amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Carlo Rizzo

FASCICOLO N. 4/2024

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009

ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudia, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini, Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Beatrice Coppa, Giuseppe Doria, Manuel Delgado Iribarren, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Giuseppina Lofaro, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Benedetta Piazza, Marcin Princ, Sara Pugliese, Bianca Nicla Romano, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Stefania Terracciano, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Disciplina sui servizi digitali erogati dai fornitori di piattaforme e motori di ricerca on line di dimensioni molto grandi e ruolo della Commissione europea

di Alessandro Chiappini

(Dottore di ricerca in diritto ed economia presso l'Università LUISS Guido Carli)

Sommario

1. Introduzione; 2. Oggetto ed ambito di applicazione del Regolamento europeo; 3. Obblighi a carico dei fornitori di piattaforme e motori di ricerca on line di dimensioni molto grandi; 4. Competenze e poteri della Commissione europea e diritti delle parti; 5. Conclusioni.

Abstract

The so-called digital service act was presented by the European Commission on 15 December 2020 as part of the package relating to the Digital Services Act together with the Digital Market Act, as announced in the communication of 19 February 2020 entitled "Shaping Europe's digital future" and in accordance with the strategy for the digital single market in Europe outlined in the communication of 6 May 2015. In the context of digital constitutionalism, the Regulation represents an expression of the digital sovereignty of the European Union which attempts to democratise the network by limiting the excessive power of platforms as private censors. After having identified the object and scope of application of the Regulation applicable from 17 February 2024, this contribution, after identifying the providers of platforms (infra VLOP) and very large online search engines (infra VLOSE), analyses the respective obligations characterised by an early application to 25 August 2023, also investigating the corresponding competence and powers of the European Commission.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review*

1. Introduzione.

Il cosiddetto *digital service act* è stato presentato dalla Commissione europea il 15 dicembre 2020 nell'ambito del pacchetto relativo alla legge sui servizi digitali insieme al *digital market act*[1], come preannunciato dalla comunicazione del 19 febbraio 2020 intitolata "*Plasmare il futuro digitale dell'Europa*" ed in conformità con la strategia per il mercato unico digitale in Europa delineata dalla comunicazione del 6 maggio 2015[2].

Nell'ambito del filone del costituzionalismo digitale[3], il Regolamento rappresenta espressione della sovranità digitale dell'Unione europea che tenta la democratizzazione della rete limitando lo strapotere delle piattaforme quali censori privati[4].

Dopo aver rilevato l'oggetto e l'ambito di applicazione del Regolamento applicabile dal 17 febbraio 2024, il presente contributo, previa individuazione dei fornitori di piattaforme (*infra* VLOP) e motori di ricerca *on line* di dimensioni molto grandi (*infra* VLOSE), analizza i rispettivi obblighi caratterizzati da un'applicazione anticipata al 25 agosto 2023, indagando altresì la corrispondente competenza ed i poteri della Commissione europea.

---

[1] Sul *digital market act* si veda il dossier n. 52 del 18 maggio 2021 dell'ufficio rapporti con l'Unione europea della Camera dei deputati; sull'argomento si confronti anche A. DE STREEL, P. LAROUCHE, *The European Digital Markets Act proposal: How to improve a regulatory revolution*, in "Concurrences", 2021, n. 2, p. 46-63.

[2] La proposta della Commissione europea, che era stata anticipata da tre risoluzioni del Parlamento europeo del 20 ottobre 2020 (P9_TA(2020)0272; P9_TA(2020)0273 e P9_TA(2020)0274), è confluita nel 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 (*infra* Regolamento), pubblicato nella Gazzetta Ufficiale dell'Unione europea del 27 ottobre 2022 ed entrato in vigore il 16 novembre 2022. Al riguardo, si veda G. M. RUOTOLO, *Le proposte di disciplina di digital services e digital markets della Commissione del 15 dicembre 2020*, in DPCE on line, 2020, p. 5419 ss.; L. WOOD, *Overview of Digital Services Act*, in EU Law Analysis, 16 dicembre 2020; BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS, *The Digital Services Act Proposal - BEUC position paper*, 2021; F. ERIXON, *"Too Big to Care" or "Too Big to Share": The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules*, ECIPE Policy Brief n. 5/2021; G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in I Post di AISDUE, III (2021), aisdue.eu, Focus "Servizi e piattaforme digitali", n. 1, 18 febbraio 2021; V. GOLUNOVA, *The Digital Services Act and Freedom of Expression: Triumph or Failure?*, 8 marzo 2021; A. SAVIN, *The EU Digital Services Act: Towards a More Responsible Internet*, Copenhagen Business School Law Research Paper Series No. 21-04; S. F. SCHWEMER, *Digital Services Act: A Reform of the e-Commerce Directive and Much More*, prepared for A Savin, Research Handbook on EU Internet Law, october 2022, p. 1 ss..

[3] Così L. GILL, D. REDEKE, U. GASSER, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, Berkman Center Research Publication No. 2015-15, 2015, che definivano il costituzionalismo digitale "*una costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di governance, e limitazioni all'esercizio del potere su Internet*". Si veda più di recente E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in International Review of Law, Computers & Technology, 2019, p. 81. In relazione a tale approccio da parte dell'Unione europea G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, in International Journal of Constitutional Law, 2020, vol. 19, issue 1, p. 41 ss.; dello stesso autore G. DE GREGORIO, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in Diritti Comparati, 17 maggio 2021; A. IANNOTTI DELLA VALLE, *Il Digital Markets Act e il ruolo dell'Unione Europea verso un costituzionalismo digitale*, in Giurisprudenza costituzionale, 2022, 1867 ss..

[4] Con riferimento alla sovranità digitale si veda tra gli altri M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, Polity Press, 2017; European Parliament, *Digital sovereignty for Europe*, luglio 2020.

2. *Oggetto ed ambito di applicazione del regolamento europeo.*

In base all'articolo 3 del Regolamento, s'intende per "*servizio della società dell'informazione*" un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535, che considera tale "*qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario*"[5].

Ebbene, il Regolamento in esame si applica ai prestatori di "*determinati*" servizi della società dell'informazione (Considerando 5); nello specifico, l'ambito di applicazione è costituito dai seguenti "*servizi intermediari*" (articoli 2 e 3):

- un servizio di semplice trasporto (*mere conduit*) diretto a trasmettere, su una rete di comunicazione, informazioni provenienti da un destinatario del servizio o a fornire accesso ad una rete di comunicazione[6];
- un servizio di memorizzazione temporanea (*caching*) diretto a trasmettere, su una rete di comunicazione, informazioni provenienti dal destinatario del servizio, che implica la memorizzazione automatica, intermedia e temporanea delle stesse con l'obiettivo di maggior efficienza nel successivo inoltro ad altri destinatari su loro richiesta[7];
- un servizio di memorizzazione di informazioni (*hosting*) diretto a memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso (c. d. *user generated content*)[8].

Ai fini dell'applicabilità del Regolamento, è necessario un collegamento sostanziale del prestatore di servizi intermediari con l'Unione europea[9]; sulla base di tale premessa, l'ambito di applicazione è costituito dai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari (articolo 2, paragrafo 1)[10]. Per destinatario del servizio s'intende "*qualsiasi persona fisica*

[5] Il riferimento è in particolare alla direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[6] Il Considerando 29 considera i punti di interscambio internet, i punti di accesso senza fili, le reti private virtuali, i risolutori e servizi di sistema dei nomi di dominio (*Domain Name System*), i registri dei nomi di dominio di primo livello, i *registrar*, le autorità di certificazione che rilasciano certificati digitali, il *Voice over Internet Protocol* (IP) e altri servizi di comunicazione interpersonale (servizi di posta elettronica e messaggistica basati sul web).

[7] Il Considerando 29 include la fornitura di reti per la diffusione di contenuti, *proxy* inversi o *proxy* di adattamento dei contenuti.

[8] Il Considerando 29 menziona categorie di servizi quali nuvola informatica (*cloud computing*), memorizzazione di informazioni di siti web (*web hosting*), servizi di referenziazione a pagamento o servizi che consentono la condivisione di informazioni e contenuti *on line*, compresa la condivisione e memorizzazione di file.

[9] Il Considerando 8 ritiene che il collegamento sostanziale con l'Unione europea sussista quando il prestatore di servizi intermediari è stabilito nel territorio europeo.

[10] Per A. MICHINELLI, *Digital Services Act: questioni tecnico-giuridiche ancora aperte sulla sua applicazione*, in Cybersecurity 360, 7 novembre 2022, l'obiettivo è "*Creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi digitali, oltre a creare condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello mondiale. A livello mondiale perché – similmente a quanto già tentato con il GDPR – si vuole ambire sia a regolamentare soggetti extra-UE/SEE sulla base del criterio dell'offerta di servizi*

ISSN 2036-7821

o giuridica che utilizza un servizio intermediario, in particolare per ricercare informazioni o renderle accessibili" (articolo 3), ritenendo tali gli utenti commerciali, i consumatori e gli altri utenti (Considerando 2).

Dopo aver inquadrato i servizi rilevanti, si rammenta che sono passati oltre venti anni dalla 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 (*infra* direttiva 2000/31/CE)[11].

E' utile sottolineare che nelle ultime decadi, anche a causa della trasformazione digitale, i predetti servizi costituiscono una componente significativa dell'economia dell'Unione europea e della vita quotidiana dei cittadini, generando nuovi rischi che i singoli Stati membri contrastano in modo divergente (Considerando 1 e 2) come emerge dal caso *Cambridge Analytica*[12].

Secondo i principi generali enunciati dal Trattato dell'Unione europea (*infra* TUE), nei settori che non sono di competenza esclusiva l'Unione europea interviene, sulla base del principio di sussidiarietà, laddove gli Stati membri non siano in grado di conseguire in modo sufficiente l'obiettivo (articolo 5 TUE).

Ciò premesso, ex articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea (*infra* TFUE) "*2. Il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni dei trattati*"; al fine di realizzare il predetto obiettivo, il successivo articolo 114 dispone che il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e

---

a destinatari/utenti ubicati nel territorio dell'Unione, sia a innalzare uno standard per analoghe iniziative estere (c.d. "Brussels effect"). Stessa visione sposata con il testo del discusso AI Act".

[11] Si veda L. ROZENFELDOVA, P. SOKOL, *Liability regime of online platforms new approaches and perspectives*, in T. PETRASEVIC, D. DUIC, A. NOVOKMET. (eds.), EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 3, 2019, p. 871; A. DE STREEL, M. HUSOVEC, *The E-commerce Directive as the Cornerstone of the Internal Market - Assessment and options for reform*, Study requested by the European Parliament's committee on Internal Market and Consumer Protection, maggio 2020; in particolare, G. MORGESE, *Proposta di digital service act e rimozione dei contenuti illegali online*, in Verso una legislazione europea sui mercati e servizi digitali, a cura di G. CAGGIANO, G. CONTALDI, P. MANZINI, 2021, evidenzia i limiti della vigente direttiva 2000/31/CE che, in primo luogo, non definisce gli aspetti sostanziali e procedurali delle misure di rimozione e disabilitazione con conseguente frammentazione delle discipline statali; in secondo luogo, si è affidata all'autoregolamentazione degli *hosting providers* la moderazione dei contenuti; infine, la disciplina europea non delinea obblighi di trasparenza e diligenza dei prestatori intermediari né poteri di controllo delle autorità europee e nazionali sulla relativa attività.

[12] In generale sulle conseguenze dell'evoluzione tecnologica in ambito regolatorio e garanzia dei diritti, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, 1997; V. ZENO ZENCOVICH, *Informatica ed evoluzione del diritto*, in Diritto dell'informazione e dell'informatica, n. 1, 2003; T.E. FROSINI, *Tecnologie e libertà costituzionali*, in Diritto dell'informazione e dell'informatica, n. 3, 2003, 487 ss.; P. COSTANZO, *Il fattore tecnologico e le sue conseguenze*, in Rassegna parlamentare, n. 4, 2012, 811 ss.; M. AINIS, *Democrazia digitale*, in Rassegna parlamentare, n. 2, 2013; M. BASSINI, *Internet e libertà di espressione*, 2019; M. OLIVETTI, *Diritti fondamentali e nuove tecnologie. Una mappa del dibattito italiano*, in Revista Estudos Institucionales, vol. 6, n. 2, 395-430, maio/ago 2020; G. E. VIGEVANI, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in Diritto Costituzionale, n. 1, 2023, 41 ss..

sociale, adottano le misure relative al ravvicinamento delle legislazioni degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno. Il Regolamento in esame evita pertanto la frammentazione del mercato interno attraverso l'adozione di norme armonizzate sull'esenzione dalla responsabilità dei prestatori di servizi intermediari, su specifici obblighi in materia di *due diligence* e sull'attuazione ed esecuzione[13]; l'obiettivo è un funzionamento corretto del mercato interno dei servizi intermediari che garantisca un ambiente *on line* sicuro, prevedibile ed affidabile in cui il contenuto della Carta dei diritti fondamentali dell'Unione europea (*infra* Carta) sia effettivamente tutelato (articolo 1 e Considerando 9)[14].
In conformità con il menzionato TUE (articolo 5), il Regolamento disciplina la materia, nel rispetto del principio di proporzionalità, nei limiti di quanto necessario allo scopo (Considerando 155)[15]. In questo senso, sebbene non applicabile alle VLOP designate di cui si dirà nel prosieguo, il Regolamento esclude da alcuni obblighi le microimprese e le piccole imprese quali definite nella raccomandazione 2003/361/CE (articoli 15, 19 e 29)[16]. Al contempo, il Regolamento disciplina l'intensità degli obblighi in base alla categoria di prestatore di servizio intermediario e alla dimensione, imponendo la

[13] Sugli obblighi di *due diligence* si veda M. HUSOVEC, I. ROCHE LAGUNA, *Digital Services Act: A Short Primer*, July 5, 2022 in M. HUSOVEC, I. ROCHE LAGUNA (eds.), Principles of the Digital Services Act, Oxford University Press, 2023, in https://ssrn.com/abstract=4153796 o http://dx.doi.org/10.2139/ssrn.4153796. Per G. ABALDO, *Una prospettiva di regolamentazione degli ISP attraverso il Digital Service Act*, in MediaLaws.eu, 3 febbraio 2022, un sistema di *due diligence* è gia` previsto nel GDPR, riferendosi in particolare al *risk assessment*.

