



28 GIUGNO 2023

L'Unione Europea e la lotta alla disinformazione *online*

di Silvia Sassi

Professore associato di Diritto pubblico comparato
Università degli studi di Firenze

L'Unione Europea e la lotta alla disinformazione *online**

di Silvia Sassi

Professore associato di Diritto pubblico comparato
Università degli studi di Firenze

Abstract [It]: Questo saggio analizza le strategie giuridiche adottate dagli Stati e dall'Unione europea per contrastare la disinformazione online. Sicché vuole chiarire, anzitutto, che cosa si intende per disinformazione, giacché sembra assumere una fisionomia giuridica sempre più autonoma. In seconda battuta, passa poi ad analizzare specificamente le misure adottate dalla UE per combatterla, anche al fine di svolgere qualche breve considerazione sull'impatto che questo nuovo assetto regolatorio avrà in materia sulle discipline dei suoi Stati membri e sui sistemi predisposti dai prestatori dei servizi di intermediazione della società digitale, in particolare quelli di dimensioni molto grandi.

Title: The European Union and the fight against online disinformation

Abstract [En]: This essay deals with the legal measures adopted by States and the European Union to counter disinformation online. The aim is to clarify, first of all, what is meant by disinformation, since it increasingly seems to be taking on a legal character of its own. Secondly, the measures taken by the EU to combat it will be specifically analysed. This is also in order to make some brief remarks on the impact that this new regulatory framework will have on the disciplines of its Member States and on the systems set up by the intermediary service providers of the digital society, especially the very large ones.

Parole chiave: Disinformazione online, Unione europea, Piattaforme online di dimensione molto grandi, Motori di ricerca online di dimensioni molto grandi, Regolamento sui servizi digitali, Doveri di diligenza

Keywords: Disinformation online, European Union, VLOPs/VLOSEs, Digital Service Act, Due diligence obligations

Sommario: 1. Introduzione. 2. Disinformazione: una concettualizzazione. 3. Linee di tendenza delle strategie giuridiche di contrasto alla disinformazione tra ordinamenti nazionali ed europeo. 4. Le misure dell'Unione europea. 4.1. ... di prima generazione: dal 2015. 4.2. ... di seconda generazione: dal 2020. 4.2.1. Il codice rafforzato sulla disinformazione. 4.2.2. Il regolamento sui servizi digitali. a) la moderazione dei contenuti. b) la valutazione dei rischi sistemici. 5. Alcune osservazioni conclusive sulle ricadute applicative. a) ... degli Stati membri UE. b) ... delle piattaforme e dei motori di ricerca *online* di dimensioni molto grandi.

1. Introduzione

Governare la disinformazione rappresenta una sfida fondamentale del nostro tempo¹. L'attualità di questo antico-tema² è dovuta principalmente allo spazio nel quale esso oggi si attua, che è quello digitale; uno

* Articolo sottoposto a referaggio.

¹ Così il rapporto del Segretario Generale dell'Assemblea delle Nazioni Unite, *Countering disinformation for the promotion and the protection of human rights and fundamental freedoms*, 12.8.2022, A/77/287, 3.

² Il fenomeno *de quo* non è inedito nella storia della umanità. Le costruzioni false e arbitrarie della realtà sono risalenti nel tempo. Al riguardo cfr.: A. KOYRÉ, *Réflexions sur le mensonge*, Allia, Paris, 2004; L. CANFORA, *La storia falsa*, Rizzoli, Milano, 2008; M. BLOCH, *La guerra e le false notizie*, trad. it., Donzelli, Roma, 2014; P. MIELI, *Le verità nascoste. Trenta casi di manipolazione della storia*, Rizzoli, Milano, 2019. Peraltro data la sua interdisciplinarietà, è stato analizzato sotto molteplici profili, da quello gius-filosofico a quello socio-politologico, finanche economico. Tra le più recenti monografie cfr. G.

spazio dominato da enti privati, sottratto alla sovranità dello Stato, che, per le sue tecniche sempre più raffinate, rende la disinformazione non solo più insidiosa rispetto al passato ma, in alcuni casi, talmente pernicioso da essere considerata una minaccia seria ed effettiva per le istituzioni democratiche³. Al punto che alcuni ordinamenti giuridici di vario livello hanno nel tempo adottato una serie di misure per provare a contrastarla⁴.

La questione è delicata, perlomeno, sotto due profili. Da un lato, perché la disinformazione è strettamente correlata alla libertà di manifestazione del pensiero, e non riguarda le sole notizie false, ma anche quelle diffuse in modo non corretto, o non diffuse affatto, per informare mendacemente o ingannare il consumatore o il cittadino. Dall'altro, perché il fenomeno *de quo* si presenta in disparate forme, può essere, infatti, attuato e/o organizzato con diversi mezzi e da diversi soggetti su molteplici temi⁵.

Innanzitutto a un fenomeno così scivoloso, il problema a monte non è quello di prevenire la diffusione intenzionale di informazioni dannose, quanto quello di arginare qualsiasi rischio al restringimento arbitrario della libertà di manifestazione del pensiero e della libertà di ricevere e accedere a un'informazione di qualità. Risposte restrittive, volte a inibire la disinformazione *online* potrebbero minare, a valle, il ruolo dell'informazione nella sua capacità di offrire notizie libere e di qualità⁶. Peraltro, limitazioni in tale ambito sono potenzialmente foriere della propaganda di Stato. La qualificazione di

PITRUZZELLA, O. POLLICINO, *Disinformation and Hate Speech. A European Constitutional Perspective*, Egea, Milano, 2020; T. GUERINI, *Fake News e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020; C.R. SUSTEIN, *Liars. Falsehood and Free Speech in Age of Deception*, OUP, Oxford, 2021; A. NICITA, *Il Mercato delle Verità. Come la disinformazione minaccia la democrazia*, il Mulino, Bologna, 2021; S. SASSI, *Disinformazione contro Costituzionalismo*, Editoriale Scientifica, Napoli, 2021; J. Attali, *Disinformati. Giornalismo e libertà nell'epoca dei social*, trad. it., Ponte alle Grazie, Milano, 2022; T. RID, *Misure attive. Storia segreta della disinformazione*, trad. it., Luiss University Press, Roma, 2022; C. HASSEN, C. PINELLI, *Disinformazione e democrazia. Populismo, rete e regolazione*, Marsilio, Venezia, 2022; B.-C. HAN, *Infocrazia*, trad. it., Einaudi, Torino, 2023; L. MCINTYRE, *On Disinformation. How to Fight for Truth and Protect Democracy*, MIT Press, Cambridge-MA, 2023.

³ Assai critica su queste posizioni è la *School of Public Policy - Georgia Institute Technology - Internet Governance Project*. Al riguardo, in particolare, v. M. MULLER, *Misinformation about Disinformation?*, in www.internetgovernance.org (25.2.2021) e T.E. FROSINI, *Liberté Egalité Internet*, 3 ed. ampliata, Editoriale Scientifica, Napoli, 2023, p. 189.

