitore possa condurre a ritenere quest'ultimo consapevole dell'illegalità in questione, comportando una perdita dell'immunità ai sensi dell'art. 14 ECD[33]. Dalla giurisprudenza non emerge, tuttavia, un automatismo tra ordine di rimozione e conoscenza dell'illegalità, che andrà valutata dal giudice nazionale caso per caso[34]. Al riguardo la Corte precisa nella sentenza *L'Oréal*: «[…] pur se, certamente, una notifica non può automaticamente far venire meno il beneficio dell'esonero dalla responsabilità previsto all'art. 14 della direttiva 2000/31 – stante il fatto

[31] Il considerando n. 45 recita: "Le limitazioni alla responsabilità dei prestatori intermedi previste nella presente direttiva lasciano impregiudicata la possibilità di azioni inibitorie di altro tipo. Siffatte azioni inibitorie possono, in particolare, essere ordinanze di organi giurisdizionali o autorità amministrative che obbligano a porre fine a una violazione o impedirla, anche con la rimozione dell'informazione illecita o la disabilitazione dell'accesso alla medesima".

[32] Corte giust. 24 novembre 2011, C-70/10, *Scarlet Extended*; 16 febbraio 2012, C-360/10, *SABAM*; 3 ottobre 2019, C-18/18, *Glawischnig-Piesczek*.

[33] *L'Oréal e a.*, sopra citata, punti 120-124.

[34] J. VAN HOBOKEN ET AL., *op. cit.*, p. 39.

che notifiche relative ad attività o informazioni che si asseriscono illecite possono rivelarsi insufficientemente precise e dimostrate –, resta pur sempre fatto che essa costituisce, di norma, un elemento di cui il giudice nazionale deve tener conto per valutare, alla luce delle informazioni così trasmesse al gestore, l'effettività della conoscenza da parte di quest'ultimo di fatti o circostanze in base ai quali un operatore economico diligente avrebbe dovuto constatare l'illiceità»[35]. Se ne desume che, a seconda delle caratteristiche dell'ordine di rimozione e, in particolare, del suo carattere sufficientemente preciso e motivato, potrà aversi una perdita dell'immunità per il servizio di *hosting* coinvolto.

3. *Il Digital Services Act: verso una maggiore responsabilizzazione delle piattaforme digitali*

Nonostante l'evoluzione del web 2.0 abbia messo in discussione il regime di responsabilità degli intermediari digitali[36], il Digital Services Act ha mantenuto i principi generali del precedente quadro normativo[37].

Gli articoli 4, 5, 6 e 8 del DSA, infatti, sono sostanzialmente sovrapponibili agli articoli 12, 13, 14 e 15 della direttiva sul Commercio Elettronico[38]. Di conseguenza, tutti gli intermediari digitali continuano a beneficiare di un'immunità per i contenuti generati dagli utenti, a meno che non siano a conoscenza della loro illegalità o, una volta appresa, non intervengano per rimuoverli (articolo 6 DSA). Allo stesso modo, essi continuano a non incorrere in un obbligo generale di monitorare i contenuti trasmessi dagli utenti (articolo 8 DSA). Rappresenta, invece, una novità, la previsione esplicita di una «Protezione del buon samaritano»[39]. Inoltre, vi sono diverse

[35] *L'Oréal e a.*, sopra citata, punto 122.
[36] Soprattutto in ragione dell'emersione di giganti del web che intervengono ampiamente nella trasmissione dei contenuti (cfr. testi citati nella nota n. 28).
[37] G. MORGESE, *op. cit.*, p. 36.
[38] *Ivi*, p. 44.
[39] L'articolo 7 del DSA stabilisce che lo spontaneo esercizio dell'attività di moderazione, purché effettuato in buona fede e in maniera diligente, non incida di per sé sull'immunità (*cfr.* considerando n. 25). Si può tuttavia ritenere che si tratti di una novità solo formale, dato che tale principio era menzionato nel considerando n. 40 della direttiva sul commercio elettronico ed è stato richiamato nel ragionamento dell'avvocato generale nel caso *L'Oréal* (conclusioni dell'Avv. gen. Jääskinen, sopra

disposizioni che incidono in maniera significativa sulle responsabilità e gli obblighi degli intermediari nei confronti dei contenuti illegali. Tali disposizioni si articolano in tre categorie principali.