[14] P. BILYANA; O. TUOMAS, *Fundamental Rights Protection Online – The Future Regulation of Intermediaries*, 2020; M. BETZU, *I baroni del digitale*, Napoli, 2022, 22; G. ALPA, *La legge sui servizi digitali e la legge sui mercati digitali,* in Contratto e Impr., 2022, 1, richiama a monte del Regolamento la menzionata comunicazione della Commissione europea intitolata "*Plasmare il futuro digitale dell'Europa*" in base alla quale "*la Commissione non intende rallentare lo sviluppo tecnologico del continente, ma adeguarlo ai valori fondanti l'Unione. Si tratta, ancora una volta, della definizione del modello europeo di economia sociale di mercato in cui la libertà economica è temperata dalla protezione dei diritti fondamentali dei cittadini*". In proposito, R.BUCCA, M.SABATINI, *Digital Services Act, la Ue a una svolta: cosa cambia per utenti, aziende e big tech*, in Agenda Digitale, 19 maggio 2022, affermano che "*l'era del "Too Big to Care" ("troppo grande per preoccuparsene") stia assumendo gradualmente i colori rossastri del tramonto*"; in effetti, l'intenzione del legislatore europeo è la protezione del cittadino nel cyberspazio ed un rapporto equo ed equilibrato tra utente e piattaforme con regole che "*secondo Ursula von der Leyen, garantiranno che "ciò che è illegale offline sarà effettivamente illegale online nell'Ue" ai fini della tutela dei diritti fondamentali degli utenti*".

[15] S. BRASCHI, *Il nuovo regolamento sui servizi digitali: quale futuro per la responsabilità degli internet service provider?*, in Dir. Pen. e Processo, 2023, 3, ritiene che il Regolamento segua un principio di proporzione affermando che "*il legislatore europeo mira, in altri termini, ad evitare che l'obiettivo perseguito dall'Unione, di creare un ambiente digitale rispettoso dei diritti e del principio di dignità personale, sia realizzato tramite l'imposizione di sacrifici insostenibili per i singoli operatori*".

[16] M. BROADBENT, *The Digital Services Act, the Digital Markets Act, and the New Competition Tool*, in Center for strategic and international studies, November 20 2021, p. 8, available at: https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool, afferma che "*regarding the DSA section, supporters note its potential to create legal certainty and deepen the European internal market while making liability and consumer-protection requirements more robust. Other voices have raised concerns over where the burden of liability and safety will fall and worry that illegal content would migrate to smaller, less regulated platforms*".

massima regolazione per le VLOP e i VLOSE[17].

Con specifico riferimento all'esenzione dalla responsabilità dei prestatori di servizi intermediari, questi ultimi non sono in generale responsabili delle informazioni trasmesse o memorizzate (articoli 4, 5 e 6), sancendo la disciplina europea l'assenza di un obbligo generale di sorveglianza (articolo 8)[18].

In effetti, i destinatari del servizio dovrebbero essere ritenuti responsabili dei contenuti illegali diffusi attraverso i servizi intermediari, laddove per contenuto illegale si intende "*qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto;*" (articolo 3)[19]; in questo senso, i terzi interessati dai contenuti illegali dovrebbero rivalersi sui destinatari piuttosto che sui prestatori di servizi intermediari (*hosting exemption*)(Considerando 27)[20].

---

[17] In questo senso G. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in Rivista italiana di informatica e diritto, fasc. 1/2022, p. 19.

[18] L. FABIANO, *Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati*, in Diritto dell'Informazione e dell'Informatica (Il), fasc. 4, 2023, precisa che "*Il Digital Services Act ed il Digital Market Act seguono ad una fase nel corso della quale l'Unione Europea ha tentato, tenendo fermo l'impianto normativo della direttiva e-commerce, di responsabilizzare maggiormente gli Internet service providers attraverso l'elaborazione di strumenti di Soft Law".* In tal senso, la Commissione europea era inizialmente intervenuta mediante la raccomandazione (UE) 2018/334 del 1° marzo 2018, atto non vincolante che invitava gli *hosting providers* ad intraprendere misure per contrastare i contenuti illegali, che aveva trovato parziale attuazione attraverso differenziate condizioni generali di servizio. B. MAZZOLAI, *Hate speech e comportamenti d'odio in rete. Casapound vs Facebook: atto III 1*, in Diritto dell'Informazione e dell'Informatica (Il), fasc. 2, 2023, specifica che il *digital service act* costituisce "*il punto di arrivo del quadro regolatorio europeo che negli anni è oscillato tra un sistema di autoregolazione cd. di "soft law" e un modello di co-regolamentazione*" sulla base di codici di condotta adottati relativamente ai fenomeni dell'*hate speech online* e della disinformazione rispettivamente nel 2016 e nel 2018; in particolare, l'autore afferma che il legislatore europeo è intervenuto attraverso uno strumento normativo vincolante di *hard law* che delinea, tra l'altro, un sistema di "*procedimentalizzazione*" dell'attività di moderazione dei contenuti.

[19] Soccorre, in proposito, il Considerando 12 secondo cui a titolo esemplificativo rientrano nella categoria i discorsi d'odio (*hate speech*), i contenuti terroristici e discriminatori, la vendita di prodotti non conformi o contraffatti e l'utilizzo non autorizzato di materiale protetto dal diritto d'autore. Al riguardo, A. NICITA, *Le piattaforme online tra moderazione e autoregolazione: verso il Digital Services Act,* in Medialaws.eu, 25 novembre 2020, afferma che "*la stessa definizione di 'contenuto illegale', e la certezza giuridica della stessa e del suo grado di enforcement, variano in funzione del tipo di contenuto: dal copyright all'hate speech, dal cyberbullismo alla disinformazione, da contenuti violenti all'online advertising ingannevole*"; M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in Rivista italiana di informatica e diritto, 2/2021, p. 14 ss., ritiene che si "*dovrà tener conto di un corpus normativo assai vasto di livello tanto europeo quanto nazionale, cosa che può rivelarsi piuttosto complicata, se si considera [...] la natura transfrontaliera dell'attività di gran parte degli intermediari digitali*".

[20] B. SAETTA, *Entra in vigore il Digital Services Act, la principale normativa europea che regolamenta il mondo digitale*, in Valigia blu, 15 gennaio 2023, afferma che "*È significativo, comunque, che il DSA prenda atto che il problema dei contenuti illegali non è risolvibile scaricando l'onere solo sulle piattaforme [...] In sostanza un diffamato dovrebbe, se possibile, prendersela con diffamante e non con la piattaforma.*". Al riguardo G. FINOCCHIARO, *Digital Services Act: la ridefinizione della limitata responsabilità del provider e il ruolo dell'anonimato*, in MediaLaws.eu, 12 gennaio 2021, ritiene che "*è il momento giusto per chiedersi se non sia possibile anche rafforzare un'ulteriore responsabilità, quella del soggetto che agisce sul web attraverso il provider, ossia [...] quella del soggetto che l'illecito compie [...]*", ritenendo che "*la soluzione migliore non sia quella di prevedere un divieto di anonimato, soluzione che sarebbe impercorribile per moltissime ragioni sia di natura etica che normativa, ma di prevedere, in taluni casi, un doppio livello, ossia un anonimato nei confronti del pubblico e un "non*

Ad ogni modo, qualora i prestatori di servizi intermediari siano effettivamente a conoscenza di contenuti illegali o non appena ne vengano a conoscenza non agiscano immediatamente per la rimozione o la disabilitazione dell'accesso, la disciplina europea configura un'apposita responsabilità (articolo 6)[21]; al riguardo, il prestatore dei servizi intermediari può tra l'altro acquisire tale conoscenza o consapevolezza circa i contenuti illegali tramite indagini volontarie di propria iniziativa *ex* articolo 7 o le segnalazioni di cui all'articolo 16 (Considerando 22).

Se il meccanismo di segnalazione sarà analizzato più avanti, sulle indagini volontarie il legislatore europeo prevede una disciplina apparentemente favorevole per i prestatori di servizi intermediari affermando che "*non sono considerati inammissibili all'esenzione dalla responsabilità prevista agli articoli 4, 5 e 6 per il solo fatto di svolgere, in buona fede e in modo diligente, indagini volontarie di propria iniziativa*" (c. d. clausola del buon samaritano)[22]. In proposito, sebbene emerga l'intendimento del legislatore europeo di esonerare da responsabilità il prestatore di servizi intermediari che svolga indagini di propria iniziativa (c. d. *safe harbour*), è comunque ravvisabile un duplice rischio derivante sia dalla potenziale conoscenza di contenuti illegali a seguito delle indagini volontarie che dall'applicazione di concetti come la buona fede e la diligenza; tali circostanze potrebbero disincentivare i prestatori di servizi intermediari allo svolgimento di indagini volontarie o qualora effettuate incentivare gli stessi a rimuovere i contenuti dubbi[23].

Rimane ferma la possibilità di azioni inibitorie nei confronti dei prestatori di servizi intermediari, attraverso gli ordini di contrasto dei contenuti illegali emessi dalle autorità giudiziarie o amministrative nazionali (articoli 4, 5 e 6, ultimo paragrafo e

---

anonimato" – una personalizzazione, una responsabilità – nei confronti del provider, di modo che il soggetto che commette l'illecito sia identificabile, quantomeno se si soddisfano determinate condizioni normativamente poste attraverso il provider".

[21] O. RAFFAELLI, *La tutela del marchio nel metaverso*, in Rivista di Diritto Industriale, fasc.4-5-6, 2022, dopo aver affermato che il *digital services act* aggiorna la disciplina della direttiva 2000/31/CE, configura gli intermediari di servizi di *marketplace* di *Non Fungible Token* quali prestatori di servizi di *hosting* obbligati "*alla tempestiva rimozione dei contenuti illegali (quali ad esempio gli NFT prodotti in pregiudizio ai diritti di proprietà industriale altrui) ovvero alla immediata disabilitazione dell'accesso ai medesimi, non appena ne vengano a conoscenza attraverso l'espletamento di indagini volontarie o le segnalazioni degli utenti lesi*".

[22] Per A. LA ROSA, M. G. MAZZILLI, *DSA: La Protezione europea del "buon samaritano" e il regime di safe harbour*, in Studio Previti.it, 11 marzo 2022, le azioni del buon samaritano "*devono essere intraprese su base volontaria, a seguito di indagini autonomamente svolte dagli intermediari di servizi online e che, dunque, non sono rese obbligatorie da ordini ricevuti dall'autorità giudiziaria e/o amministrativa, ma che potrebbero essere sollecitate da notifiche/segnalazioni dei titolari dei diritti lesi*".

[23] J. BARATA, *Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act*, in Center for Democracy & Technology, 29 luglio 2020; A. KUCZERAWY, *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, in Verfassungblog, 1 gennaio 2021, secondo cui "*voluntary monitoring could be tricky, as it could lead to awareness of facts or circumstances from which an illegal activity or information is apparent, and therefore to obtaining constructive knowledge [...] As a result, voluntary monitoring could lead to loss of the liability exemption for hosting providers*". G. VASINO, *Censura "privata" e contrasto all'hate speech nell'era delle Internet Platforms*, in Federalismi, 8 febbraio 2023, paventa "*un blocco sistematico dei contenuti sospetti*".

ISSN 2036-7821

articolo 9)[24].
Per concludere sull'argomento, si fa presente che il Regolamento da un lato sopprime i corrispondenti articoli da 12 a 15 della direttiva 2000/31/CE, dall'altro afferma che i riferimenti ai predetti articoli si intendono fatti rispettivamente agli articoli 4, 5, 6 e 8 del Regolamento (articolo 89)[25].

3. Obblighi a carico dei fornitori di piattaforme e motori di ricerca on line di dimensioni molto grandi.

Prima di effettuare una disamina degli specifici obblighi europei, dopo aver delimitato l'ambito di applicazione del Regolamento ai prestatori di servizi intermediari è necessario inquadrare la specifica categoria dei VLOP eVLOSE.
Alla luce della definizione europea (articolo 3), con il termine piattaforma *on line* s'intende "*un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento;*"[26]. Si tratta, pertanto, come

[24] Premesso che l'ordine deve contenere, tra le altre cose, la base giuridica a norma del diritto dell'Unione o nazionale, la motivazione circa l'illegalità dei contenuti e i meccanismi di ricorso utilizzabili, localizzando al contempo i contenuti illegali (*Uniform Resource Locator*), i prestatori di di servizi intermediari informano poi l'autorità ed il destinatario del servizio del seguito dato all'ordine (articolo 9). M. ALOVISIO, *Rimozione delle recensioni false su Google: accolto il ricorso di un ristoratore di Genova*, in Diritto & Giustizia, fasc. 206, 2022, p. 5, commenta la sentenza del Tribunale di Genova del 2 agosto 2022 in cui a seguito di un ricorso cautelare *ex* art. 700 c.p.c. di un ristorante, il giudice emetteva il 6 giugno 2022 un decreto *inaudita altera parte* con cui ordinava a Google di rendere inaccessibili le recensioni denunciate come false e di ripristinare il punteggio assegnato antecedentemente alla pubblicazione dei commenti. Dopo che Google provvedeva alla rimozione delle false recensioni, il giudice ha dichiarato cessata la materia del contendere e ha condannato Google al pagamento delle spese processuali a favore di parte ricorrente. Per quanto riguarda il profilo della conoscenza legale dell'illecito perpetrato dal destinatario del servizio, Google era stato destinatario di una segnalazione sulle recensioni false e diffamatorie e aveva omesso la cancellazione dei contenuti, nonostante secondo il giudice, usando l'ordinaria diligenza, avrebbe potuto facilmente riconoscere la falsità delle recensioni e avrebbe potuto provvedere quindi autonomamente alla loro eliminazione.