⁴ Se nel contesto analogico gli Stati, per affrontare la diffusione di falsità, hanno creato e regolato fattispecie giuridiche quali la diffamazione, la frode, la pubblicità ingannevole e la falsa testimonianza, in quello digitale le modalità attraverso cui i Paesi stanno contrastando lo stesso fenomeno vanno da legislazioni censorie, punitive o limitative a legislazioni che permettono l'adozione di misure di blocco di accesso a Internet. O ancora a legislazioni volte a regolamentare le piattaforme digitali, vuoi conferendo ad alcune autorità pubbliche un ruolo diretto nel controllo dei contenuti dalle stesse veicolate, vuoi concentrandosi piuttosto sulle procedure con cui la manipolazione delle informazioni viene gestita dalle aziende digitali. Per approfondimenti con approccio comparato cfr. T. GUERINI, *Fake News ...*, cit., p. 60 ss. e S. SASSI, *Disinformazione ...*, cit., p. 47 ss.

⁵ La complessità del fenomeno è efficacemente descritta da C. WARDLE, *Information Disorder*, 2^{en} ed., Strasbourg, 2018 e dal rapporto del Segretario Generale dell'Assemblea delle Nazioni Unite, *Countering disinformation ...*, cit.

⁶ V. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Disease pandemics and the freedom of opinion and expression*, A/HRC/44/49, 23.4.2020 (<https://undocs.org/en/A/HRC/44/49>) secondo cui: «the penalization of disinformation is disproportionate, failing to achieve its goal of tamping down information while instead deterring individuals from sharing what could be valuable information», 13.

“falsa informazione” potrebbe facilmente degenerare in un’argomentazione retorica volta a screditare un discorso opposto, polarizzando le posizioni.

Ecco perché la disinformazione, come giustamente è stato già affermato⁷, non può essere considerata una pratica illegale di per sé, a meno che non ci sia l'intenzione di contrastare i principi costituzionali.

È in questa ottica che qui si affronta il tema della disinformazione. In particolare, questo studio vuole chiarire, in primo luogo, che cosa si intende per disinformazione, poiché, a parere di chi scrive, sembra assumere sempre più una fisionomia giuridica autonoma. Si passerà poi ad analizzare specificamente le misure adottate dalla UE per combatterla, anche al fine di svolgere qualche breve considerazione sull’impatto che questo nuovo assetto regolatorio avrà in materia sulle discipline dei suoi Stati membri e sui sistemi predisposti dai prestatori dei servizi di intermediazione della società digitale, in particolare quelli di dimensioni molto grandi.

2. Disinformazione: una concettualizzazione

La disinformazione è comunque da considerare un fenomeno degenerativo dell’informazione. Già l’etimo della parola — dis-informazione — dà l’idea di una situazione peggiorativa, ovvero di un mal-funzionamento nella erogazione della informazione. L’informazione arricchisce la democrazia; la disinformazione la impoverisce. La qualità delle informazioni che si ricevono e si diffondono è fondamentale per il buon funzionamento del sistema democratico perché è la base su cui poggiano le deliberazioni e si assumono decisioni consapevoli. La disinformazione inquina questo sistema, perché vi immette informazioni imprecise o fuorvianti e al limite anche false e giuridicamente sanzionabili che destabilizzano, in tale caso, il sistema per provocare intenzionalmente un danno pubblico. Non è un caso, infatti, che la disinformazione è una delle tecniche più antiche utilizzate dal potere per conquistare il territorio nemico⁸. Una strategia talmente sofisticata ed efficace che nel 1923 viene ad essere sistematizzata in via ufficiale da un’unità speciale della Direzione politica statale (GPU) come “arma da guerra”⁹; che nel periodo della pandemia generata dal Covid-19 è stata in grado di ostacolare l’efficacia

⁷ P. BARILE, *Diritti dell'uomo e libertà fondamentali*, il Mulino, Bologna, 1984, p. 229.

⁸ A. KOYRÉ (*Rèflexions ...*, cit., p. 25) ricorda, tra i primi a far uso di questa tecnica, gli ittiti che, prima della battaglia di Qadesh nel 1274 A.C., trasmisero false informazioni agli egiziani per influenzare l'esito del conflitto. L'A. ritiene, inoltre, che l'arte della manipolazione delle informazioni sia stata diffusa fin dall'antichità attraverso opere quali l'*Arthashastra* risalente al IV sec. A.C., i *Dialoghi* di PLATONE, la *Retorica* di ARISTOTELE, e più recentemente *L'arte di persuadere* di PASCAL (1660) o *L'arte di ottenere ragione* di SCHOPENHAUER (1831).

⁹ Secondo il rapporto del Centre d'analyse, de prévision et de stratégie (CAPS) et de l'Institut de recherche stratégique de l'École militaire (IRSEM) (J.-B. JEANGÈNE VILMER, A. ESCORCIA, M. GUILLAME, J. HERRERA, *Les Manipulations de l'information. Un défi pour nos démocraties*, Paris, 2018) la prima operazione significativa di disinformazione sovietica è stata l'“operazione Trust” (1923-1927), organizzata dalla GPU che ha istituito una falsa organizzazione di resistenza anti-bolscevica (“Unione monarchica della Russia centrale”) al fine di identificare i veri monarchici e gli anti-bolscevichi. Questa tecnica – che comprendeva interviste con esperti fittizi, documenti contraffatti, foto e video ritoccati – divenne poi più sofisticata alla fine degli anni '60 sotto la guida del direttore del KGB Yuri Andropov: così riporta il rapporto

della risposta della sanità pubblica, generando confusione e sfiducia tra le persone¹⁰; e che, in occasione della crisi Ucraina-Russia, è stata identificata dalla Corte di Giustizia dell'UE come «parte integrante dell'arsenale della guerra moderna [...] in grado di minare le fondamenta delle società democratiche»¹¹.

In questa prospettiva, è evidente quanto la pratica della disinformazione, e quella *online* in particolare, non sia da sottovalutare. Non solo perché, come sopra detto, la sua individuazione è sfuggente. Essa non si riconosce unicamente con le *fake news*. Almeno non sempre. A volte, le informazioni vere possono essere manipolate in forme diverse, mescolate con fatti, fonti e pratiche plausibili. Ma anche perché la tecnologia digitale ne ha potenziato l'efficacia. Internet consente, per esempio, la creazione di *account* semi-automatici e di *bot* completamente automatizzati, così come reti di falsi *follower*, video e contenuti multimediali manipolati (*deep-fakes*)¹², pubblicità mirata, *trolling* organizzato, memo visivi e molto altro ancora. La vasta gamma di tecniche digitali in circolazione permette un uso spregiudicato dei mezzi di comunicazione incentrato sul “rimbalzo” di messaggi attraverso la pubblicazione, i commenti e la loro condivisione per il tramite di *tweet* e *re-tweet* o di bolle di filtraggio e di eco-camere che radicalizzano il pensiero annientando il confronto delle idee. Peraltro, queste tecniche, dettate dall'economia comportamentale dell'informazione, non implicano una dicotomia tra verità e falsità. Nella maggior parte dei casi, l'organizzatore di questi sistemi non si posiziona rispetto alla verità, ma cerca piuttosto di ottenere un vantaggio. Un vantaggio che si ottiene in virtù degli algoritmi più intelligenti, non degli argomenti migliori¹³.