In primo luogo, il DSA contiene una disciplina comune per quanto riguarda gli ordini di rimozione dei contenuti e le richieste di informazioni emessi dalle autorità nazionali. Come già menzionato, la direttiva sul commercio elettronico si limitava a lasciare liberi gli Stati membri su questo punto. Invece, gli articolo 9 e 10 del DSA hanno stabilito i requisiti minimi affinché tali provvedimenti comportino un obbligo "di risposta" in capo agli intermediari digitali. In particolare, l'articolo 9 descrive le modalità di trasmissione di un ordine di rimozione emesso dalle autorità nazionali, nonché le informazioni che questo deve contenere per consentire l'identificazione del contenuto illegale e le relative motivazioni. Se l'ordine è conforme a questi requisiti, il destinatario sarà obbligato ad informare senza indebito ritardo le autorità competenti in merito al seguito che vi ha dato. I requisiti affinché una richiesta di informazione produca i medesimi effetti sono invece dettagliati dal successivo articolo 10. Si noti che, in entrambi i casi, l'obbligo che sorge in capo all'intermediario non è di agire in conformità all'ordine (*i.e.*, rimuovere il contenuto o fornire l'informazione), ma comunicare al più presto le azioni intraprese al riguardo. È lecito, quindi, chiedersi se il destinatario sia autorizzato a non adempiere all'ordine, purché spieghi le ragioni del suo comportamento.

Strettamente connessa al carattere prescrittivo degli ordini di cui agli artt. 9 e 10, è la questione della conoscenza dell'illegalità. Nonostante l'adozione di regole comuni, il DSA continua però a non chiarire se la trasmissione di un ordine conforme a queste regole comporti automaticamente la conoscenza dell'illegalità da parte dell'intermediario. Si può, quindi, ritenere applicabile lo stesso principio affermato dalla Corte di giustizia nel precitato caso *L'Oréal*, che richiede una valutazione caso per caso dell'effettiva conoscenza dell'illegalità da parte dell'intermediario. In quel contesto, la Corte

citate, parr. 130-168). Tuttavia, alcuni autori (J. VAN HOBOKEN ET AL., *op. cit.*, p. 7) hanno ritenuto che l'assenza di una disposizione esplicita in tal senso avesse creato un'incertezza giuridica nel diritto dell'Unione.

aveva affermato che l'effettiva conoscenza dell'illegalità andava valutata in particolare alla luce della precisione e della sufficiente motivazione dell'ordine in questione. Dato che l'art. 9 del DSA si preoccupa di definire i requisiti di precisione e motivazione affinché un ordine sia produttivo di effetti, appare ragionevole supporre che la trasmissione di un ordine conforme a questi requisiti implichi in linea generale una conoscenza dell'illegalità, con conseguente perdita dell'immunità. Tale interpretazione appare tanto più ragionevole se si considera ciò che dispone al riguardo l'articolo 16 del DSA (v. par. *infra*).

La seconda novità del DSA riguarda le disposizioni di cui agli articoli 16 e 18, applicabili esclusivamente agli *hosting providers* (incluse, quindi, le piattaforme online). L'articolo 16 impone a questi di predisporre un meccanismo c.d. di "segnalazione e azione" che permetta a tutti gli utenti di segnalare la presenza di contenuti illegali. Il medesimo articolo stabilisce espressamente che segnalazioni di tal tipo, se correttamente inoltrate, permettono di considerare che il prestatore di servizi abbia conoscenza dell'illegalità, con conseguente perdita dell'immunità. L'articolo 18, invece, stabilisce che il prestatore di servizi, qualora venga a conoscenza di informazioni che fanno sospettare la commissione di un reato, debba informare tempestivamente 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. Ciò significa che, pur in assenza di un obbligo generale di sorveglianza sui contenuti trasmessi dagli utenti, il rilevamento di un reato nell'ambito di attività di controllo volontarie, dà luogo a un obbligo giuridico di segnalazione alle autorità competenti. Dall'insieme di queste disposizioni emerge come, nonostante la riaffermazione del principio di irresponsabilità per i contenuti trasmessi per conto di terzi, il suo ambito di applicazione sia sempre più ristretto.

Infine, occorre richiamare una terza novità del DSA connessa alla responsabilità degli intermediari nei confronti di contenuti dannosi[40].