[25] In proposito, R. NIRO, *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive*, in Osservatorio sulle fonti, n. 3/2021, in: http://www.osservatoriosullefonti.it, secondo cui le previsioni regolamentari "*non sostituiscono, ma innovano, in parte, la disciplina già racchiusa nella Direttiva 2000/31/CE sul commercio elettronico, riproducendo, per altri versi, le norme ivi contenute (in specie agli artt. 12-15), relative alla responsabilità dei prestatori di servizi intermediari, come interpretate dalla Corte di giustizia*".

Oltre alla citata direttiva sul commercio elettronico, si rammenta che il Regolamento non pregiudica l'applicazione delle altre normative settoriali europee, con particolare riferimento ai servizi di media audiovisivi, al diritto d'autore, alla protezione dei dati personali, al c. d. regolamento (UE) 2019/1150 (*platform to business* P2B) ecc. (articolo 2). Con riferimento a quest'ultimo regolamento europeo si veda F. FOLTRAN, *Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri negoziali*, in MediaLaws.eu, 2019, n. 3, pp. 162-176.

[26] La risoluzione del Parlamento europeo del 15 giugno 2017 sulle piattaforme *on line* e il mercato unico digitale (2016/2276(INI), sottolineava la difficoltà di una definizione unitaria "*a causa di fattori quali la grande varietà di tipi*

rimarcato dal Considerando 13, di una sottocategoria dei prestatori di servizi di memorizzazione di informazioni, rientrando nella fattispecie sia le reti sociali (*social network*) che le piattaforme che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali.

Per motore di ricerca (*search engine*) *on line* si considera "*un servizio intermediario che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto*" (articolo 3).

Fatte le dovute premesse definitorie, l'indagine rivolge lo sguardo alle VLOP e ai VLOSE che, a causa del loro significativo raggio d'azione, comportano rischi sistemici con effetti potenzialmente sproporzionati sull'Unione europea (Considerando 75 e 76); tale significativo raggio d'azione sussisterebbe quando le piattaforme e i motori di ricerca *on line* raggiungono una quota pari al 10% della popolazione dell'Unione europea (Considerando 76). Per questa ragione, il Regolamento attribuisce obblighi supplementari alle piattaforme e motori di ricerca *on line* che "*hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni*"[27] e che sono designati VLOP e VLOSE con decisione della Commissione europea (articolo 33)[28].

---

delle piattaforme online esistenti e dei loro settori di attività nonché del mondo digitale in rapido cambiamento". Al riguardo, S.RUDOHRADSKÁ -D.TREŠČÁKOVÁ, *Proposals for the digital markets act and digital services act: broader considerations in context of online platforms*, in EU and Comparative Law Issues and Challenges Series (ECLIC), 5/2021, p. 495 ss., dopo aver affermato che le piattaforme possono essere classificate secondo differenti prospettive, precisa che "*according to the criterion of target persons, referring to OECD sources, prof. Bejček divides platforms into connecting peers (P2P), traders with traders (B2B), or consumer with traders (B2C). According to the functionality, we can divide platforms to the so-called search engines (GoogleSearch, TripAdvisor), electronic online markets (Amazon, Booking.com, eBay), common economic networks in a shared or interconnecting economy (Uber, Airbnb), social networks (LinkedIn, Instagram, Facebook), or app stores (Apple´s App Store, Google Play)*".

[27] Al fine di determinare se le piattaforme e i motori di ricerca *on line* soddisfino il requisito numerico per la designazione a VLOP e VLOSE (Considerando 65), i medesimi soggetti sono tenuti a pubblicare entro il 17 febbraio 2023 e di seguito almeno ogni sei mesi il numero medio mensile di destinatari attivi del servizio nell'Unione europea, comunicando, su richiesta, le medesime informazioni al DSC del luogo di stabilimento e alla Commissione europea (articolo 24, paragrafi 2 e 3). Al riguardo, in attuazione del Regolamento, in data 8 marzo 2024 l'AGCOM pubblicava un avviso in cui richiedeva ai prestatori di piattaforme *on line* e di motori di ricerca *on line* stabiliti in Italia di comunicare il numero medio mensile di destinatari attivi del servizio. Secondo A. F. FERRARIS, *In vigore il Digital Service Act: Innovazione, Sicurezza e Trasparenza UE*, in Altalex, 19 febbraio 2024, la "d*isposizione è finalizzata non soltanto all'identificazione delle piattaforme di ampia dimensione, ma anche al monitoraggio dell'andamento del mercato dei servizi intermedi, consentendo così alla Commissione Europea di ottenere una visione sempre aggiornata dello stesso*".

[28] In relazione alla designazione di cui all'articolo 33, paragrafo 4, del Regolamento, la Commissione europea ha effettuato 24 designazioni esprimendosi in data 25 aprile 2023, 20 dicembre 2023, 26 aprile 2024 e 31 maggio 2024. Secondo il dettato regolamentare (articolo 33, paragrafo 6), la Commissione europea pubblica (ed aggiorna) l'elenco delle VLOP e dei VLOSE nella Gazzetta Ufficiale dell'Unione europea. Considerato che era prevista un'applicazione anticipata alle VLOP e ai VLOSE designate dalla Commissione europea a decorrere da quattro mesi dalla relativa notifica qualora anteriore al 17 febbraio 2024, il Regolamento è stato applicabile dal 25 agosto 2023 alle piattaforme designate in data 25 aprile 2023.

Ebbene, nel caso delle piattaforme *on line* per destinatari attivi si intendono "*tutti i destinatari che effettivamente ricorrono al servizio almeno una volta in un determinato periodo di tempo*" (Considerando 77). Nell'ipotesi, invece, dei motori di ricerca, i destinatari attivi sono "*coloro che visualizzano informazioni sulla loro interfaccia online*" (Considerando 78).

Delimitato il perimetro soggettivo rilevante per l'analisi, è utile sottolineare che gli obblighi a carico della categoria descritta sono supplementari rispetto agli altri; in effetti, il Regolamento precisa che "*se i servizi offerti da un prestatore sono contemplati da diverse sezioni del presente regolamento, le pertinenti disposizioni del presente regolamento dovrebbero applicarsi solo in relazione ai servizi che rientrano nel loro ambito di applicazione*" (Considerando 15).

Pertanto, premesso che i soggetti obbligati sono in un rapporto di genere a specie, le VLOP e i VLOSE applicano, oltre agli obblighi esclusivi della relativa categoria (Capo III, Sezione 5), anche gli obblighi previsti per i prestatori di servizi intermediari (Sezione 1), per i prestatori di servizi di memorizzazione (Sezione 2) e per i fornitori di piattaforme *on line* (Sezione 3) anche quando consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (Sezione 4)[29].

Infine, il Regolamento dispone alcuni obblighi a contenuto variabile a seconda della categoria di appartenenza, prevedendo la massima estensione per le VLOP e i VLOSE.

Prestatori di servizi intermediari (*Internet service providers*)

Ciò premesso, tutti i prestatori di servizi intermediari dovranno designare punti di contatto unici raggiungibili per via elettronica sia per la Commissione, il Comitato europeo per i servizi digitali (*infra* Comitato)[30] e gli Stati membri che per i destinatari del servizio, garantendo che le relative informazioni siano facilmente accessibili ed aggiornate (articolo 11 e 12)[31] .

Al contempo, i prestatori di servizi intermediari stabiliti in Paesi terzi possono (per il Considerando 44 "*dovrebbero*") nominare un rappresentante legale in uno degli Stati membri in cui offrono servizi (articolo 13); al riguardo, è opportuno precisare che la nomina è un atto dovuto, come emerge dalla versione inglese del Regolamento la quale

[29] A. L. RUM, *Le nuove frontiere della normativa sui servizi digitali nel mercato unico europeo: si rafforza la protezione dei diritti fondamentali degli utenti online con la garanzia pubblicistica delle Authorities. Il Digital Services Act.*, in Il diritto amministrativo, marzo 2024, afferma che viene messo a punto un articolato sistema di obblighi differenziati e asimmetrici a seconda della categoria di servizi di intermediazione e anche in funzione della dimensione dell'operatore digitale.

[30] Il Comitato, presieduto dalla Commissione europea, è composto dai coordinatori dei servizi digitali e fornisce consulenza alla Commissione europea e ai coordinatori dei servizi digitali al fine di un'applicazione coerente del Regolamento (articolo 61 ss.).

[31] In attuazione dell'articolo 11 del Regolamento, in data 8 marzo 2024 la Direzione servizi digitali dell'Autorità per le garanzie nelle comunicazioni (*infra* AGCOM) pubblicava un avviso per la comunicazione del punto di contatto unico designato dai prestatori di servizi intermediari per i rapporti con la Commissione, il Comitato e gli Stati membri.

afferma che i fornitori di servizi intermediari "*shall designate*" un rappresentante legale, paventando al riguardo un obbligo piuttosto che una facoltà. La predetta scelta è notificata al coordinatore dei servizi digitali (*infra* DSC) dello Stato membro in cui il rappresentante legale risiede o è stabilito; il DSC è il punto di contatto unico per tutte le questioni relative all'applicazione del Regolamento per la Commissione, il Comitato, i coordinatori dei servizi digitali degli altri Stati membri nonché per le altre autorità competenti dello Stato membro (Considerando 110)[32].
La designazione del rappresentante legale "*dovrebbe consentire una vigilanza efficace e, se necessario, l'esecuzione*" del Regolamento in relazione ai prestatori che ottemperano al relativo obbligo (Considerando 44). In effetti, nelle predette ipotesi il Regolamento delinea poteri condivisi tra Commissione e Stati membri in cui il rappresentante legale risiede o è stabilito (articolo 56, paragrafo 6)[33].

Prestatori di servizi di memorizzazione (*Hosting providers*)
Oltre a notificare i sospetti di reati che minacciano la vita o la sicurezza di una persona alle autorità dello Stato membro interessato (articolo 18), i prestatori di servizi di memorizzazione di informazioni (incluse le piattaforme *on line*) predispongono meccanismi di segnalazione e azione (*notice and action* o *notice and take down*) esclusivamente per via elettronica che consentono a persone o enti (o segnalatori attendibili[34]) la notifica di contenuti illegali (articolo 16)[35]. Un'interpretazione letterale induce a considerare inutilizzabili i meccanismi di segnalazione per le informazioni incompatibili con le condizioni generali, individuate, invece, dai prestatori di servizi intermediari tramite un'attività di moderazione dei contenuti svolta anche volontariamente[36].

[32] In conformità all'articolo 49 del Regolamento, l'articolo 15 del decreto legge 15 settembre 2023, n. 123, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159, designava quale DSC per l'Italia l'AGCOM; di seguito, in data 8 marzo 2024, la Direzione servizi digitali dell'AGCOM pubblicava un avviso per la comunicazione del rappresentante legale da parte dei prestatori di servizi intermediari stabiliti in un Paese terzo, attuando in tal modo l'articolo 13 del Regolamento.

[33] Ad ogni modo, anche in assenza della nomina del rappresentante legale, il Regolamento prevede una competenza concorrente della Commissione europea e di tutti gli Stati membri (articolo 56, paragrafo 7).

[34] I fornitori di piattaforme *on line* trattano prioritariamente e senza indebito ritardo le segnalazioni provenienti dai *trusted flagger* (articolo 22). Considerato che la qualifica di segnalatore attendibile è riconosciuta ad un ente dal corrispondente DSC che può revocarla previo contraddittorio, AGCOM, con delibera n. 40/24/CONS del 14 febbraio 2024, ha avviato una consultazione pubblica sullo schema di regolamento di procedura per il riconoscimento della qualifica di segnalatore attendibile ai sensi dell'articolo 22 del Regolamento; i DSC degli Stati membri comunicano i segnalatori attendibili alla Commissione europea che procede alla pubblicazione (e all'aggiornamento) delle informazioni in una banca dati accessibile al pubblico.

[35] Per quanto riguarda la funzione degli utenti quali "platform prosecutors"si veda Q. WEINZIERL, *Institutionalizing Parallel Governance: The Digital Services Act, Platform Laws, Prosecutors, and Courts*, in Verfassungsblog, 18 dicembre 2020.

[36] In base alle definizioni del Regolamento (articolo 3), le condizioni generali sono "*tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio*", includendo le informazioni riguardanti la moderazione dei contenuti

Le segnalazioni sono sufficientemente precise e adeguatamente motivate, da un lato spiegando i motivi per cui le informazioni costituiscono contenuti illegali, dall'altro indicando l'esatta ubicazione elettronica delle informazioni stesse (indirizzi *Uniform Resource Locator*). In tali casi "*qualora consentano a un prestatore diligente di servizi di memorizzazione di informazioni di individuare l'illegalità della pertinente attività o informazione senza un esame giuridico dettagliato*", il prestatore di servizi di memorizzazione acquisisce quella conoscenza o consapevolezza circa i contenuti illegali, a seguito della quale si ritiene responsabile delle informazioni memorizzate se non agisce immediatamente per la rimozione dei contenuti o la disabilitazione dell'accesso[37].

Il prestatore del servizio è altresì tenuto a notificare la relativa decisione ai segnalanti, e nel caso di restrizioni, ai destinatari interessati[38], garantendo la possibilità di ricorso in merito alla decisione motivata (articoli 16 e 17)[39].

Ebbene, le predette decisioni sono collegate all'attività di moderazione dei contenuti che è svolta in modo automatizzato o meno "*dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio, comprese le misure*

(articolo 14). I *terms and conditions* sono pubblicati nei casi di VLOP e VLOSE in tutte le lingue degli Stati membri in cui offrono i servizi affiancati da una sintesi dei principali elementi (articolo 14).

[37] S. RUGGIERO, *NFT e proprietà intellettuale: problemi e prospettive*, in Medialaws.eu, 21 febbraio 2023, precisa che ai sensi dell'articolo 6, paragrafo 4, le esenzioni di responsabilità lasciano impregiudicati "*i provvedimenti inibitori emanati da autorità giurisdizionali o amministrative volte a porre fine alle violazioni contestate, anche mediante rimozione dei contenuti illegali o disabilitazione dell'accesso a tali contenuti*".