Va da sé che questa mutazione genetica della disinformazione generata dalle nuove tecnologie digitali e diffusa nel ciberspazio ha comportato un nuovo approccio al suo contrasto.

Prima però di sviluppare questo aspetto, è necessario inquadrare il fenomeno nella sua dimensione tecnico-giuridica. Tra le definizioni impiegate per configurare la disinformazione¹⁴, nel suo profilo

del CANADIAN SECURITY INTELLIGENCE SERVICE, *Who said What? The Security Intelligence of Modern Disinformation*, Canada, 2018, 26-27.

¹⁰ Motivo per cui l'OMS ha impiegato il termine «infodemia» (il cui conio – secondo L. CORBOLANTE, www.treccani.it – risale a D.J. ROTHOPF, in occasione di un articolo sulla SARS, dal titolo *When the Buzz Bites Back* e pubblicato nel *Washington Post* l'11.5.2003) per indicare «un eccesso di informazioni su un problema che rende difficile individuare una soluzione. Durante un'emergenza sanitaria può contribuire alla diffusione di informazioni false, fuorvianti e non confermate. L'infodemia può ostacolare l'efficacia della risposta della sanità pubblica e generare confusione e sfiducia tra le persone» in: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4.

¹¹ Tribunale UE, sent. 27.7.2022, causa T-125/22, *RT France c. Consiglio dell'Unione europea*, par. 56. Per commenti al caso: cfr. S. SASSI, *La Soft War dell'Unione europea: il caso RT- France vs. Consiglio*, in *Dir. Inf.*, n. 6, 2022; S. LATTANZI, *Il Consiglio sanziona “la propaganda del Cremlino” e sospende le attività di diffusione dell'agenzia di informazione Sputnik e del canale RT/Russia Today*, in www.aisdue.eu (BlogDUE), 2022.

¹² Si pensi alle recenti fotografie divenute virali sul *Web* di Donald Trump con le manette (22.3.2023) e di Papa Francesco che indossava un piumino Moncler (26.3.2023).

¹³ B.-C. HAN, *Infocrazia ...*, cit., p. 31.

¹⁴ Pochissime sono le definizioni normative di disinformazione. Al riguardo si segnalano quella fornita dall'autorità italiana per le garanzie per le comunicazioni, nel suo rapporto del 2018, *News v. Fake nel sistema della informazione*, 25; e,

ovviamente deteriore, si ritiene utile riprendere quella fornita dal gruppo di esperti di alto livello sulle notizie false e sulla disinformazione *on-line* istituito nel 2018 dalla Commissione europea che la intende come l'insieme di «informazioni false, inesatte o fuorvianti progettate, presentate e diffuse a scopo di lucro o per ingannare intenzionalmente il pubblico, e che possono arrecare un pregiudizio pubblico»¹⁵. Essa «non include [...] errori, [...] satira [...] parodia, o notizie e commenti chiaramente identificabili come di parte»¹⁶. La scelta di concepire la disinformazione in questo senso vuole precisamente evidenziare due elementi¹⁷: l'intento ostile sotteso alla pratica, per un verso, e l'impatto potenzialmente dannoso prodotto dalla stessa, per altro verso. Più specificamente, un intento che causa un danno pubblico per obiettivi politico-ideologici o di vantaggio economico e che mina la legittimità di un processo elettorale, rovina la reputazione di una grande società o crea un ambiente ostile boicottando il dibattito democratico, esacerbando la polarizzazione sociale per migliorare la propria immagine. Il danno da scongiurare è, in estrema sintesi, la messa in pericolo dei processi e dei valori democratici. Sicché, la disinformazione che qui intendiamo assumere come concetto si distingue dalla misinformazione — «che si verifica quando contenuti falsi vengono diffusi accidentalmente da utenti inconsapevoli, convinti di divulgare contenuti che corrispondono a un reale interesse sociale»¹⁸ — e dalla mala-informazione, che si riscontra «quando informazioni veritiere vengono pubblicate con lo specifico scopo di creare conseguenze avverse»¹⁹. Governare una sfida così caleidoscopica richiede ineluttabilmente l'adozione di una molteplicità di misure da assumere sulla base di una sinergica e trasparente cooperazione tra i diversi attori (pubblici e privati) che competono in questa nuova dimensione.

come vedremo qui di seguito, dalla Commissione europea, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*, DG for Communication Networks, Content and Technology, Bruxelles, 2018, p. 10. Le piattaforme digitali, a loro volta, hanno definito, ciascuna per sé, il concetto di disinformazione. Al riguardo cfr. S. SASSI, *Disinformazione ...*, cit., p. 34 ss. e M. MULLER, *Misinformation ...*, cit.

¹⁵ Commissione europea, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation ...*, cit.

¹⁶ Così Commissione europea nella sua comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final, Bruxelles, 26.4.2018, p. 4. Cfr. anche comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Piano d'azione contro la disinformazione*, JOIN(2018)36 final, Bruxelles, 5.12.2018, p. 1.

¹⁷ Come peraltro si può trarre dalla interpretazione congiunta di alcuni *considerando*, in particolare 2, 9, 69, 84 e 104 del regolamento UE 2022/2065 sui servizi digitali. Al riguardo v. par. 5 di questo saggio.

¹⁸ G. CERRINA FERONI, *Cosa fare contro la dittatura del pensiero dominante*, in www.garanteprivacy.it, 18.1.2023.

¹⁹ G. CERRINA FERONI, *op.cit.*

3. Linee di tendenza delle strategie giuridiche di contrasto alla disinformazione tra ordinamenti nazionali ed europeo

In concomitanza con una serie di eventi politici di notevole importanza in termini di dinamiche geopolitiche²⁰, Stati e organizzazioni di vario genere hanno iniziato ad agire contro la disinformazione con diversi approcci, riconducibili, in linea di massima, a due orientamenti: l'uno liberale, in certi casi quasi anomico, in quanto regolato dalla dialettica del dibattito²¹ e dal principio della irresponsabilità delle piattaforme digitali²²; l'altro dirigista, che ha trasformato la Rete in un ferreo sistema di controllo di ogni singolo cittadino²³.