[40] Si utilizza in questo caso il più ampio termine "dannosi", piuttosto che "illegali", perché non tutti i rischi individuati dall'art. 34 DSA fanno riferimento a contenuti o attività strettamente illegali. Ad esempio, può considerarsi inclusa la disinformazione in quanto implicante effetti negativi sul dibattito civico (v. nota 46). La mancata

Essa è contenuta nelle disposizioni relative alle Piattaforme online di dimensioni molto grandi ("VLOP")[41], la cui supervisione è affidata alla Commissione. Gli articoli 34 e 35 impongono alle piattaforme designate come VLOP l'obbligo di effettuare una valutazione dei rischi sistemici generati dal loro utilizzo, e di adottare le misure necessarie per mitigarli. Tra i rischi sistemici individuati dal DSA, figurano la diffusione di contenuti illegali, gli effetti negativi sul dibattito civico, sui processi elettorali e sulla salute pubblica, la violenza di genere e la protezione dei minori[42], mentre tra le misure di mitigazione è citato l'*adeguamento* dei sistemi di moderazione[43]. Sebbene queste disposizioni siano formulate in termini generici, esse sembrano introdurre quantomeno un incentivo, se non un obbligo[44], ad una certa proattività nella moderazione dei contenuti al fine di mitigare alcuni tipi di rischi sistemici. Questa interpretazione appare confermata dall'apertura da parte della Commissione di un procedimento per violazione del DSA, e in particolare degli artt. 34 (1), 34 (2) e 35 (1), nei confronti di X (Twitter) per un'azione inadeguata nei confronti dei contenuti illegali e la disinformazione[45] e dalle richieste di informazioni inviate relativamente al taglio del personale dedicato alla moderazione[46]. Si noti, però, che in questo caso non si instaura una vera

distinzione tra contenuti "dannosi" e "illegali" all'interno del DSA è criticata da diversi autori (e.g., G. FROSIO, C. GEIGER, *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, in *European Law Journal*, nn. 1-2, 2021, pp. 31-77, spec. p. 42.

[41] Definite, assieme ai motori di ricerca di dimensioni molto grandi ("VLOSEs"), dall'articolo 33 DSA secondo dei requisiti dimensionali.

[42] Art. 34 (1).

[43] Art. 35 (1), lettera (c) DSA.

[44] Per una critica di questo approccio si veda ad esempio: N Helberger, *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power*, in *Digital Journalism*, 2020, pp. 842-854; G. FROSIO, C. GEIGER, *op. cit.*, p. 45.

[45] V. Commissione europea, DSA.100100 – X (formerly Twitter) – Investigation into compliance with articles 34 (1) and (2), 35 (1), 16 (5) and (6) of Regulation (EU) 2022/2065, 18.12.2023, C (2023) 9137final. Le stesse osservazioni possono essere effettuate relativamente alla lettera che il commissario Thierry Breton ha inviato a TikTok (ma anche X e Meta) relativamente ai contenuti a stampo terroristico dopo l'attacco di Hamas del 7 ottobre 2023 (www.x.com/ThierryBreton/status/1712472108222329056?lang=en).

[46] V. comunicato stampa della Commissione europea, del 8 maggio 2024, *Commission requests information from X on decreasing content moderation resources under the Digital Services Act* (www.digital-strategy.ec.europa.eu/en/news/commission-

e propria responsabilità (*liability*) per i contenuti dannosi diffusi sulla piattaforma, in quanto l'immunità rimane applicabile; ma si assiste piuttosto una responsabilizzazione (*accountability*)[47] nei confronti di questi contenuti, accompagnata un ruolo cruciale della Commissione nella definizione degli standard di diligenza richiesti[48].

Si noti che il DSA non pregiudica le norme precedentemente adottate in ambiti specifici, frutto anch'esse della tendenza ad una maggiore responsabilizzazione dei fornitori di servizi intermediari nei confronti di determinati contenuti illegali[49]. La direttiva sui servizi di media audiovisivi (AVMSD), adottata nel 2010 ed emendata nel 2018[50], contiene una serie di disposizioni rivolte ai Servizi di piattaforme di condivisione video (VSPS), creando doveri di diligenza per proteggere i minori e combattere il terrorismo, l'incitamento alla violenza e l'odio contro gruppi o individui. Tuttavia, non imponendo un controllo *ex ante* sulle informazioni trasmesse, queste disposizioni sono stati considerati coerenti con il divieto di obbligo generale di sorveglianza di cui all'art. 25 dell'ECD. La direttiva 2019/790 sul diritto d'autore[51] ha introdotto un meccanismo di responsabilità specifico per le violazioni dei diritti di proprietà intellettuale che si applica ai fornitori di servizi di condivisione di contenuti online[52]. Infine, ulteriori obblighi specifici

requests-information-x-decreasing-content-moderation-resources-under-digital-services).