[38] In caso di decisioni che impongono restrizioni, il contenuto minimo della motivazione riferisce, tra le altre cose, sulla base giuridica o sulla clausola contrattuale rispettivamente fondamento di un contenuto illegale o dell'incompatibilità delle informazioni con le condizioni generali. In proposito, si veda E. CREMONA, *Le piattaforme digitali come public utilities: perchè non applicare alcuni principi di servizio pubblico*, in Giurisprudenza Costituzionale, fasc. 1, 1° febbraio 2023, pag. 467, secondo cui al soggetto, ancorché privato, in posizione di potere è attribuito "*l'onere di spiegare decisioni complesse, quasi sempre automatizzate e spesso impattanti su diritti e libertà fondamentali*". E. SPILLER, *Il diritto di comprendere, il dovere di spiegare. Explainability e intelligenza artificiale costituzionalmente orientata*, in BioLaw Journal, fasc. 2/2021, 419 ss..

[39] Il Regolamento si riferisce, in particolare, ai meccanismi interni di gestione dei reclami, alla risoluzione extragiudiziale delle controversie e al ricorso per via giudiziaria; si ritiene, tuttavia, attivabile anche il diritto di reclamo al DSC competente. Per O. POLLICINO, *Piattaforme digitali e libertà di espressione: l'ora zero*, in Lavoce.info, 19 gennaio 2021, "*se il costituzionalismo analogico è quello dei diritti sostanziali, quello digitale si fonda invece sulla dimensione procedurale*". Secondo F. MARCHETTI, *Esiste una "azione inibitoria europea"? La tutela dei diritti in rete tra vecchi problemi e nuove declinazioni rimediali all'alba del Digital Services Act,* in Il Processo, fasc.1, 1° aprile 2023, l'emanazione del Regolamento "*lungi dal costituire frutto e approdo della ricerca di un nuovo equilibrio, appare, per parte qua, piuttosto dettato da esigenze di chiarezza; fare ratio scripta dell'aquis giurisprudenziale, insomma, con piena conferma dell'impalcatura rimediale che regge la tutela dei diritti in Rete. Il quid novi albergherebbe più propriamente nel rafforzamento dei meccanismi dialogico-partecipativi, preludio di una procedimentalizzazione dell'intervento dei grandi players di Internet — nel che taluni scorgono una fase di legificazione del "data due process" —, e, più in generale, nella moltiplicazione delle possibilità di risolvere la lite prima che giunga "alle soglie del Tempio di Temi", anche con l'intervento di una autorità indipendente neo-istituita*".

ISSN 2036-7821

adottate" (articolo 3)[40]; a quest'ultimo proposito, si distinguono le restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio (la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti), la sospensione, la cessazione o altra limitazione dei pagamenti in denaro, la sospensione o la cessazione totale o parziale della prestazione del servizio ed infine le misure che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni (la sospensione o la chiusura dell'*account* del destinatario del servizio) (articolo 17).

Nel rispetto dei diritti fondamentali della Carta, a seguito della ricezione di una segnalazione l'azione del prestatore di servizi di memorizzazione "*dovrebbe essere rigorosamente mirata, nel senso che dovrebbe servire a rimuovere o disabilitare l'accesso alle informazioni specifiche considerate come contenuti illegali*" (Considerando 51), contemperando la propria libertà di impresa sia con la libertà di espressione e di informazione dei destinatari del servizio che con i diritti (dignità umana e principio di non discriminazione, tutela dei minori, tutela della proprietà intellettuale ecc.) delle parti interessate dai contenuti illegali[41]. Il predetto obiettivo regolamentare corrispondente all'effettiva tutela dei diritti fondamentali della Carta (articolo 1, paragrafo 1) emerge anche dall'applicazione proporzionata richiesta ai prestatori di servizi intermediari sulle restrizioni imposte in base alle condizioni generali, considerando anche nell'attività di moderazione dei contenuti svolta volontariamente i diritti di tutte le parti coinvolte (articolo 14, paragrafo 4).

---

[40] Le condizioni generali includono anche le regole di moderazione dei contenuti, compreso il processo decisionale algoritmico e la verifica umana (articolo 14). Circa la trasparenza agli utenti dei sistemi di *content moderation*, G. DE GREGORIO, *Democratising online content moderation: A constitutional framework*, in Computer law & security review, vol. 36, 2020, p. 1 - 17. Quanto alla censura privata in generale si veda M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in Rivista italiana di informatica e diritto, 1/2019. Si veda altresì, The European Law Students' Association (ELSA), *Comparative Report on Internet Censorship: International Focus Programme on Law and Technology: Final Report of the International Legal Research Group on Internet Censorship*, 2020.

[41] In materia di bilanciamento della libertà di espressione con altri diritti, E. A. BERTONI, *The Inter-American Court of Human Rights and the European Court of Human Rights: a dialogue on freedom of expression standards*, in European Human Rights Law Review, 2009; J. F. FLAUSS, *The European Court of Human Rights and the Freedom of Expression*, in Indiana Law Review, 2009; J. M. BALKIN, *The Future of Free Expression in a Digital Age*, in Pepperdine Law Review, 2009, vol. 36, no. 2, p. 427-444; I. RORIVE, *What Can Be Done against Cyber Hate - Freedom of Speech versus Hate Speech in the Council of Europe*, in Cardozo Journal of International and Comparative Law. 2009, vol. 17, no. 3, p. 417-426; D. VOORHOOF, H. CANNIE, *Freedom of Expression and Information in a Democratic Society*, in The International Communication Gazette, 2010, vol. 72(4–5), p. 407-423; G. LANE, *Human Rights and the Internet in Europe*, in Human Rights and the Internet,, 2014. p. 116-129; A. OOZER, *Internet and Social Networks: Freedom of Expression in the Digital Age*, in Commonwealth Law Bulletin. 2014, vol. 40, no. 2, p. 341-362; B. WAGNER, *Global Free Expression – Governing the Boundaries of Internet Content*, 2016.; D. KEATS CITRON, N. M. RICHARDS, *Four Principles for Digital Expression*, in Washington University Law Review. 2018, vol. 95, no. 6, p. 1353-1388; R. RACOLTA, A. VERTES-OLTEANU, *Freedom of Expression. Some Considerations for the Digital Age*, in Jus et Civitas: A Journal of Social and Legal Studies. 2019, vol. 6, no. 1, p. 7-16; W. BENEDEK, M. C. KETTEMAN, *Freedom of Expression and the Internet. Strasbourg: Council of Europe*, 2020; R. L. WEAVER, *Free Speech in an Internet Era*, University of Louisville Law Review, 2020, vol. 58, no. 2, p. 325-348.

In proposito, appare *prima facie* un grande passo in avanti la considerazione espressa della Carta nell'attività di moderazione dei contenuti, ancorando il *far west* digitale ai valori riconosciuti dall'articolo 6 del TUE che, oltre al riconoscimento da parte dell'Unione europea della Carta, afferma che i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (*infra* CEDU) e risultanti dalle tradizioni costituzionali comuni agli Stati membri "*fanno parte del diritto dell'Unione in quanto principi generali*". In questo senso, la Carta da un lato dispone che le relative disposizioni non sono interpretabili quale limite ai diritti umani riconosciuti dal diritto costituzionale degli Stati membri, dal diritto europeo e internazionale (articolo 53), dall'altra in caso di diritti della Carta corrispondenti a quelli della CEDU "*il significato e la portata*" sono identici a quelli conferiti da quest'ultima (articolo 52)[42].

I fornitori di piattaforme on line

I fornitori di piattaforme *on line* garantiscono altresì un sistema interno di gestione per via elettronica di reclami gratuiti ed entro sei mesi contro tutte le decisioni adottate nei confronti dei destinatari del servizio (incluse le persone o gli enti segnalanti), garantendo, a seguito di decisione motivata, la possibilità di ricorso (articolo 20).

A quest'ultimo proposito, fermo restando il diritto di contestare di fronte ad un organo giurisdizionale le decisioni dei fornitori di piattaforme *on line* anche successive a segnalazioni e reclami, i destinatari del servizio (incluse le persone o gli enti segnalanti) hanno comunque la possibilità di rivolgersi gratuitamente (o per un importo simbolico) ad un organismo certificato per una risoluzione extragiudiziale delle controversie (articolo 21)[43].

Il Regolamento attribuisce comunque ai fornitori di piattaforme *on line* la possibilità di emanare, previo avviso preventivo, misure di protezione temporanea contro gli abusi, sospendendo la prestazione dei servizi ai destinatari che forniscono frequentemente

[42] Si veda il sito della European Union Agency for fundamental rights (https://fra.europa.eu/it) in cui per ogni singolo diritto della Carta è possibile verificare, tra le altre cose, il diritto costituzionale, europeo ed internazionale e la giurisprudenza correlata, con indicazione specifica dei paragrafi delle sentenze che si riferiscono alla Carta.

[43] Considerato che il DSC del luogo di stabilimento è competente a certificare l'organismo (e a revocare tale certificazione previo contraddittorio), AGCOM, con delibera n. 39/24/CONS del 14 febbraio 2024, ha avviato una consultazione pubblica concernente il regolamento sulla procedura di certificazione degli organismi di risoluzione extragiudiziale delle controversie tra fornitori di piattaforme *on line* e destinatari del servizio ai sensi dell'articolo 21 del Regolamento. I DSC degli Stati membri comunicano gli organismi certificati alla Commissione europea che pubblica (ed aggiorna) il relativo elenco su un sito web dedicato facilmente accessibile. Ad ogni modo, in base al Regolamento (articolo 21, paragrafo 2), il predetto organismo "*non ha il potere di imporre una risoluzione della controversia vincolante per le parti*". Al riguardo, A.M. FELICETTI, *La risoluzione extragiudiziale delle dispute nei mercati digitali: alcune novità dall'Europa*, in Rivista trimestrale di diritto e procedura civile, 2023, fasc. 1, secondo cui "*La procedura intrapresa, che seguirà in alternativa il modello di uno strumento autonomo o eteronomo di composizione della lite, non potrà comunque giungere — diversamente da quanto inizialmente proposto dalla commissione — ad una decisione che vincola le parti*". Si veda altresì D. HOLZNAGEL, *The Digital Services Act wants You to "sue" Facebook over Content Decisions in Private De Facto Courts*, in Verfassungsblog, 24 giugno 2021.

"*contenuti manifestamente illegali*"(articolo 23)[44]; anche nella fattispecie, le decisioni "*dovrebbero poter essere sempre oggetto di ricorso*" (Considerando 64).
Inoltre, i fornitori di piattaforme *on line* progettano le interfacce *on line* in modo trasparente, evitando di pregiudicare i destinatari dei servizi nelle loro decisioni (articolo 25)[45].
Infine, i fornitori di piattaforme *on line* adottano misure adeguate e proporzionate per la protezione dei minori attraverso una mirata progettazione delle interfacce *on line*, l'adozione di specifiche norme o l'adesione a codici di condotta (articolo 28 e Considerando 71); a quest'ultimo proposito, la Commissione incoraggia l'elaborazione di codici di condotta a livello dell'Unione europea per la corretta applicazione del Regolamento (articolo 45) ed in particolare per la pubblicità *on line* e l'accessibilità (articoli 46 e 47). Al riguardo, fermo restando il carattere volontario dei codici e la libertà di adesione (Considerando 103)[46], la Commissione e il Comitato esercitano poteri di monitoraggio e valutazione, invitando i firmatari, in caso di inottemperanza sistematica, ad emanare le misure necessarie (articolo 45, paragrafo 4)[47].

I fornitori di piattaforme on line che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali

Al fine di concorrere ad un ambiente *on line* sicuro, affidabile e trasparente (Considerando 72), i fornitori provvedono sia alla tracciabilità degli operatori commerciali (dati di contatto, numero di iscrizione nel registro delle imprese ecc.) che alla progettazione dell'interfaccia *on line* idonea a fornire determinate informazioni (ad esempio identificative di prodotti e servizi) propedeutiche all'utilizzo della piattaforma *on line* (articoli 29 e 30).
Sebbene siano richiesti "*sforzi ragionevoli*" ai fornitori di verificare l'offerta di prodotti e servizi illegali, non sussiste alcun obbligo di sorveglianza generale a carico degli stessi (Considerando 74), imputando il Regolamento la responsabilità agli operatori commerciali. Ciò non toglie che qualora il fornitore venga a conoscenza di prodotti o

[44] Allo stesso modo, i fornitori di piattaforme *on line* sospendono temporaneamente il trattamento di segnalazione e reclami, quando sono presentati frequentemente "*segnalazioni o reclami manifestamente infondati*".

[45] In questo senso V. FALCE, *Piattaforme ed ecosistemi digitali. Scelte pro-concorrenziali*, in Rivista di Diritto Industriale, fasc. 4-5-6, 1° agosto 2022, pag. 172, si riferisce al "*divieto di utilizzare i cosiddetti percorsi oscuri ("dark pattern") sull'interfaccia delle piattaforme online*"; al riguardo, i percorsi oscuri sono "*pratiche che distorcono o compromettono in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate*" (Considerando 67).

[46] G. CALIMA', *Il Codice di Condotta dell'Unione Europea contro l'incitamento all'odio online*, in Ius in itinere, 21 settembre 2020, ritiene che "*il Codice non ha un valore obbligatorio né vincolante, il che significa che l'adesione è del tutta volontaria, così come volontaria è l'applicazione degli impegni in esso cristallizzati. Ciò comporta, tra le tante cose, l'impossibilità di impugnare eventuali violazioni tanto dinanzi ai giudici nazionali quanto dinanzi alla Corte di giustizia dell'Unione Europea*".

[47] M.BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in Rivista "Gruppo di Pisa", fasc. 2/2021, pp.180-181, non valuta positivamente l'articolo 45 sui codici di condotta che "*legittima sul piano positivo l'assunzione da parte delle big tech di inediti compiti para-normativi*".

ISSN 2036-7821

servizi illegali, il Regolamento impone l'obbligo di informare i consumatori (per gli acquisti fino a sei mesi prima) circa l'illegalità, l'identità del produttore e i mezzi di ricorso (articolo 32)[48].