L'ordinamento europeo, se da sempre ha marcato la distanza rispetto a questo ultimo, di recente si sta distinguendo anche nei confronti di quello prettamente liberale, in particolare quello statunitense²⁴. Questo atteggiamento è riscontrabile, in particolare, dal 2020, ovvero da quando l'Unione europea ha adottato una serie di misure che, per l'appunto, in questa sede qualificiamo di seconda generazione, giacché formalmente e sostanzialmente diverse rispetto a quelle assunte in precedenza. Preme, tuttavia, precisare che il cambio di marcia della UE non è nel suo approccio alla lotta alla disinformazione *on-line*; un approccio che non è punitivo²⁵ bensì di tutela – nel bilanciamento degli interessi – delle libertà garantite dalla Carta dei diritti fondamentali dell'UE, tra cui in particolare la libertà di espressione e di informazione (art. 11) e la libertà di impresa (art. 16). In più occasioni la Commissione europea ha ribadito che la disinformazione, sebbene dannosa, non debba essere categorizzata come una pratica dal contenuto necessariamente "illegale"²⁶. Ciò che sono mutati sono gli strumenti impiegati per combatterla. In altre parole, l'Unione Europea nel tempo, ha sviluppato – attraverso un dialogo strutturato tra le parti interessate, la Commissione e le altre autorità nazionali ed europee del settore, ai sensi dell'art. 11 del

²⁰ In ordine temporale: 2016: *referendum* sulla Brexit e elezioni presidenziali americane; 2017: elezioni presidenziali francesi e elezioni federali in Germania; 2019: elezioni europee.

²¹ Così Corte EDU: *Mehmet Hasan Altan v. Turkey*, n. 13237/17, 20 March 2018, § 210; *Sabin Alpay v. Turkey*, n. 16538/17, 20 March 2018, § 180.

²² Sul ruolo e sulla responsabilità dei servizi di intermediazione cfr. F. DONATI, *Il principio del pluralismo delle fonti informative al tempo di Internet*, in *Percorsi Cost.*, n. 1, 2014, p. 31 ss.; O. POLLICINO, *Tutela del pluralismo dell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi Cost.*, n. 1, 2014, p. 45 ss.; M. BETZU, *I baroni del digitale*, Editoriale Scientifica, Napoli, 2022.

²³ Al riguardo si rinvia a S. SASSI, *Disinformazione ...*, cit., p. 71.

²⁴ Governato ancora dalla *sect. 230 Communication Decency Act 1996* e dalla *sect. 512 Digital Millenium Copyright Act 1998*.

²⁵ La Commissione europea nella sua comunicazione del 25.6.2020 (*Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*, COM(2021) 262 final, p. 1) dichiara apertamente che l'approccio dell'ordinamento europeo alla lotta contro la disinformazione si caratterizza per tutelare la libertà di espressione e gli altri diritti di libertà garantiti dalla Carta UE e non già per «criminalizzare o vietare la disinformazione in quanto tale».

²⁶ Cfr. le comunicazioni della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Tackling COVID-19 disinformation – Getting the facts right*, Bruxelles, 10.6.2020, JOIN(2020)8 final, p. 4 e della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *sul piano d'azione per la democrazia europea*, Bruxelles, 3.12.2020, COM(2020) 790 final, p. 20. Di recente anche il reg. DSA ribadisce questo concetto, per la sua definizione v. nota 48.

TUE – un quadro comune di regole con l’obiettivo, da un lato, di rendere l’ecosistema digitale più sicuro e trasparente per garantire agli internauti un esercizio effettivo delle loro libertà, e, dall’altro, di responsabilizzare gli attori privati che in esso gravitano. Questa strategia, come vedremo qui di seguito, è stata attuata in origine con strumenti in prevalenza di *soft law*, fino a giungere alla adozione di misure sempre più *hard*.

4. Le misure dell’Unione europea

Il 2015 rappresenta la fase di inizio dell’avvio dell’Unione europea per contrastare il fenomeno della disinformazione.

4.1. ... di prima generazione: dal 2015

È da quella data infatti che l’Unione europea ha cominciato ad affrontare ufficialmente il problema della disinformazione. Da quando, in particolare, le campagne di disinformazione *online* condotte dalla Russia²⁷ si rivelavano sempre più pericolose. Al riguardo, embrionale è stato il lancio, da parte dell’Alto rappresentante per la politica estera, di una *task-force* (East StratCom) per le comunicazioni strategiche del servizio europeo per l’azione esterna (SEAE).

Tuttavia, è con la risoluzione del Parlamento europeo del giugno del 2017²⁸ che si è dato avvio a una serie di misure volte a contrastare il fenomeno in essere a tutela dei valori europei, impegnando una molteplicità di attori – statali e non, interni ed esterni alla stessa Unione – secondo un’intensa e stringente logica di cooperazione.

Alla fine del 2017, la Commissione europea inseriva la lotta alle *fake news on-line* tra le priorità del suo programma quadro²⁹ lanciando, da un lato, una consultazione pubblica su «notizie false e disinformazione on-line» e istituendo, dall’altro, un gruppo di esperti di alto livello per elaborare un sistema che bilanciassero

²⁷ Più precisamente nel marzo del 2015 il Consiglio europeo ha invitato l’Alto rappresentante per la politica estera e di sicurezza comune a elaborare un piano di azione per far fronte alle campagne di disinformazione condotte dalla Russia: <http://www.consilium.europa.eu/it/press/press-releases/2015/03/20/conclusions-european-council/>. A questo piano ha fatto seguito, nell’aprile del 2016, la comunicazione relativa al quadro congiunto per contrastare le minacce ibride che ha portato alla istituzione di due organi: 1) la cellula per l’analisi delle minacce ibride, nell’ambito del Servizio europeo per l’azione esterna, e 2) il centro europeo di eccellenza per la lotta contro le minacce ibride. Al riguardo v. Alto rappresentante dell’Unione europea, comunicazione congiunta al Parlamento europeo e al Consiglio, *Quadro congiunto per contrastare le minacce ibride. La risposta dell’Unione europea*, Bruxelles, 6.4.2016, JOIN(2016)18 *final*.

²⁸ Risoluzione del Parlamento europeo del 15 giugno 2017 «sulle piattaforme on-line e il mercato unico digitale» (2016/2276(INI)), n. 36. Con questa risoluzione il Parlamento europeo non solo condannava fermamente la diffusione di notizie false nell’ecosistema digitale ma sollecitava, da un lato, le piattaforme on-line a fornire agli utenti strumenti per denunciarle e, dall’altro, la Commissione europea a verificare la possibilità di un intervento legislativo per limitare la divulgazione di contenuti falsi.

²⁹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, «Commission Work Program 2018. An agenda for more united, stronger and more democratic Europe», Strasbourg 24.10.2017, COM(2017)650 *final*, p. 4.

il diritto dei cittadini di accedere a un'informazione di qualità con il diritto alla libertà di manifestazione del pensiero e al pluralismo dei media.