[47] M. HUSOVEC, *Principles of the Digital Services Act*, Oxford Academic, 2024, p. 17.

[48] Il cui mancato rispetto può comportante l'irrogazione delle pesanti sanzioni pecuniarie di cui all'art. 74 DSA.

[49] G. MORGESE, *op. cit.*, p. 37; A. BERTOLINI ET AL., *op. cit.*, p. 36 ss.

[50] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), così come modificata dalla direttiva 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018.

[51] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[52] L'articolo 17 della direttiva prevede che le piattaforme debbano ottenere l'autorizzazione dei titolari dei diritti (ad esempio mediante un contratto di licenza) per rendere disponibili i contenuti protetti caricati dai loro utenti. In assenza di un'autorizzazione esplicita, le piattaforme saranno ritenute responsabili, a meno che non dimostrino di aver intrapreso tutte le attività necessarie ad evitare che tali materiali fossero resi disponibili. Il regolamento prevede anche una serie di contromisure: alle piattaforme viene chiesto di ridurre al minimo i rischi di filtraggio e di blocco eccessivo e di fornire meccanismi di reclamo contro la rimozione.

sono contemplati in materia di contrasto alla diffusione dei contenuti pedopornografici[53], e relativamente alla diffusione di contenuti terroristici[54].

4. *Responsabilità e obblighi di Telegram nei confronti dei contenuti illegali*

Alla luce delle disposizioni esaminate, è possibile effettuare almeno tre ordini di considerazioni in merito a responsabilità e doveri di Telegram rispetto alla diffusione dei contenuti illegali. Anzitutto, rientrando Telegram nella categoria di intermediario e, più precisamente *hosting provider*, la sua responsabilità è disciplinata attualmente dell'articolo 6 del DSA (prima art. 14 ECD). Per questo motivo, nonostante goda di una generale immunità per i contenuti illegali dei propri utenti, può essere ritenuto responsabile per questi qualora ne venga a conoscenza e non si adoperi per disattivarli. Per quanto riguarda la natura giuridica di tale responsabilità, la sua definizione rimane di competenza dei diritti nazionali, dato che l'Unione europea si è limitata ad armonizzare i casi di esenzione.

In secondo luogo, gli ordini di rimozione di contenuti illegali e le richieste di informazioni emessi dalle autorità nazionali competenti possono indurre a ritenere che l'intermediario digitale sia a conoscenza dell'illegalità, facendo dunque venire meno l'immunità. Lo stesso può accadere nel caso in cui un utente segnali un'illegalità mediante il meccanismo di "segnalazione e azione" che gli *hosting providers* sono obbligati ad attivare in conformità all'art. 18 del DSA. Ne consegue che, nel caso in cui Telegram abbia ricevuto richieste formali di disattivazione di determinati account e/o contenuti illegali, questi può tessere ritenuto consapevole e, quindi, responsabile per i medesimi

[53] Direttiva 2011/92/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.

[54] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online. Richiede agli *hosting providers* di adottare misure specifiche contro i contenuti legati al terrorismo e prevede l'obbligo di collaborare con le autorità nazionali del settore, a pena di sanzioni.

conformemente alle norme nazionali applicabili. Inoltre, non avere risposto a richieste di rimozione di contenuti o a richieste di informazioni trasmesse dalle autorità competenti conformemente al DSA può comportare l'applicazione delle sanzioni previste dal medesimo regolamento[55].

Infine, al momento Telegram non è stato designato come VLOP avendo dichiarato un numero di utenti attivi mensili di poco inferiore a 45 milioni[56]. Pur essendo probabile una prossima revisione di questo status[57], Telegram è attualmente esente dall'obbligo di valutare e mitigare i rischi sistemici generati dal suo utilizzo. Per questo motivo, al contrario di altri social media, Telegram è stato per ora al riparo da indagini da parte della Commissione. Peraltro, non essendo stato designato come VLOP, la sua conformità con le regole del DSA è vigilata dal coordinatore nazionale dei servizi digitali belga e non dalla Commissione. Un prossimo mutamento di status comporterebbe un obbligo di valutazione dei rischi sistemici e di adozione di misure di mitigazione, la cui effettività verrà valutata dalla Commissione. È possibile che questo richieda una significativa revisione del modello di business di Telegram che, rispetto alle piattaforme online più diffuse, conta pochissimo personale, e prevalentemente composto da sviluppatori[58], nonché un adeguamento di alcune sue funzionalità ritenute pericolose, quali la gestione dei gruppi aperti.