VLOP e VLOSE

Le VLOP e i VLOSE effettuano, almeno una volta l'anno, una valutazione dei "*rischi sistemici*" derivanti dal funzionamento del servizio, tenendo conto, in particolare, delle condizioni generali, dei sistemi di raccomandazione e di altri sistemi algoritmici[49], dei sistemi di moderazione dei contenuti e delle pratiche relative ai dati (articolo 34), ma anche di altre variabili come i sistemi pubblicitari (Considerando 84)[50].

Quanto ai rischi sistemici si identificano quattro ipotesi.

La prima ipotesi è costituita dalla diffusione dei contenuti illegali tramite i servizi erogati, riferendosi a materiale pedopornografico, incitamento all'odio e vendita di prodotti o servizi vietati (Considerando 80).

La seconda ipotesi riguarda gli effetti negativi sull'esercizio dei diritti fondamentali della Carta, richiamando nello specifico la dignità umana (articolo 1 della Carta), il rispetto della vita privata e familiare (articolo 7 della Carta), la tutela dei dati personali (articolo 8 della Carta), la libertà di espressione e informazione (articolo 11 della Carta), la non discriminazione (articolo 21 della Carta), i diritti del minore (articolo 24 della

[48] In mancanza dei recapiti di tutti i consumatori interessati, il fornitore della piattaforma *on line* pubblica le informazioni previste sull'interfaccia *on line*.

[49] In materia di algoritmi tra gli altri si veda M. HILDEBRANDT, *The Dawn of a Critical Transparency Right for the Profiling Era*, in J. Bus (ed.), Digital Enlightenment Yearbook, 2012, 41 ss.; D. K. CITRON, F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in Wash. L. Rev., 89, 2014, 1 ss.; K. CRAWFORD, J. SCHULTZ, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, in B.C. L. Rev., 55, 2014, 93 ss.; N.M. RICHARDS, J.H. KING, *Big Data Ethics*, in Wake Forest L. Rev., 49, 2014, 393 ss.; M. ANANNY, K. CRAWFORD, *Seeing without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability*, in New Media & Soc., 1, 2016; D. R. DESAI, J. A. KROLL, *Trust But Verify: A Guide to Algorithms and the Law*, in Harv. J.L. & Tech., 31, 2017, 1 ss.; J. A. KROLL, J. HUEY, S. BAROCAS, E. W. FELTEN, J. R. REIDENBERG, D. G. ROBINSON, H. YU, *Accountable Algorithms*, in U. Pa. L. Rev, 165, 2017, 633 ss.; P. KIM, *Auditing Algorithms for Discrimination*, in U. Pa. L. Rev. Online, 166, 2017, 189 ss.; W. NICHOLSON PRICE II, *Regulating Black Box Medicine*, in Mich. L. Rev., 116, 2017, 421 ss.; M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità, accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (ed.), Intelligenza artificiale, protezione dei dati personali e regolazione, Torino, 2018, 141 ss.; A.I. NICOTRA, V. VARONE, *L'algoritmo, intelligente ma non troppo*, in Rivista AIC, 4, 2019; G. AVANZINI, *Decisioni amministrative e algoritmi informatici*, Napoli, 2019; G. PESCE, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in Giustizia-amministrativa.it, 2020; L. VIOLA, *Attività amministrativa e intelligenza artificiale*, in Ciberspazio e Diritto, 1-2, 2019, 65 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in BioLaw Journal, 1, 2019, 63 ss.; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in Pol. Dir. 2, 2019; F. DONATI, *Intelligenza artificiale e giustizia*, in Rivista AIC, 1, 2020; R. BIN, *L'algoritmo e l'autonomia privata*, in BioLaw Journal, fasc. 4/2021, 466.

[50] C.A. DE MICHELIS, *Il Digital Services Act: i nuovi obblighi volti a migliorare la lotta alla contraffazione ed i temi aperti*, in Dir. ind., 2022, afferma che "*se il principio guida è che ciò che è illegale off-line è illegale anche online, allora non si vede per quale ragione siano solo le piattaforme, e solo quelle molto grandi, a dover far fronte ad obblighi di analisi e prevenzione del rischio sistemico collegato al loro business model, di implementazione di misure di mitigazione, e ad essere sottoposte ad un penetrante controllo esterno circa l'ottemperanza e l'implementazione dei suddetti obblighi e misure*".

Carta) e l'elevata tutela dei consumatori (articolo 38 della Carta).
La terza ipotesi si riferisce agli effetti negativi sul dibattito civico e sui processi democratici ed elettorali, nonché sulla sicurezza pubblica[51].
Infine, l'ultima ipotesi considera gli effetti negativi sulla violenza di genere, la protezione della salute pubblica e dei minori ed il benessere fisico e mentale della persona, rischi derivanti anche da campagne di disinformazione coordinate (Considerando 83).
Di seguito, le VLOP e i VLOSE dispongono misure di attenuazione ragionevoli, proporzionate ed efficaci, dei rischi sistemici, adeguando, eventualmente, i medesimi fattori che influenzano i rischi sistemici (condizioni generali, moderazione dei contenuti, sistemi di raccomandazione e di pubblicità)[52]; ad ogni modo, in caso di rischi concreti, previa consultazione pubblica la Commissione può elaborare, in cooperazione con i DSC, orientamenti sull'attenuazione dei predetti rischi (articolo 35, paragrafo 3)[53].
Nel caso di circostanze eccezionali che configurano una minaccia grave alla sicurezza pubblica o alla salute pubblica nell'Unione europea (o in una parte significativa)

---

[51] Si confronti E. PARISER, *Il filtro. Quello che Internet ci nasconde*, Milano, 2012; C. CEPERNICH, *Le campagne elettorali al tempo della networked politics*, 2017; G. GORI, *Social media ed elezioni. I limiti del diritto e il rischio di una modulated democracy*, in Informatica e diritto, n. 1-2, 2017, 203 ss.; B. RABAI, *I Big Data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in Amministrare, n. 3, 2017, 407; G. GIACOMINI, *Verso la neointermediazione. Il potere delle grandi piattaforme digitali e la sfera pubblica*, in Iride, n. 3, 2018, 457-468; E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analityca*, in Federalismi.it, 25 aprile 2018; E. LONGO, *Dai big data alle "bolle filtro": nuovi rischi per i sistemi democratici*, in Percorsi costituzionali, n. 1, 29-44, 2019; M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in MediaLaws.eu, n. 2, 2019, 39 ss.; O. GRANDINETTI, *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi" ma, per ora, tutti attuali*, in MediaLaws.eu, n. 3, 2019, 92; P. NORRIS, R. INGLEHART, *Cultural Backlash, Trump, Brexit and Authoritarian Populism*, Cambridge, 2019. A. VENANZONI, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in Rivista italiana di Informatica e Diritto, n. 1, 2020, 5 ss..

[52] Il Regolamento elenca, a titolo non esaustivo, le misure di attenuazione dei rischi (articolo 35), precisando che il Comitato, in cooperazione con la Commissione europea, pubblica relazioni annuali che elencano i rischi sistemici e le *best practices* relative alle misure di attenuazione.

Ad ogni modo, le VLOP e i VLOSE dovrebbero coinvolgere una serie di *stakeholders* (rappresentanti dei destinatari del servizio ecc.) ai fini della valutazione dei rischi sistemici e dell'adozione delle corrispondenti misure di attenuazione (Considerando 90).

Relativamente ai codici di condotta adottabili nell'ambito delle misure di attenuazione dei rischi in cooperazione con altri fornitori (articolo 35), L. AMMANATI, *Regolatori e supervisori nell'era digitale: ripensare la regolazione*, in Giurisprudenza costituzionale, fasc. 3, 1° giugno 2023, riporta che "*Oltre il regolamento 'Platform to business' una interessante evoluzione del modello è nel Digital Services Act che riserva una maggiore attenzione alla costruzione di codici di condotta attraverso una strategia di "cooperazione" (co-regolazione) finalizzata a definire misure, impegni e successiva misurazione dei risultati*"; in particolare, l'autrice rileva che in caso di rischi sistemici "*significativi*" (articolo 45, paragrafo 2), la Commissione europea "*può allargare la partecipazione alla co-definizione dei codici a piattaforme o motori di ricerca molto grandi, a fornitori di piattaforme online, a prestatori di servizi intermediari nonché ad autorità competenti, ad organizzazioni della società civile e ad altre parti interessate*".

[53] Si veda la comunicazione della Commissione europea recante gli orientamenti per le VLOP e i VLOSE sull'attenuazione dei rischi sistemici per i processi elettorali, pubblicata nella Gazzetta Ufficiale dell'Unione europea 26 aprile 2024, Serie C.

derivanti da atti di terrorismo, conflitti armati, catastrofi naturali e pandemie, il Regolamento prevede un apposito meccanismo di risposta alla crisi mediante decisione della Commissione europea, su raccomandazione del Comitato, che impone, per un periodo non superiore a tre mesi, una valutazione e/o l'adozione di misure specifiche scelte da VLOP e VLOSE e/o una relazione (articolo 36 e Considerando 91)[54]. Successivamente, la Commissione europea svolge un'attività di monitoraggio circa l'applicazione delle misure specifiche, riferendo sia al Comitato che al Parlamento europeo e al Consiglio[55].

Ai fini della valutazione, tra l'altro, della conformità agli obblighi regolamentari fino ad ora esaminati (Capo III), le VLOP e i VLOSE si sottopongono a revisioni indipendenti che confluiscono nella "*relazione di revisione*" motivata contenente, tra le altre cose, un giudizio di revisione (articolo 37)[56]. A questo proposito, il giudizio può essere positivo, positivo con osservazioni e negativo, prevedendo, in quest'ultimo caso, raccomandazioni operative sulle misure specifiche da adottare; nella predetta fattispecie, le VLOP e i VLOSE predispongono una "*relazione di attuazione*" che dia conto delle misure specifiche adottate o delle eventuali misure alternative[57].

Inoltre, le VLOP e i VLOSE permettono, entro un determinato termine, alla Commissione europea e al DSC competente, l'accesso ai dati necessari a verificare il rispetto degli obblighi regolamentari (articolo 40)[58]; i dati sono utilizzati dall'ente richiedente al solo fine di valutare la conformità al Regolamento, rispettando comunque le informazioni riservate ed in particolare i segreti commerciali delle VLOP e dei VLOSE.

Al contempo, le VLOP e i VLOSE istituiscono un'apposita funzione di controllo della conformità al Regolamento che, oltre a fornire consulenza sugli obblighi regolamentari, collabora con la Commissione e il DSC competente (articolo 41); il capo della funzione (*compliance officer*), i cui riferimenti sono comunicati alla Commissione

---

[54] In base all'evoluzione della crisi, la Commissione può, a seconda dei casi, prorogare il periodo di ulteriori tre mesi o revocare la decisione. Inoltre, sebbene le misure specifiche siano scelte dalle VLOP e dai VLOSE, qualora si ritenga che le misure adottate non siano proporzionate o efficaci, la Commissione europea, previa consultazione del Comitato, adotta una decisione che richiede il riesame delle stesse.

[55] A titolo di completezza, si precisa che il Regolamento prevede che il Comitato possa raccomandare alla Commissione europea l'avvio dell'elaborazione di protocolli di crisi volontari per fronteggiare situazioni di crisi riferite a circostanze straordinarie relative alla sicurezza pubblica o salute pubblica (articolo 48).

[56] Si veda in proposito il regolamento delegato della Commissione europea 20 ottobre 2023, n. 2024/436/UE, che integra il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, stabilendo norme relative all'esecuzione delle revisioni per le VLOP e i VLOSE. V. C. CAUFFMAN, C. GOANTA, *A New Order:The Digital Services Act and Consumer Protection*, in European Journal of Risk Regulation, vol. 12, issue 4, 2021, p. 758 ss., ritiene che "*A reliable framework for "auditing the auditors" is therefore required. [...] However, a specific supervisory framework for the auditors involved seems to be lacking*".

[57] Ad ogni modo, le relazioni dovrebbero essere trasmesse al DSC competente, alla Commissione europea e al Comitato (Considerando 93).

[58] Il DSC competente può altresì chiedere alle VLOP e ai VLOSE l'accesso ai dati ai ricercatori abilitati per ricerche relative all'individuazione dei rischi sistemici e alla valutazione dell'adeguatezza delle misure di attenuazione.

ISSN 2036-7821

europea e al DSC competente, riporta direttamente all'organo di gestione del fornitore che, a sua volta, garantisce risorse sufficienti.
Infine, sulla base dei costi stimati tenendo conto dei costi sostenuti nell'anno precedente, il Regolamento dispone a carico delle VLOP e dei VLOSE un contributo annuale per le attività di vigilanza espletate dalla Commissione europea non superiore allo 0,05% del reddito netto annuo mondiale, proporzionato al numero medio mensile di destinatari attivi nell'Unione europea per ciascun fornitore (articolo 43)[59].
Gli obblighi supplementari attribuiti alle VLOP e ai VLOSE secondo un criterio di proporzionalità, si giustificano in base all'ampio raggio d'azione su una quota significativa della popolazione dell'Unione europea caratterizzante i soggetti obbligati; conseguentemente, i potenziali effetti significativi sull'Unione europea sono controbilanciati dall'attribuzione di specifici obblighi che, oltre a richiedere una valutazione *ex ante*, conferiscono a soggetti interni (*compliance officer*) ed esterni indipendenti l'*audit* sugli obblighi in materia di dovere di diligenza. A quest'ultimo proposito, è fondamentale che il Regolamento abbia inserito la relazione di revisione (e l'eventuale relazione di attuazione) all'interno degli obblighi di trasparenza, garantendo ai titolari della *governance* di conoscere lo stato dell'arte prima ancora dell'eventuale utilizzo dei poteri di accesso ai dati, ispezione e monitoraggio.