Il gruppo di esperti consegnava il suo rapporto nel marzo 2018³⁰. L'idea centrale era quella di creare un ecosistema digitale il più trasparente, affidabile e responsabile possibile³¹ in cui la società civile e il settore privato (in particolare le piattaforme *on-line* e i *media*) avrebbero dovuto svolgere un ruolo chiave. Il rapporto esortava a elaborare un codice di principi che le aziende digitali e i *social-network* avrebbero dovuto rispettare; a promuovere l'alfabetizzazione mediatica; a sviluppare strumenti che permettessero agli utenti e ai giornalisti di combattere la disinformazione e a difendere la diversità e la sostenibilità dei mezzi di informazione europei. Questa relazione del gruppo di esperti e il *forum multi-stakeholder* organizzato dalla Commissione europea nel maggio del 2018 costituivano le basi per la stesura in regime di auto-regolamentazione del «Codice di buone pratiche sulla disinformazione», pubblicato, poi, a fine settembre 2018. Nello stesso periodo, la Commissione lanciava una rete indipendente di verificatori dei fatti e una piattaforma *on-line* sulla disinformazione nonché misure volte a migliorare l'alfabetizzazione mediatica.

Peraltro, il succedersi, per un verso, di segnalazioni su diversi eventi distorti da campagne di disinformazione prodotte e/o diffuse da fonti esterne all'UE³², e l'imminenza, per altro verso, delle elezioni europee del 2019, nonché di oltre cinquanta elezioni presidenziali, nazionali o regionali/locali che avrebbero avuto luogo negli Stati membri entro il 2020, hanno reso necessaria l'attivazione di ulteriori azioni. Tra di esse, si ricorda il sistema di allarme rapido (*Rapid Alert System* – RAS) creato sulla base del «Piano d'azione contro la disinformazione»³³ al fine di rendere più agevole, tra l'Unione e gli Stati membri, lo scambio di informazioni e migliori prassi a sostegno della lotta contro le campagne di disinformazione

³⁰ Marzo 2018: <https://ec.europa/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

³¹ Relazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *sull'attuazione della comunicazione "Contrastare la disinformazione on-line: un approccio europeo"*, Bruxelles, 5.12.2018, COM(2018)794 *final*, p. 1.

³² Ci si riferisce, in particolare, alla disinformazione prodotta via *social network* nel caso Cambridge-Analytica, a quella diffusa da fonti russe nel contesto di alcune elezioni e alle interferenze generatesi in alcuni *referendum* svoltisi in Stati UE (al riguardo v. la relazione del Centro di analisi, previsioni e strategia (CAPS) e dell'istituto francese di ricerca strategica (IRSEM): http://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf); alle campagne di disinformazione sulla guerra in Siria (v. dichiarazione congiunta di 17 Paesi membri dell'Organizzazione per la proibizione delle armi chimiche (OPCW) sugli attacchi chimici a Duma: https://www.diplomatie.gouv.fr/en/french-foreign-policy/manipulation-of-information/article/syria-chemical-attacks-in-douma-7-april-joint-statement-by-france-and-16-other_rvb_cle838736) nonché sull'abbattimento di un aereo MH-17 nell'Ucraina orientale nonché sull'uso delle armi chimiche nell'attacco di Salisbury (cfr. i diversi articoli pubblicati dalla *task force* di comunicazione strategica per l'Est nel sito www.euvdisinfo.eu).

³³ Commissione europea - comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Piano d'azione contro la disinformazione ...*, *cit.*, p. 7 ss.

– attraverso ad es. il *micro-targeting* – per permettere alle rispettive istituzioni di condividere in tempo reale dati e analisi e valutare il contesto informativo³⁴.

L'infodemia generata intorno al Covid-19 ha poi accelerato il processo di rafforzamento dei meccanismi finora predisposti dall'ordinamento europeo³⁵. L'impulso ad affrontare con maggiore vigore e celerità questa sfida epocale – che, ricordiamo, ha investito il mondo intero³⁶ – è stato dato da una serie di iniziative politiche adottate in tempistiche molto ravvicinate tra loro. La prima è databile nel dicembre 2019, quando il Consiglio dell'Unione europea, sottolineando la necessità di conseguire *standard* più elevati di responsabilità, trasparenza e rendicontabilità da parte delle piattaforme *online* relativamente alla disinformazione, ha invitato la Commissione europea a «rafforzare maggiormente l'attuazione del Codice di buone pratiche»³⁷. Questa sollecitazione è stata poi riformulata nelle conclusioni del Consiglio europeo del 2020³⁸, in accoglimento della quale la Commissione ha elaborato nel maggio del 2021 gli «orientamenti sul rafforzamento del Codice di buone pratiche sulla disinformazione»³⁹. La successiva iniziativa politica è collocabile nel marzo del 2020, con la dichiarazione congiunta dei membri del Consiglio europeo⁴⁰; cui

³⁴ Più specificamente, con questo meccanismo si consente una conoscenza della situazione comune che permette un coordinamento efficace delle attività atte a individuare i responsabili della disinformazione e a formulare risposte adeguate, anche sotto il profilo delle tempistiche e delle risorse a disposizione. Peraltro di recente questo sistema, basato essenzialmente sulla condivisione di informazioni *open-source*, è stato rinvigorito, essendo stato impiegato anche per cooperare con *partner* internazionali, come il G7 e la Nato. E nel prossimo futuro non si esclude la possibilità di estendere questo tipo di cooperazione all'ONU e alle organizzazioni regionali, inclusi l'OCSE, il Consiglio d'Europa e l'Unione africana: Commissione europea, comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Tackling COVID-19 disinformation – Getting the facts right ...*, cit., p. 7-8.

³⁵ Al riguardo, icastiche sono le parole dell'Alto Rappresentante/Vicepresidente Josep Borrell: «La disinformazione ai tempi del coronavirus può uccidere. Abbiamo il dovere di proteggere i nostri cittadini rendendoli consapevoli della diffusione di informazioni false e denunciando i responsabili di tali pratiche. Nel mondo odierno, basato sulla tecnologia, nel quale i guerrieri si servono di tastiere anziché di spade e le operazioni di influenza e le campagne di disinformazione mirate sono un'arma riconosciuta di soggetti statali e non statali, l'Unione Europea sta intensificando le proprie attività e migliorando le proprie capacità per combattere questa battaglia». Così come quelle del Vicepresidente per i valori e la trasparenza, Věra Jourová: «Ondate di disinformazione hanno colpito l'Europa durante la pandemia di coronavirus, provenienti tanto dall'interno quanto dall'esterno dell'UE. Per lottare contro la disinformazione, dobbiamo mobilitare tutti i soggetti interessati, dalle piattaforme digitali alle autorità pubbliche, e sostenere i verificatori di fatti e i media indipendenti. Pur avendo intrapreso iniziative positive durante la pandemia, le piattaforme digitali devono intensificare i loro sforzi. Le nostre azioni hanno radici profonde nei diritti fondamentali, in particolare nella libertà di espressione e di informazione» (Comunicato stampa, *Coronavirus: azione rafforzata dell'UE contro la disinformazione*, 10.6.2020, Bruxelles).