[55] In questo senso, il recente impegno di Telegram a collaborare con le richieste delle autorità giudiziarie nazionali (L. JAMALI, *Telegram will now provide some user data to authorities*, in *BBC*, 2024 – www.bbc.com/news/articles/cvglp0xny3eo.) costituisce l'adempimento di un obbligo derivante dal diritto europeo.

[56] È questa la principale soglia dimensionale richiesta dall'art. 33 del DSA. F. Y. CHEE, *Eu in touch with Telegram as it nears criterian for EU tech rules*, in *Reuters*, 2024 (www.reuters.com/technology/eu-touch-with-telegram-it-nears-criterion-eu-tech-rules-2024-05-28/).

[57] *Ibidem*.

[58] Secondo la già citata inchiesta di P. MOZUR ET AL., *op. cit.*, Telegram, con quasi un miliardo di utenti al mondo, ha solo 60 dipendenti, di cui la metà sono sviluppatori, e poche centinaia di moderatori, mentre Instagram, YouTube e TikTok hanno intere divisioni dedicate alla collaborazione con le autorità e migliaia di moderatori.

ABSTRACT (ITA)

L'analisi prende spunto dalla recente vicenda dell'arresto del fondatore di Telegram Pavel Durov per illustrare le principali responsabilità e obblighi delle piattaforme digitali in merito ai contenuti illegali diffusi dai propri utenti. Muovendo dalle prime regolamentazioni statunitensi ed europee in tema di immunità degli intermediari digitali per i contenuti illegali, si illustrano le principali novità introdotte in materia dal Digital Services Act. Questo, pur riaffermando il principio dell'immunità, contiene diverse disposizioni implicanti una maggiore responsabilizzazione degli intermediari. Sulla base delle norme esaminate, si traggono alcune conclusioni su obblighi e responsabilità di Telegram rispetto ai contenuti illegali e dannosi. Ne emerge come Telegram possa essere ritenuto responsabile per i contenti illegali di cui sia a conoscenza, anche in seguito a segnalazioni di autorità competenti o utenti, qualora non intervenga per rimuoverli. Inoltre, Telegram è tenuto a rispondere alle richieste di rimozione di contenuti o di fornire informazioni inoltrate dalle autorità nazionali conformemente al Digital Services Act, a pena di sanzioni. Tuttavia, non essendo stato designato quale VLOP, per ora Telegram non è soggetto ad un obbligo generale di contrasto ai contenuti illegali o dannosi (all'infuori di regolamentazioni settoriali e segnalazioni specifiche). Una futura designazione in tal senso potrebbe, invece, spingere la Commissione a richiedere alcuni adeguamenti in un'ottica di mitigazione dei rischi sistemici, ad esempio relativamente alla gestione dei gruppi pubblici o al potenziamento delle risorse dedicate alla moderazione.

ABSTRACT (ENG)

The analysis builds on the recent arrest of Telegram founder Pavel Durov to illustrate the main responsibilities and obligations of digital platforms regarding illegal content disseminated by their users. Building on early U.S. and European regulations on the immunity of digital intermediaries for illegal content, the main changes introduced in this regard by the Digital Services Act are outlined. The DSA reaffirms the principle of immunity, but contains provisions implying

increased accountability of intermediaries. Based on the analysis of certain DSA provisions, some conclusions are drawn about Telegram's obligations and responsibilities with respect to illegal and harmful content. First, Telegram can be held liable for illegal content of which it has knowledge, also as a consequence of reports transmitted by national competent authorities or users, unless it takes action to remove it. Secondly, Telegram is required to respond to requests to remove content or provide information forwarded by national authorities in accordance with the Digital Services Act, or it may be sanctioned. On the other side, as it has not been designated as a VLOP by the European Commission, Telegram is not currently subject to a general obligation to counter illegal or harmful content (outside of sector-specific regulations). A future designation as such could, however, prompt the EC to require certain adjustments under the systemic risks mitigation obligations, for instance regarding the functioning of public groups and resources dedicated to moderation.