Obblighi a contenuto variabile
Esistono altresì obblighi trasversali ai differenti soggetti il cui contenuto si espande nel passaggio da una categoria all'altra.
In primo luogo, al fine di garantire un adeguato livello di trasparenza, il Regolamento prevede a carico dei prestatori di servizi intermediari l'obbligo di pubblicare relazioni annuali sulle attività di moderazione dei contenuti, precisando, al contempo, se avviate di propria iniziativa o a seguito di segnalazione o reclami o ordini emessi dalle autorità nazionali o con utilizzo di strumenti automatizzati (articolo 15)[60]; il contenuto delle "*relazioni di trasparenza*" si espande, per i fornitori di piattaforme *on line* (articolo 24), con le controversie sottoposte agli organismi di *alternative dispute resolution* e le misure di protezione contro gli abusi e per le VLOP e i VLOSE (articolo 42), con l'indicazione delle risorse umane utilizzate e delle qualifiche, competenze linguistiche

[59] Al riguardo, in conformità con l'articolo 43, paragrafo 4, è stato emanato il Regolamento delegato (UE) 2023/1127 della Commissione europea del 2 marzo 2023 che integra il *digital service act* con le metodologie e le procedure dettagliate relative ai contributi per le attività di vigilanza addebitati ai VLOP e ai VLOSE.
[60] A quest'ultimo proposito, M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, cit., afferma che "*la proposta di DSA sembra allinearsi all'opinione, oggi generalmente condivisa, secondo cui il ricorso a filtri di ricerca automatizzati, soprattutto per le piattaforme di grandi dimensioni, sia in concreto l'unico strumento praticabile per garantire, da una parte, una tutela effettiva della vita privata e dei diritti della personalità degli utenti e, dall'altra parte, per non imporre oneri economici straordinari a carico del gestore del servizio, a patto di assicurare un adeguato livello di trasparenza dei parametri di funzionamento degli algoritmi di filtraggio*".

e formazione del personale addetto alla moderazione dei contenuti[61].
Si precisa che nell'ambito degli obblighi in materia di trasparenza, le VLOP e i VLOSE trasmettono al DSC competente ed alla Commissione europea la valutazione del rischio, le conseguenti misure di attenuazione, la relazione di revisione e di attuazione, mettendo a disposizione del pubblico l'intero materiale (articolo 42, paragrafo 3).
A proposito di pubblicità presentata dai fornitori di piattaforme *on line* attraverso le interfacce *on line*, oltre alle informazioni sui parametri (e modalità di modifica) utilizzati per individuare i destinatari, essi garantiscono, tra le altre cose, ai destinatari di identificare sia la pubblicità (anche mediante contrassegni visibili) che la persona per la quale è presentata e che paga la pubblicità al fornitore, fornendo comunque ai medesimi destinatari una funzionalità che permette di segnalare eventuali loro comunicazioni commerciali ai fornitori, che rendono edotti gli altri destinatari anche mediante contrassegni visibili (articolo 26)[62]. Con riferimento alle VLOP e ai VLOSE, è prevista una maggiore trasparenza della pubblicità *on line* attraverso l'adozione di un registro contenente, tra le altre cose, l'oggetto, la durata e i gruppi destinatari (e i parametri utilizzati), accessibile al pubblico per facilitare la vigilanza su eventuali rischi emergenti dalla distribuzione pubblicitaria (articolo 39 e Considerando 95).
In ultimo, premesso che un sistema di raccomandazione è "*un sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire informazioni specifiche, tramite la propria interfaccia online, ai destinatari del servizio o mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate*" (articolo 3), il Regolamento prevede un obbligo di trasparenza a carico dei fornitori di piattaforme *on line* che specificano nelle condizioni generali sia i parametri utilizzati che le opzioni di modifica a disposizione dei destinatari (articolo 27). Per quanto riguarda, invece, le VLOP e i VLOSE, è assicurata anche un'opzione per la non ricezione (*opt-out*) di suggerimenti sui contenuti basati sulla profilazione accessibile dall'interfaccia *on line* (articolo 38 e Considerando 94)[63].
Si ritiene che i menzionati obblighi a contenuto variabile rivestano un'importanza fondamentale, garantendo un'ampia trasparenza in settori rilevanti come la moderazione dei contenuti, i sistemi di raccomandazione e la stessa pubblicità.

---

[61] Per le VLOP e i VLOSE le relazioni sono semestrali piuttosto che annuali, aggiungendo al contempo le informazioni sul numero medio mensile di destinatari del servizio per ciascuno Stato membro.

[62] A parte gli obblighi di trasparenza rispetto alla pubblicità mirata, il Regolamento prevede anche un divieto di pubblicità ai destinatari basata sulla profilazione che utilizza particolari categorie di dati personali (articolo 26, paragrafo 3). In proposito, si veda D. SBORLINI, *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in Diritto dell'Informazione e dell'Informatica (Il), fasc.6, 1° dicembre 2022, pag. 1173.

[63] V. E.GARZONIO, *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in Rivista italiana di informatica e diritto, 2/2021, valuta positivamente la trasparenza dei sistemi di raccomandazione e il correlato diritto di *opt-out* da parte degli utenti, ritenendo che "*la conoscibilità dell'algoritmo [...] rappresenta un'importante riappropriazione di coscienza e di modalità con cui controbattere alla predeterminazione dei contenuti e dell'informazione con cui entriamo in contatto*".

Come sempre la trasparenza è utile agli attori della *govenance* ed agli *stakeholders* per esercitare in modo corretto gli obblighi istituzionali e i diritti garantiti dalla Carta.

4. Competenze e poteri della commissione europea e diritti delle parti.

Competenze

Il Regolamento predispone una struttura di *governance* complessa che prevede la "*stretta cooperazione*" tra Commissione europea e Stati membri in cui sono situati gli stabilimenti principali delle VLOP e dei VLOSE, al fine della vigilanza ed applicazione degli obblighi europei (articoli 56 e 57)[64].

In relazione agli obblighi supplementari a carico delle VLOP e dei VLOSE (Capo III, Sezione 5), si prevede una competenza esclusiva della Commissione europea[65].

Per tutti gli altri obblighi regolamentari a carico della medesime categorie soggettive (VLOP e VLOSE), si prevedono poteri di vigilanza ed applicazione della Commissione europea condivisi con gli Stati membri i quali, per il tramite dei DSC, agiscono solo nell'ipotesi in cui l'istituzione europea non abbia avviato procedimenti per la medesima infrazione[66].

E' evidente che una siffatta ripartizione dei poteri necessita di un sistema di condivisione delle informazioni in tempo reale (articolo 85 e Considerando 148) attraverso il quale la Commissione europea e i DSC degli Stati membri si informano reciprocamente circa l'intenzione di esercitare i relativi poteri, evitando duplicazioni sanzionatorie nel rispetto del principio del *ne bis in idem* (Considerando 123 e 125)[67].

---

[64] B. WAGNER, H. JANSSEN, *A First Impression of Regulatory Powers in the Digital Services Act*, in Verfassungsblog, 4 gennaio 2021; P. CARDILLO, *Digital Services Act, ecco chi verifica che venga rispettato*, in Agenda digitale, 28 febbraio 2023, afferma che "*Si delinea ancor più, in questo caso, una specifica e articolata Governance del mercato dei Servizi Digitali laddove accanto al principio della competenza connessa alla localizzazione territoriale dell'azienda si affianca e prevale il principio della dimensione aziendale correlata al numero di utenti forniti.*".

[65] La Commissione europea agisce anche a seguito di richiesta del DSC presentata mediante il sistema di condivisione delle informazioni (articolo 65, paragrafo 2).

[66] D. HOLZNAGEL, *All Member States should contribute to the Supervision of Very Large Online Platforms under the Digital Services Act*, in Verfassungsblog, 27 aprile 2021, afferma che "*the role of the Commission would be crucial to counterbalance the not-so-unrealistic scenario that the country of origin (for most Big Tech companies that is Ireland) fails to fulfill its oversight role for the whole Union and all its citizens*". Ferma restando un'azione di propria iniziativa (ad esempio per violazioni transfrontaliere riguardanti più Stati membri secondo il Considerando 125), la Commissione europea può intervenire quando, per il tramite del sistema di condivisione delle informazioni, il DSC segnala la sospetta "*sistematica*" violazione di una disposizione regolamentare da parte delle VLOP e dei VLOSE con "*gravi ripercussioni*" per i destinatari del servizio all'interno dello Stato membro (articolo 65, paragrafo 2).

Qualora la Commissione europea non abbia avviato un'indagine, il Comitato può richiedere al DSC del luogo di stabilimento di valutare la condotta di un fornitore di servizi intermediari sulla base della richiesta di almeno tre DSC del luogo di destinazione, raccomandando, eventualmente, indagini comuni transfrontaliere (articolo 58 e 60); al riguardo, in caso di omessa risposta nei termini o di disaccordo, il Comitato è altresì titolare di un potere di deferimento alla Commissione europea, che può a sua volta chiedere il riesame della questione (articolo 59).

[67] In proposito, si veda il regolamento di esecuzione della Commissione europea 15 febbraio 2024, n. 2024/607/UE, relativo alle modalità pratiche e operative per il funzionamento del sistema di condivisione delle informazioni, che istituisce il sistema AGORA.

Per tutte le altre fattispecie, il Regolamento prevede poteri esclusivi degli Stati membri[68]; in particolare, la competenza è del DSC in cui è situato lo stabilimento del fornitore di servizi intermediari o, in mancanza, del luogo in cui risiede o è stabilito il rappresentante legale[69].
In sostanza, con riferimento alle oltre venti VLOP e VLOSE designate, la Commissione europea è l'unica istituzione pubblica competente relativamente agli obblighi supplementari; nulla esclude che la medesima istituzione europea intervenga riguardo agli altri obblighi regolamentari in capo ai medesimi soggetti, sebbene in tal caso gli Stati membri possano esercitare i relativi poteri fino all'intervento della Commissione europea[70].
Non bisogna trascurare che la maggior parte dei soggetti designati ha la propria sede in uno Stato membro (Irlanda); si dubita, pertanto, che un serio *enforcement* sia ipotizzabile ad opera del corrispondente DSC, anche considerato che il medesimo organo è competente per tutte le altre ipotesi regolamentari non connesse alle VLOP e ai VLOSE.
Alla luce delle predette considerazioni, si ritiene rilevante il ruolo attivo della Commissione anche per gli obblighi non supplementari, ipotizzabile solo attraverso un importante supporto alla competente Direzione "Piattaforme" della DG *Connect*.

Poteri

Dopo aver delineato il sistema di *governance* progettato dal Regolamento, si rappresenta che la Commissione, d'ufficio o su richiesta del DSC, si avvale dei poteri di indagine anche prima dell'avvio del procedimento istruttorio (articolo 65); si tratta di una pre istruttoria effettuata dall'istituzione europea, a seguito della quale la Commissione può discrezionalmente decidere di avviare un'indagine formale o adottare misure provvisorie (Considerando 138 e 139).
A tal proposito, quando la Commissione europea, in base alle proprie valutazioni discrezionali, sospetta la violazione del Regolamento ad opera della condotta delle

[68] D. HOLZNAGEL, *All Member States should contribute to the Supervision of Very Large Online Platforms under the Digital Services Act*, cit., rileva che il *digital service act* si basa sul *country of origin principle*.

[69] Fermo restando il diritto al risarcimento dei danni (articolo 54), i destinatari del servizio (e associazioni rappresentative) hanno il diritto di presentare un reclamo al DSC dello Stato membro in cui sono situati o stabiliti, al fine di evidenziare una violazione del Regolamento da parte dei fornitori di servizi intermediari (articolo 53); previa valutazione del reclamo, il DSC trasmette, eventualmente, lo stesso al DSC del luogo di stabilimento del fornitore, affiancando, qualora lo ritenga utile, un parere (facoltativo). Premessa la titolarità di poteri di indagine e di esecuzione, anche sanzionatori (articolo 51), i DSC pubblicano una relazione annuale sulle attività svolte, inserendo, tra le altre cose, il numero di reclami ed il relativo seguito, comunicando la stessa alla Commissione europea ed al Comitato (articolo 55). Con riferimento ai reclami, AGCOM, con delibera n. 41/24/CONS del 14 febbraio 2024, avviava un procedimento istruttorio finalizzato all'adozione delle procedure per la presentazione dei reclami.

[70] Per F. PIZZETTI, *Accordo sul DSA*, in Agenda digitale, 26 aprile 2022, uno degli aspetti più importanti del nuovo pacchetto normativo è l'attribuzione di un potere rilevante alla Commissione chiamata a vigilare direttamente sul rispetto delle nuove regole.

ISSN 2036-7821

VLOP e dei VLOSE, l'avvio del procedimento istruttorio è notificato, oltre che al fornitore interessato, anche ai DSC e al Comitato per il tramite del sistema di condivisione delle informazioni, evitando potenziali violazioni del principio del *ne bis in idem* (articolo 66)[71].

I poteri di indagine utilizzabili dalla Commissione, anche per il tramite dei DSC interessati, sono le richieste di informazioni, i poteri di audizione, le ispezioni e le azioni di monitoraggio, le cui informazioni raccolte sono funzionali "*esclusivamente*" all'applicazione del Regolamento (articolo 66, paragrafo 3 e 79, paragrafo 5)[72].

Riguardo alle richieste di informazioni che devono essere evase "*entro un termine ragionevole*" (articolo 67)[73], la Commissione europea può acquisirle, oltre che dalle VLOP e dai VLOSE interessate, anche da qualsiasi altra persona fisica o giuridica che agisce per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale (ad esempio le organizzazioni che effettuano le revisioni); la Commissione europea, inoltre, dovrebbe poter chiedere informazioni anche a "*qualunque autorità pubblica, organismo o agenzia negli Stati membri*" inclusi i DSC (Considerando 141).

Con riferimento, invece, al potere di audizione (articolo 68), previo consenso la Commissione europea può ascoltare qualsiasi persona fisica o giuridica, registrando al contempo l'audizione. Al pari della richiesta di informazioni, l'obiettivo è la raccolta di informazioni pertinenti alla presunta violazione; tuttavia, nella fattispecie l'ambito soggettivo sembra più ampio, necessitando, altresì, il consenso della persona, motivo per il quale il Regolamento non prevede alcuna sanzione. L'istituto in esame rientra comunque nei poteri di indagine della Commissione europea, differenziandosi strutturalmente dal diritto di essere ascoltati (*right to be heard*) delle parti che se espletato oralmente comporta un'audizione di fronte alla Commissione europea.