³⁶ Come precisa A. VEDASCHI, *Il Covid-19, l'ultimo stress test per gli ordinamenti democratici: uno sguardo comparato*, in *dpce online*, vol. 43, n. 2, 2020, p. 1453: «[...] con la sola, ed invero marginale, eccezione dell'Antartide, tutti i continenti sono stati colpiti dalla [...] pandemia».

³⁷ In particolare il Consiglio dell'UE suggerisce che questa operazione doveva farsi alla luce delle informazioni e dei risultati raccolti dalla valutazione indipendente effettuata sul rispetto degli impegni sottoscritti dai firmatari del codice sulla disinformazione di buona pratiche del degli impegni sottoscritti da parte dei firmatari: v. Consiglio dell'Unione europea, *Sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride*, Bruxelles, 10.12.2019, 14972/19, p. 10.

³⁸ V. <https://www.consilium.europa.eu/media/47296/1011-11-20-euco-conclusions-en.pdf>.

³⁹ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione ...*, cit.

⁴⁰ v. *Joint statement of the Members of the European Council*, Brussels, 26 March 2020.

ha fatto seguito, il 10 giugno 2020, la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza ⁴¹ con la quale sono state gettate le basi per sviluppare – nel pieno rispetto dei diritti e delle libertà fondamentali sanciti dai Trattati e dalla Carta dei diritti fondamentali, nonché dalle norme nazionali e internazionali in materia di diritti – un quadro politico-normativo volto a intensificare gli sforzi dell'ordinamento europeo contro la disinformazione che, senza precedenti, si era sviluppata intorno al Covid-19. Con questa comunicazione l'Unione europea ha avocato a sé la cabina di regia per una complicata cooperazione tra più soggetti chiave – interni ed esterni alla stessa, tra cui non ultimi gli attori privati –, da condurre secondo una strategia modulare e sulla base del principio di trasparenza. Questo atto è interessante perché, tenendo conto dell'evoluzione delle minacce e delle manipolazioni, ha posto le basi per l'adozione nel dicembre 2020 del «piano d'azione per la democrazia europea» che ha prospettato una serie di soluzioni che configurano l'attuale nuova strategia giuridica della UE in materia di lotta alla disinformazione⁴².

4.2. ... di seconda generazione: dal 2020

Il 2020 si presenta come data di cesura tra un sistema costellato precipuamente da misure di iniziativa politica, o quanto meno *soft*, a uno che prevede una regolazione sempre più *hard* nella lotta contro la disinformazione, cercando, in particolare, di imporre alcuni obblighi di diligenza ai prestatori di servizi intermediari della società dell'informazione. Sotto questo profilo strumenti centrali sono indubbiamente: il codice rafforzato di buone pratiche sulla disinformazione (d'ora innanzi: codice rafforzato sulla disinformazione) e il regolamento UE 2022/2065 del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (c.d. *Digital Service Act*, d'ora innanzi: regolamento DSA). Entrambi adottati nel 2022⁴³.

4.2.1. Il codice rafforzato sulla disinformazione

Il codice rafforzato sulla disinformazione⁴⁴ sostituisce quello del 2018, con il quale l'Unione europea, per la prima volta, aveva definito una politica contro la disinformazione *online* da sviluppare, monitorare e

⁴¹ Comunicazione congiunta della Commissione europea e Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Tackling COVID-19 disinformation – Getting the facts right ...*, cit.

⁴² V. Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Bruxelles, COM(2020) 790 *final*, p. 24 ss. V. anche proposta della Commissione europea di un Regolamento del Parlamento europeo e del Consiglio *relativo a un mercato unico servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, Bruxelles, 15.12.2020, COM(2020) 825 *final*.

⁴³ Rispettivamente il 16 giugno e il 19 ottobre.

⁴⁴ Al riguardo cfr. i commenti di M. MONTI sui due testi: *Il Code of Practice on Disinformation dell'UE: tentativi in fieri di contrasto alle fake news*, e *Lo strengthened Code of Practice on Disinformation: un'altra pietra della nuova fortezza digitale europea?*, entrambi pubblicati in www.medialaws.eu, rispettivamente n. 1, 2019 e n. 2, 2022. V. anche A. KUCZERAWY,

attuare, per quanto possibile, per il tramite di una collaborazione strutturale tra aziende digitali e pubblicitarie, da un lato, e istituzioni e organismi europei, dall'altro. L'impianto di questo nuovo codice rimane pressoché invariato rispetto a quello precedente. I firmatari sono impegnati ad agire su più fronti: demonetizzando la diffusione della disinformazione; garantendo la trasparenza della pubblicità politica; responsabilizzando gli utenti; rafforzando la cooperazione con i verificatori dei fatti; fornendo un migliore accesso ai dati in loro possesso. Tra le novità sostanziali, previste per conferire maggiore trasparenza a un ecosistema da sempre opaco e governato da una asimmetria informativa, si ricordano: a) la creazione di una *task force* permanente – presieduta dalla Commissione europea e composta da alcuni *stakeholders* interessati e organismi europei⁴⁵ –, con il precipuo compito di rivedere e di adeguare gli impegni già presi in ragione dei probabili sviluppi tecnologici, sociali, di mercato e legislativi; b) l'istituzione di un centro di trasparenza, accessibile al pubblico, utile a fornire una soddisfacente conoscenza delle politiche dei fornitori dei servizi di intermediazione, della loro attuazione nonché di un aggiornamento costante di dati pertinenti. I firmatari si sono impegnati, poi, a concordare una concettualizzazione del “comportamento non autentico” e a stilare un elenco completo di tattiche, tecniche e procedure di manipolazioni non consentite sulle loro piattaforme, nonché una serie di azioni efficaci da intraprendere contro di esse. Il codice, infine, è anche stato dotato di un solido quadro di monitoraggio che prevede, tra le altre cose, meccanismi di valutazione – per il tramite di indicatori di prestazione (*Key Performance Indicators*) – capaci di misurare l'efficacia e l'adeguatezza delle iniziative delle piattaforme.

Tutte queste novità sostanziali hanno trasformato il codice nella sua natura giuridica: da strumento volontario posto in essere dai rappresentanti dell'industria tecnologica e pubblicitaria in regime di autoregolamentazione a strumento di co-regolamentazione, il cui funzionamento e la cui osservanza da parte dei firmatari sono soggetti al controllo della Commissione europea (art. 45, reg. DSA). E in questo mutamento della fonte è ravvisabile «la costruzione di un primo sistema di effettivo controllo sull'operato delle piattaforme, in una logica di tutela del discorso pubblico»⁴⁶. Un intendimento quest'ultimo che, a parere di chi scrive, trova più solida conferma negli strumenti di *hard law*, tra cui *in primis* il regolamento DSA.