In relazione ai poteri di ispezione espletati nei confronti dei medesimi soggetti sottoposti a richieste di informazioni (articolo 69), la Commissione europea può accedere ai locali e sigillarli, esaminare libri e documenti su qualsiasi supporto (estraendo eventualmente copia), accedere al sistema informatico, agli algoritmi e alla gestione dei dati, effettuando al contempo domande al personale con contestuale

[71] In base ad un comunicato stampa del 14 marzo 2024, si apprende che la Commissione europea ha aperto un procedimento formale nei confronti di AliExpress al fine di verificare la violazione del Regolamento, ed in particolare, delle disposizioni sull'organizzazione e mitigazione dei rischi, la moderazione dei contenuti e il sistema interno di trattamento dei reclami, la trasparenza della pubblicità e i sistemi di raccomandazione, la tracciabilità degli operatori commerciali e l'accesso ai dati per i ricercatori.

[72] Anche nella fattispecie, la Commissione europea informa sia il Comitato che il DSC del luogo di stabilimento (articolo 66, paragrafo 4).

[73] Fermo restando il diritto di adire la Corte di giustizia dell'Unione europea per il controllo di legittimità sulle decisioni della Commissione europea, l'omessa risposta nei termini o la comunicazione di informazioni inesatte, incomplete o fuorvianti è potenzialmente oggetto di sanzioni pecuniarie (articolo 74) e penalità di mora (articolo 76).

ISSN 2036-7821

verbalizzazione[74].
Infine, la Commissione europea può effettuare, anche tramite esperti e revisori esterni, un'azione di monitoraggio dell'attuazione degli obblighi regolamentari da parte di VLOP e VLOSE (articolo 72), ordinando, eventualmente, l'accesso a banche dati e algoritmi (e relative spiegazioni) e la conservazione dei documenti necessari[75].
Quanto ai poteri di esecuzione esercitabili a seguito dell'avvio del procedimento, la Commissione europea si avvale dei medesimi poteri attribuiti ai DSC[76].
Preliminarmente, al fine di evitare il "*rischio di danni gravi*" per i destinatari del servizio, la Commissione ha il potere di adottare misure provvisorie senza attendere l'esito del procedimento avviato (articolo 70); le predette misure cautelari sono possibili solo se l'istituzione europea constati *prima facie* la sussistenza di un'infrazione agli obblighi regolamentari da parte della VLOP e del VLOSE (Considerando 142).
Inoltre, la Commissione europea può rendere vincolanti gli impegni offerti dalle VLOP e dai VLOSE, purché garantiscano la conformità alle disposizioni regolamentari (articolo 71); in tal caso, la decisione dell'istituzione europea termina il procedimento avviato a carico delle parti.
Infine, l'avvio del procedimento da parte della Commissione europea in caso di sospetto di violazione regolamentare è collegato, salva eventuale decisione di archiviazione, alla successiva decisione di non conformità (*non-compliance*) con potere di ordinare l'adozione delle misure necessarie (correttive) e/o di irrogare sanzioni pecuniarie non oltre il 6% o l'1% del fatturato annuo (articoli 73 e 74)[77]. Qualora la potenziale violazione riguardi gli obblighi supplementari, l'ordinamento europeo prevede una "*vigilanza rafforzata*" delle misure correttive (articolo 75); in particolare, le VLOP e i VLOSE comunicano un piano di azione dettagliato contenente le misure necessarie ai DSC, al Comitato ed alla Commissione europea. Dopo aver deciso l'idoneità delle misure rispetto alla violazione tenendo in massima considerazione il parere del Comitato, la Commissione europea monitora l'attuazione del piano anche attraverso le relazioni di revisione trasmesse, informando al contempo i DSC ed il

[74] Fermo restando il diritto di adire la Corte di giustizia dell'Unione europea per il controllo di legittimità sulle decisioni della Commissione europea, il rifiuto di sottoporsi ad un'ispezione è potenzialmente oggetto di sanzioni pecuniarie (articolo 74) e penalità di mora (articolo 76). Si veda inoltre l'articolo 2 ("*Spiegazioni fornite durante le ispezioni*") del Regolamento di esecuzione (UE) 2023/1201 della Commissione europea del 21 giugno 2023 relativo alle modalità dettagliate di attuazione da parte della Commissione di determinate procedure a norma del *digital service act* (*infra* Regolamento di esecuzione (UE) 2023/1201).

[75] Si veda, inoltre, l'articolo 3 del Regolamento di esecuzione (UE) 2023/1201 sulle azioni di monitoraggio.

[76] La Commissione europea informa il DSC del luogo di stabilimento ed il Comitato qualora adotti misure provvisorie o renda vincolanti gli impegni (articolo 66, paragrafo 4).

[77] Oltre che alle violazioni delle disposizioni regolamentari, la soglia del 6% del fatturato annuo è collegata agli altri poteri decisori della Commissione europea; il riferimento è in particolare sia al non rispetto delle misure provvisorie che alla non conformità agli impegni vincolanti.
Quanto alla soglia dell'1%, si ricollega alla violazione dei poteri di indagine della Commissione europea; il riferimento è nella fattispecie all'omessa, inesatta, incompleta o fuorviante risposta alla richiesta di informazioni, al rifiuto di sottoporsi ad un'ispezione e all'inottemperanza ai provvedimenti adottati nelle azioni di monitoraggio.

ISSN 2036-7821

Comitato.
Al contempo, al fine di imporre alle VLOP e ai VLOSE il rispetto dei poteri decisori, la Commissione europea ha il potere di imporre penalità di mora periodiche non oltre il 5% del reddito giornaliero medio (articolo 76)[78].
Ad ogni modo, in coerenza con l'articolo 261 del TFUE, è previsto un controllo giurisdizionale di merito ad opera della Corte di giustizia dell'Unione europea nei confronti delle decisioni della Commissione europea che irrogano sanzioni pecuniarie e penalità di mora (articolo 81).
Infine, il Regolamento prevede una clausola residuale in base alla quale, qualora una violazione non sia terminata, nonostante i poteri decisori, causando danni gravi, la Commissione europea, previo invito alle parti a presentare osservazioni scritte, domanda al DSC del luogo di stabilimento di chiedere all'autorità giudiziaria una restrizione temporanea dell'accesso al servizio interessato dalla violazione da parte dei destinatari o, in via residuale, all'interfaccia *on line* della VLOP e del VLOSE (articolo 82)[79].
Sull'argomento non si può comunque sottacere la mancanza di coordinamento tra i poteri di indagine e l'obbligo previsto a carico delle VLOP e dei VLOSE di fornire l'accesso ai dati entro un termine ragionevole su richiesta della Commissione europea funzionale alla verifica della conformità regolamentare (articolo 40). Quest'ultima ipotesi contempla altresì la spiegazione dei sistemi algoritmici, come esplicitato sia per le ispezioni che nelle azioni di monitoraggio. Ad ogni modo, si ritiene che l'accesso ai dati costituisca un obbligo supplementare a carico delle VLOP e dei VLOSE la cui violazione comporti una potenziale decisione di non conformità e/o sanzionatoria ad opera della Commissione; al contrario, le altre ipotesi rappresentano un'esplicazione dei poteri di indagine attribuiti dal Regolamento alla Commissione per lo svolgimento dei compiti assegnati.

Diritti delle parti
Si è visto fino ad ora che la Commissione europea è titolare di una serie di poteri che utilizza nell'ambito del procedimento amministrativo avviato in caso di sospetta violazione delle disposizioni regolamentari di relativa competenza, anticipato eventualmente dalla cosiddetta preistruttoria nell'ambito della quale utilizza i poteri di indagine a disposizione.
Ciò premesso, la Commissione europea emana le constatazioni preliminari (*preliminary findings*), punto di partenza per l'eventuale successivo esercizio dei poteri

[78] Nello specifico, l'irrogazione di penalità di mora periodiche tende ad imporre la fornitura di informazioni corrette e complete, la sottoposizione ad ispezioni, la conformità alle misure provvisorie, agli impegni vincolanti e alle *non compliance decisions* della Commissione europea.
[79] Considerato il richiamo all'articolo 51, paragrafo 3, del Regolamento, si ritiene che la fattispecie sia applicabile solo alle violazioni che integrino un reato grave che comporti una minaccia per la vita o la sicurezza delle persone.

ISSN 2036-7821

di adottare decisioni di non conformità, sanzioni o penalità di mora; in sostanza, al pari della *statement of objections* nel diritto della concorrenza, si tratta di un atto formale in cui la Commissione europea prende una posizione preliminare ufficiale, sollevando obiezioni su specifiche questioni.
Oltre ad informare il DSC del luogo di stabilimento ed il Comitato sulle constatazioni preliminari, tenendo in massima considerazione il relativo parere del Comitato nella successiva decisione (articolo 66), la Commissione europea garantisce i diritti di difesa delle parti interessate sia mediante accesso al fascicolo che tramite il diritto di essere ascoltati (articolo 79 e Considerando 146).
Ebbene, la Commissione europea può emanare decisioni legittime solo se le relative obiezioni provenienti dalle constatazioni preliminari siano state garantite da un corretto esercizio del *right to be heard* ad opera delle parti interessate (articolo 79, paragrafo 3).
Propedeutico al *right to be heard* è il diritto di accesso al fascicolo della Commissione europea.
Nel fascicolo confluiscono, oltre ai documenti della Commissione e di altre autorità, anche le informazioni provenienti dall'esercizio dei poteri di indagine nei confronti di VLOP, VLOSE e di qualsiasi altra persona fisica o giuridica che agisce per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale (ad esempio le organizzazioni che effettuano le revisioni).
Sebbene il Regolamento non definisca le "*parti interessate*", dal Considerando 146 si deduce che siano tali le VLOP e i VLOSE e le "*altre persone soggette all'esercizio dei poteri della Commissione i cui interessi possono essere lesi da una decisione*"; in proposito, l'articolo 5 del Regolamento di esecuzione (UE) 2023/1201 prevede che la Commissione conceda l'accesso al fascicolo all'istante destinatario delle constatazioni preliminari tramite la fornitura di tutti i documenti ivi citati.
In base al Regolamento, il diritto di accesso al fascicolo si svolge secondo una "*divulgazione negoziata*"; tuttavia, in caso di disaccordo tra le parti, la Commissione europea impone la procedura di divulgazione in base ad una decisione (articolo 79, paragrafo 4)[80].
Ad ogni modo, il Regolamento prevede che siano protetti i segreti commerciali (articolo 79, paragrafo 4); in questo senso, il Regolamento di esecuzione (UE) 2023/1201 dispone che dai documenti citati nelle constatazioni preliminari siano espunti parti connesse alla protezione dei segreti aziendali o altre informazioni riservate (articolo 5,

[80] In base al Regolamento di esecuzione (UE) 2023/1201, la divulgazione di tutti i documenti del fascicolo senza espunzioni "*può essere effettuata per via elettronica o (per alcuni o per tutti i documenti) presso i locali della Commissione*" (articolo 5, paragrafo 3, lettera e). Tuttavia, in circostanze eccezionali, l'istituzione europea effettua un bilanciamento tra i benefici ai fini del diritto di essere ascoltati dell'ostensione di un documento ed il danno potenziale per colui che ha presentato lo stesso; a seguito di tale analisi, è possibile escludere l'accesso a determinati documenti o permettere un accesso parziale (articolo 5, paragrafo 4, del Regolamento di esecuzione (UE) 2023/1201).

paragrafo 2), come individuate dalle VLOP, dai VLOSE e da qualsiasi altra persona fisica o giuridica che agisce per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale, che forniscono, al contempo, una versione non riservata (*non-confidential version*) con descrizione sintetica delle parti espunte (articolo 6).

La Commissione europea può comunque ritenere che eventuali ipotesi non costituiscano segreti commerciali o, sebbene siano ritenute tali, sussista un interesse prevalente alla divulgazione, informando, al riguardo, gli interessati che, in assenza di opposizione, si disporrà l'accesso; al contrario, nel caso di opposizione, la Commissione europea emana una decisione motivata (articolo 6, paragrafo 6).

Infine, il diritto di accesso al fascicolo non include le informazioni riservate e i documenti interni della Commissione europea, del Comitato, dei DSC e di altre autorità pubbliche, inclusa la corrispondenza (articolo 79, paragrafo 4).

Si rammenta, in proposito, che il Regolamento prevede un potere sanzionatorio pecuniario della Commissione europea in caso di violazione ad opera delle parti interessate delle condizioni di accesso al fascicolo (articolo 74, paragrafo 2, lettera f).

Sulla base delle conoscenze acquisite con l'esercizio dell'accesso agli atti, le parti interessate esercitano eventualmente il diritto di essere ascoltati in merito alle constatazioni preliminari della Commissione europea (articolo 79, paragrafo 1 e Considerando 146).

Primariamente, il *right to be heard* consiste nella presentazione di osservazioni scritte (non oltre cinquanta pagine) entro un termine ragionevole (non inferiore a quattordici giorni) stabilito dalla Commissione europea in una delle lingue ufficiali dell'Unione europea (articolo 4 del Regolamento di esecuzione (UE) 2023/1201).

A seguito di un'interpretazione sistematica derivante dalla lettura degli articoli 79 e 83 del Regolamento, si poteva ampliare la nozione del *right to be heard* anche alle audizioni orali come avviene nel campo del diritto europeo della concorrenza; in effetti, da un lato l'articolo 79 parla genericamente di osservazioni, dall'altro l'articolo 83 si riferisce alle "*audizioni previste dall'articolo 79*". Tuttavia, il Regolamento di esecuzione (UE) 2023/1201 emanato dalla Commissione europea si focalizza sulle sole osservazioni scritte, limitando il *right to be heard* rispetto alla potenziale apertura regolamentare. L'eventuale riconoscimento delle osservazioni orali avrebbe garantito, oltre ad una più completa esplicazione del diritto di essere ascoltati per le parti interessate, anche una maggiore possibilità per la Commissione europea di verificare in modo diretto la consistenza delle constatazioni preliminari. Tuttavia, l'istituzione europea avrebbe avuto una posizione parziale in assenza di una figura più indipendente come il consigliere auditore (T*he Hearing Officer*) istituito al di fuori della DG Competition nel diritto della concorrenza europeo in cui si occupa anche di garantire il diritto di accesso al fascicolo e la riservatezza.