Fighting on-line disinformation: did the EU Code of Practice forget about freedom of expression?, in E. KUZELEWSKA, G. TERZIS, D. TROTIER, D. KLOZA (ed.), *Disinformation and Digital Media as a Challenge for Democracy*, Intersentia, 2019, 8-9 e F. ZORZI GIUSTINIANI, *L'Unione europea e regolamentazione del digitale: il Digital Services Package e il Codice di buone pratiche sulla disinformazione*, in *Nomos*, n. 2, 2022.

⁴⁵ E cioè dai rappresentanti dell'industria tecnologica e pubblicitaria, dal gruppo dei regolatori europei per i servizi di media audiovisivi, dall'Osservatorio europeo dei media digitali e dal Servizio europeo per l'azione esterna.

⁴⁶ M. MONTI, *Lo strengthened Code of Practice on Disinformation ...*, cit., p. 319.

4.2.2. Il regolamento sui servizi digitali

Il regolamento DSA⁴⁷ è interessante sotto molteplici profili. Tra di essi due lo sono in particolare ai nostri fini. Il primo perché mette in discussione la neutralità della Rete. Il *considerando (1)* del DSA riconosce che la trasformazione digitale e l'impiego dei servizi che ne derivano possono essere forieri di una serie di rischi per i diritti fondamentali; e tra questi rischi, il *considerando (2)* del DSA annovera esplicitamente la disinformazione *online*. Il secondo profilo perché conferma l'approccio antropologico con cui l'ordinamento europeo affronta il tema delle tecnologie digitali. Sicché anche la regolamentazione sui servizi digitali è strutturata antepoendo la persona alla macchina (anche algoritmica), a tutela dei diritti e delle libertà fondamentali dell'uomo.

In un simile quadro, il regolamento sui servizi digitali persegue un obiettivo principale: responsabilizzare i prestatori dei servizi di intermediazione della società digitale⁴⁸, in modo proporzionale alla rispettiva capacità di *business*, dei contenuti non solo "illegali"⁴⁹ che corrono lungo le loro dorsali ma anche di quelli "legali", sebbene "dannosi", che possono avere un impatto negativo sui diritti fondamentali. In questa logica, il regolamento DSA impone a tutti questi soggetti una serie di doveri di diligenza in tema di moderazione dei contenuti⁵⁰; solo, invece, sulle piattaforme e motori di ricerca *online* di dimensioni molto grandi⁵¹ grava l'obbligo di gestire alcuni rischi sistemici, che possono ricorrere per una serie di motivi, come qui di seguito vedremo. Peraltro, il regolamento DSA prevede in caso di inosservanza di tutti questi doveri un sistema di *due process*.

⁴⁷ Per commenti al riguardo: R. BUCCA, M. SABATINI, *Digital Service Act, la UE a una svolta: cosa cambia per utenti, aziende e big tech*, in *Agenda Digitale*, 19.5.2022; F. ZORZI GIUSTINIANI, *L'Unione europea e regolamentazione del digitale ...*, cit.; C. HASSEN, C. PINELLI, *Disinformazione e democrazia ...*, cit., p. 125 ss.

⁴⁸ Ai sensi dell'art. 3, lett. g) rientrano in questa categoria i servizi di semplice trasporto (c.d. *mere conduit*), quelli di memorizzazione temporanea (c.d. *caching*), e i servizi di memorizzazione di informazioni (c.d. *hosting*).

⁴⁹ Che l'art. 3, lett. h) del reg. DSA definisce come «qualsiasi informazione che, di per sé o in relazione a una 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». Una definizione chiaramente ampia nel suo oggetto che il *considerando 12* DSA giustifica, da un lato, per conseguire «l'obiettivo di garantire un ambiente on-line sicuro, prevedibile e affidabile» e, dall'altro, per «comprendere anche le informazioni riguardanti i contenuti i prodotti, i servizi e le attività illegali». In estrema sintesi il contenuto illegale si manifesta con: il discorso di incitamento all'odio, contenuti terroristici, violazioni del copyright; il contenuto legale ma dannoso, invece, con: disinformazione, contenuti sensibili, contenuti di nudo, contenuti di gioco d'azzardo.

⁵⁰ L'art. 3, lett. t), reg. DSA, definisce la moderazione dei contenuti come «le attività, automatizzate o meno, svolte 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 adottate che incidono sulla disponibilità, sulla visibilità e sulla accessibilità di tali contenuti illegali o informazioni, quali la retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio».

⁵¹ Ai sensi dell'art. 33.1, DSA, una piattaforma o un motore di ricerca *online* è di dimensione molto grande quando ha «un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni».

a) la moderazione dei contenuti

L'art. 14.4 del reg. DSA⁵² prescrive a tutti i prestatori di servizi di intermediazione digitale⁵³ di moderare i contenuti «in modo diligente, obiettivo e proporzionato» parametrando ai diritti e le libertà come sanciti dalla Carta UE (art. 14.4, reg. DSA). Sicché, pur nel rispetto della loro libertà contrattuale, essi sono soggetti a una serie di doveri di diligenza. Anzitutto, sono sollecitati a codificare nelle loro condizioni generali⁵⁴ con linguaggio facilmente fruibile e specifico tutte le restrizioni che gli stessi impongono nell'uso dei loro servizi⁵⁵ (artt. 14-17 reg. DSA). Si impone, inoltre, di motivare in modo chiaro e specifico la restrizione da loro posta al contenuto “legale ma dannoso” diffuso utilizzando il rispettivo servizio (art. 17, reg. DSA). E infine, le piattaforme e i motori di ricerca *online* di dimensioni molto grandi devono prevedere sia un sistema interno in grado di gestire i reclami degli utenti contro le decisioni assunte dagli stessi (art. 20 reg. DSA) sia uno esterno. Con riguardo a quest'ultimo, si prescrive che la risoluzione della controversia sorta debba avvenire in via extragiudiziale, ad opera di un organismo certificato dal coordinatore dei servizi digitali di uno Stato membro (art. 21, reg. DSA). Se la decisione assunta da questo organismo è a favore del destinatario del servizio, il fornitore del servizio sostiene i costi del giudizio e rimborsa al destinatario le spese da esso sostenute; in caso inverso, ovvero se la controversia è risolta a favore della piattaforma *online*, il destinatario del servizio non è tenuto al rimborso dei diritti e delle altre spese sostenute dal prestatore del servizio, a meno che l'organismo di risoluzione extragiudiziale della controversia non ritenga che detto destinatario abbia agito manifestamente in mala fede.

b) la valutazione dei rischi sistemici

La gestione di alcuni “rischi sistemici”⁵⁶ derivanti dalla progettazione e dal funzionamento dei loro servizi e relativi sistemi (compresi quelli algoritmici), nonché dalla manipolazione e dall'uso intenzionali e talvolta

⁵² Cfr. anche i *considerando* 45, 47 e 48 del reg. DSA.