ISSN 2036-7821

5. Conclusioni.

Si è effettuata un'analisi teorica della disciplina regolamentare delineata dal Parlamento europeo e dal Consiglio dei ministri dell'Unione europea che rappresenta l'esito del costituzionalismo digitale e della sovranità digitale nell'Unione europea[81]; in particolare, la regolazione sembra rappresentare un giusto punto intermedio tra il modello privatistico americano (*digital liberalism*) ed il modello pubblicistico ed antidemocratico dei regimi autoritari[82].

La Commissione europea, *dominus* nella *governance* per lo meno sulle VLOP e i VLOSE e titolare di atti delegati[83] e di esecuzione[84], dovrà presentare una relazione, eventualmente corredata di proposte di modifica, agli organi legislativi dell'Unione europea ed al Comitato economico e sociale europeo sull'applicazione delle disposizioni relative, tra le altre, ai rappresentanti legali, al meccanismo di segnalazione e azione, al sistema interno di gestione dei reclami, alla risoluzione extragiudiziale delle controversie, ai VLOP e VLOSE, al contributo per le attività di vigilanza, sull'efficacia dei meccanismi di vigilanza ed applicazione, sul funzionamento del Comitato e sull'impatto nei confronti del diritto alla libertà di espressione e di informazione.

E' evidente, pertanto, che l'applicazione pratica in gran parte espletata a livello decentrato decreterà il successo o meno dell'impianto normativo attuale, motivo per cui la Commissione europea nell'ambito del "*riesame*" si avvale anche delle relazioni annuali dei DSC. Conseguentemente, il prossimo futuro sarà utile a comprendere se la disciplina europea attuale possa fungere da punto di riferimento a livello globale, procedendo, in caso contrario, ad effettuare gli appositi correttivi alla luce delle indicazioni della Commissione europea. Durante la trattazione è emersa comunque

---

[81] G. DE MINICO, *Fundamental rights, european digital regulation and algorithmic challenge*, in Medialaws.ue, 1/2021, p. 21, si sofferma "*on the perspective of the offline constitutional acquis of democratic countries being transported online, in order that a better protection of fundamental rights and liberties be achieved [...]*", precisando poi che "*a binding regulation, although held to a minimum, will be able to draw an algorithm in accordance with the European Constitutional values*".

[82] M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in Rivista italiana di informatica e diritto, 1/2022, pp. 47-48, parla di "*terza via alla governance di Internet, alternativa tanto al modello di private self-regulation promosso dagli USA quanto al modello statocentrico a guida governativa sostenuto dai regimi autoritari*". In senso contrario T. E. FROSINI, *L'ordine giuridico del digitale*, in Giurisprudenza Costituzionale, fasc.1, 1° febbraio 2023, pag. 377, il quale afferma che "*non è da condividere la scelta della UE, peraltro opposta a quella adottata negli USA, di regolare gli sregolati con un profluvio di norme di dettaglio, alcune delle quali di difficile attuazione e pertanto rimandate alla concreta applicazione da parte dei singoli Stati*".

[83] In conformità all'articolo 290 TFUE, l'articolo 87 del Regolamento prevede il potere di adottare atti delegati (in parte, come visto, esercitato) per gli articoli 24 ("*Obblighi di comunicazione trasparente per i fornitori di piattaforme on line*"), 33 ("*Piattaforme online di dimensioni molto grandi e motori di ricerca online di dimensioni molto grandi*"), 37 ("*Revisioni indipendenti*"), 40 ("*Accesso ai dati e controllo*") e 43 ("*Contributo per le attività di vigilanza*").

[84] In conformità all'articolo 291 TFUE, il Regolamento prevede atti di esecuzione ad opera della Commissione europea (in parte, come visto, emanati) per gli articoli 15 ("*Obblighi in materia di relazioni di trasparenza per i prestatori di servizi intermediari*"), 24 ("*Obblighi di comunicazione trasparente per i fornitori di piattaforme on line*"), 43 ("*Contributo per le attività di vigilanza*"), 83 ("*Atti di esecuzione relativi all'intervento della Commissione*") e 85 ("*Sistema di condivisione delle informazioni*").

ISSN 2036-7821

l'opportunità di correggere l'articolo 13 del Regolamento nella versione italiana, laddove paventa la facoltà piuttosto che l'obbligo di nomina del rappresentante legale. Al contempo, si potrebbe valutare l'inserimento espresso delle audizioni orali insieme all'istituzione di una figura indipendente che tuteli anche il diritto di accesso e la riservatezza, garantendo con maggiore efficacia il *right to be heard* delle VLOP e dei VLOSE, anche considerate le potenziali sanzioni irrogabili.

Ad ogni modo, l'impianto normativo costituisce una vera e propria rivoluzione nel campo del digitale che regolamenterà nel prossimo futuro i servizi digitali nello spazio europeo[85]. L'Unione europea è intervenuta sul mercato interno dei servizi intermediari attraverso un atto di *hard law* direttamente applicabile, prevedendo una funzionalizzazione del potere privato al perseguimento di un interesse pubblico costituito da un ambiente *on line* fondato sui diritti della Carta[86].

Nella sostanza, è importante comprendere la reale implementazione della clausola del buon samaritano, valutando in termini più generali l'attività di moderazione dei contenuti dei prestatori di servizi intermediari ed in particolare delle piattaforme[87].

Nella fattispecie emerge da un lato un problema di concentrazione delle piattaforme digitali[88], dall'altro un "*power to disseminate*" informazioni assai diffuso rispetto al passato[89]. Ciò significa che pochi soggetti dovranno moderare una moltitudine di

---

[85] In questi termini F. G. MURONE, *Il Digital Service Act e il contrasto ai contenuti illeciti (pt. II)*, in Ius in itinere, 28 febbraio 2022.

[86] Nel senso di una funzionalizzazione del potere privato ad un interesse pubblico diretto alla tutela dei diritti di libertà E. CREMONA, *Le piattaforme digitali come public utilities: perchè non applicare alcuni principi di servizio pubblico*, cit. Quanto ai poteri privati in generale G. DI GASPARE, *Poteri privati e Corporation nella globalizzazione*, 847-869, in Rivista Diritto Pubblico, n. 3/2021; R. PARDOLESI, *Piattaforme digitali, poteri privati e concorrenza*, 941-960, in Rivista Diritto Pubblico, n. 3/2021; M. R. FERRARESE, *Poteri nuovi. Privati, penetranti, opachi,* Bologna 2022, 138 ss.; E. CREMONA, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato*, tutela dei diritti, Napoli 2023. M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale,* in P. Costanzo-P. Magarò -L. Trucco, Il diritto costituzionale e le sfide dell'innovazione tecnologica, Napoli 2022, 39-68.

[87] Secondo L. ALBERTINI, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione*, in MediaLaws, Law and Media Working Paper Series, 2019, n. 4, pp. 1-182, sebbene "t*utti i grandi provider si riservino questa facoltà, probabilmente poi nei fatti non controllano alcunché: a meno che ciò venga in via automatica tramite i filtri oppure dopo denuncia di illecito*".

[88] L. M. KHAN, *Amazon's Antitrust Paradox*, in The Yale Law Journal, 2017, 710 ss.; S. MANNONI, G. STAZI, *Is Competition a Click Away? Sfida al monopolio nell'era digitale*, Napoli 2018; N. SMYRNAIOS, *Internet Oligopoly. The Corporate Takeover of Our Digital World*, Bingley, 2018, spec. 83 ss.; M. MOORE, D. TAMBINI, *Digital Dominance. The Power of Google, Amazon, Facebook and Apple*, New York 2018; F. BASSAN, *Innovazione tecnologica e regolazione nell'Unione Europea, I mercati dell'algoritmo tra concorrenza e protezione dei dati*, in S. DOMINELLI, G. L. GRECO, *I mercati dei servizi fra regolazione e governance*, Torino 2018, 20-21; L. ZINGALES, F. M. LANCIERI, *Committee on Digital Platforms: Policy Brief. Chicago Booth*, 2019, Stigler Center for the Study of the Economics and the State; F. DUCCI, *Natural Monopolies in Digital Platform Markets*, Cambridge 2020, 24 ss.; N. PETIT, *Big Tech and the Digital Economy: The Moligopoly Scenario*, Oxford 2020; A MANGANELLI, *Il regolamento Eu per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in Mercato Concorrenza Regole fasc. 3/2021, 473-500.

[89] I. A. HARTMANN, *A new framework for online content moderation*, Computer Law & Security Review: The International Journal of Technology Law and Practice, in https://doi.org/10.1016/j.clsr.2019.105376, precisa che "*There is far less concentration in the power to disseminate information. Whereas before there was a very small number of people capable of making judgement calls on the circulation of specific instances of information that would reach a wide audience, now*

informazioni, senza considerare che la stessa individuazione dei contenuti illegali sarà problematica per piattaforme che operano all'interno di plurimi Stati con potenziali differenti ordinamenti giuridici.

In tale ambito, oltre all'iniziativa dei fornitori di servizi intermediari, sarà fondamentale il ruolo svolto dai cittadini che se attivi nell'esercizio dei propri diritti tramite il meccanismo di segnalazione e gli altri istituti potranno dare un forte impulso all'implementazione della Carta e della legalità; grazie anche ad una maggiore trasparenza all'interno delle condizioni generali, l'iniziativa dei destinatari sarà altresì utile per contrastare i processi di selezione delle informazioni ad opera delle piattaforme nei sistemi di raccomandazione.

In proposito, saranno utili le relazioni di trasparenza con le decisioni adottate, sia di iniziativa, che a seguito di segnalazioni/reclami, dai fornitori di servizi intermediari nell'attività di moderazione dei contenuti, nonché i provvedimenti adottati dagli attori istituzionali nazionali ed europei coinvolti nella *governance* del *digital service act* e gli eventuali correlati contenziosi giurisdizionali instaurati.

Con specifico riferimento alle VLOP e ai VLOSE, sarà utile verificare l'applicazione della valutazione dei rischi sistemici e delle conseguenti misure di attenuazione riguardanti qualsiasi sistema algoritmico anche nella moderazione dei contenuti[90]; non è infatti casuale che a parte un potere di accesso ai dati necessari a verificare la conformità regolamentare (articolo 40), la Commissione europea, sia nell'ambito del potere di effettuare ispezioni (articolo 69) che nelle azioni di monitoraggio (articolo 72), possa accedere e richiedere chiarimenti/spiegazioni sugli algoritmi[91].

In proposito, è opportuno rilevare che l'attuale sistema di *governance* per le VLOP e i VLOSE basato su poteri esclusivi della Commissione e poteri condivisi con gli Stati

billions of people make decisions on what to share, forward or give visibility to on a daily basis", aggiungendo poi che "*if problems with the quality of speech arise as a collateral damage of the Internet, we should not hurry to blame it on the fact that access to media is more democratic.*". L. FABIANO, *Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati*, cit., ritiene che "*le tecnologie informatiche della comunicazione (ICT) presentano delle evidenti differenze con i media tradizionali in primo luogo con riguardo al c.d. "modello comunicativo" giacché i media precedenti (tanto la stampa quanto radio e televisione) erano improntati ad un modello c.d. "one to many" ed orientati ad una comunicazione unidirezionale (ove è ben distinto il ruolo di coloro che esprimono il messaggio e di coloro che lo ricevono); diversamente le ICT sono strumenti di comunicazione c.d. "many to many" e si caratterizzano per il fatto che tutti gli utenti che li utilizzano sono allo stesso tempo produttori e riceventi dell'informazione*".

[90] In proposito, D. DESAI, J. KROLL, *Trust but Verify: A Guide to Algorithms and the Law*, in Harward Journal of Law and Technology, 2017; M. PEREL, N. ELKIN-KOREN, *Accountability in Algorithmic Copyright Enforcement*, in Stanford Technology Law Review, 2016. Si riferisce agli obblighi di trasparenza algoritmica O. POLLICINO, *Contraddizioni americane, europee e la ricerca di un terreno comune*, in Medialaws.eu, 17 giugno 2021.

[91] Secondo F. PASQUALE, *The black box society*, 2015, considerato che "*The Power to include, exclude, and rank is the power to ensure which public impressions become permanent and which remain fleeting*", è tempo "*for us as citizens to demand that important decisions about our financial and communication infrastructures be made intelligible, soon, to independent reviewers— and that, over the years and the decades to come, they be made part of a public record available to us all*". Sul tema della creazione di una agenzia si veda anche A. TUTT, *An FDA for Algorithms*, in Administrative Law Review, 2017.

membri sulla base del principio del paese d'origine suscita perplessità.
Anche considerata l'attuale dislocazione geografica degli stabilimenti delle VLOP e dei VLOSE, si concentra l'intero sistema di vigilanza su uno o pochi altri Stati membri e sulla Commissione europea; pertanto, il ruolo futuro della Commissione europea ed in particolare dell'ufficio europeo per l'intelligenza artificiale all'interno della DG Connect sarà fondamentale per compensare le difficoltà dei DSC degli Stati membri coinvolti dal principio del paese d'origine.
Nel caso in cui il sistema non regga sarà utile considerare eventuali alternative quali il coinvolgimento, oltre alla Commissione, di altri Stati membri estranei al perimetro del principio del paese d'origine, come avviene attualmente, ai sensi dell'articolo 56, paragrafo 7, del Regolamento, per le ipotesi in cui un fornitore di servizi intermediari, non avendo uno stabilimento nell'Unione europea, abbia omesso di nominare un rappresentante legale.

ISSN 2036-7821