⁵³ Art. 14.1, reg. DSA. Il c. 5 dello stesso articolo prevede poi ulteriori obblighi per le piattaforme digitali di dimensioni molto grandi e i motori di ricerca online.

⁵⁴ Ai sensi dell'art. 3, lett. u, reg. DSA, 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».

⁵⁵ Che riguardano tra le altre cose «le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché le regole procedurali del loro sistema interno di gestione dei reclami».

⁵⁶ L'art. 34.1, classifica i rischi in quattro categorie, tenendo conto della loro gravità e della loro probabilità nel provocare danni. La prima riguarda i rischi associati alla diffusione di contenuti illegali (lett. a). La seconda concerne gli effetti reali o prevedibili del servizio sull'esercizio dei diritti fondamentali tutelati dalla Carta UE (lett. b). La terza attiene agli effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica (lett. c). La quarta categoria, infine, «deriva dalle preoccupazioni analoghe relative alla progettazione, al funzionamento o all'uso, anche mediante manipolazione, di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori e gravi conseguenze per il benessere fisico e mentale della persona o per la violenza di genere» (cfr. *considerando* 83, e art. 34.1, lett. c), reg. DSA).

coordinati dei loro servizi, o, infine, dalla violazione sistemica delle loro condizioni di servizio⁵⁷ è onere invece solo delle piattaforme e dei motori di ricerca *online* di dimensioni molto grandi.

Più specificamente, questi devono valutare il rischio in modo preciso e tenere conto della sua gravità anche in ragione delle probabilità di produrre effetti negativi, attuali o prevedibili, sull'esercizio dei diritti fondamentali, tra cui la libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sulla tutela della salute pubblica, sul dibattito civico, sui processi elettorali e sulla sicurezza pubblica (art. 34, c. 1, lett. b), c) e d), DSA).

Nel caso in cui i *social networks* o i motori di ricerca *online* di dimensioni molto grandi dovessero individuare uno dei sopra citati rischi, essi hanno l'obbligo di adottare una serie di misure che, in modo ragionevole, proporzionale ed efficace, possano attenuarli (art. 35, DSA). Tra gli strumenti proposti a tal fine vi sono quelli, ad esempio, di adeguare i sistemi di moderazione dei contenuti o di raccomandazione, ovvero i loro processi decisionali, le caratteristiche o il funzionamento dei loro servizi, o le loro condizioni generali, così come anche rafforzare i processi interni o di vigilanza sulle loro attività nel rilevamento di questi rischi.

Se poi si dovesse verificare una crisi di sistema⁵⁸ – ovvero quando «circostanze eccezionali [...] comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa» (art. 36, DSA) –, le piattaforme digitali e i motori di ricerca *online* di dimensioni molto grandi possono adottare in via di urgenza misure specifiche, valide per un periodo non superiore a tre mesi, al fine di prevenire, eliminare o calmierare in modo proporzionale ed efficace la situazione di crisi. Queste misure si attivano su richiesta della Commissione europea, sotto raccomandazione del comitato europeo per i servizi digitali. Tra le misure adottabili dal fornitore o dai fornitori destinatari della decisione della Commissione, il *considerando* (91) del DSA prevede: «l'adeguamento dei processi di moderazione dei contenuti e l'aumento delle risorse destinate alla moderazione dei contenuti, l'adeguamento delle condizioni generali, i sistemi algoritmici e i sistemi pubblicitari pertinenti, l'intensificazione della cooperazione con i segnalatori attendibili, l'adozione di misure di sensibilizzazione, la promozione di informazioni affidabili e l'adeguamento della progettazione delle loro interfacce online». Nel periodo in cui tali azioni sono attive tra la Commissione europea e il *provider* di riferimento sussisterà un dialogo aperto per una valutazione sostanziale, procedurale e temporale degli atti adottati.

⁵⁷ Cfr. *considerando* (84), e art. 34, reg. DSA.

⁵⁸ Il *considerando* (90) del DSA afferma che queste crisi possono derivare da «conflitti armati o atti di terrorismo, compresi conflitti armati o atti di terrorismo emergenti, catastrofi naturali quali terremoti e uragani, nonché pandemie e altri gravi minacce per la salute pubblica a carattere transfrontaliero».

La valutazione annuale del rispetto degli obblighi previsti dal regolamento *de quo* viene affidata ad *audit* esterni e indipendenti (art. 37, DSA) mentre uno o più responsabili nominati dalle stesse piattaforme si occupano della loro gestione (art. 43 e ss., DSA).

Numerosi altri obblighi sono posti a carico delle aziende tecnologiche di dimensioni molto grandi quanto alla condivisione dei loro dati e a una loro comunicazione trasparente; tra di essi l'art. 45 del regolamento DSA prevede l'elaborazione di codici di condotta per contribuire alla corretta applicazione del regolamento stesso.

5. Alcune osservazioni conclusive sulle ricadute applicative

Entro il 17 febbraio 2024 sia gli Stati membri UE sia i fornitori dei servizi di intermediazione della società dell'informazione⁵⁹, dovranno adeguarsi alle disposizioni di cui al regolamento DSA. Funzionerà? La domanda non è retorica, perché il cambio di paradigma, soprattutto per le piattaforme e motori di ricerca *online* di dimensioni molto grandi, è realisticamente significativo. Al punto che già uno di questi – Twitter, in particolare⁶⁰ – ha mostrato reticenze al rispetto di alcune sue norme.

Ma riavvolgiamo il nastro e cerchiamo di verificare quali potrebbero essere le ricadute di questa nuova regolamentazione sui Paesi UE e sui fornitori di servizi digitali, soprattutto quelli di dimensioni molto grandi, il cui scopo è «contribuire [a] corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta [...] siano tutelati in modo effettivo» (art. 1 reg. DSA).

In una simile logica apprezzabile è la volontà di rendere più chiari alcuni concetti attorno ai quali ruota l'intera disciplina, tra cui rileva anche il concetto di disinformazione. Al riguardo, pur in assenza di una definizione specifica, essa sembra configurarsi come una pratica che comporta un rischio sistemico «sulla

⁵⁹ Con specifico riguardo alle diverse scadenze che tutti questi soggetti devono osservare rispettivamente per adempiere a quanto statuito dal regolamento DSA v. A.T. MADIEGA, M. FRANCIOSI, *Digital Services Act: Application timeline*, EPRS, Bruxelles, November 2022.

⁶⁰ Come dichiarato Thierry Breton, commissario europeo per il mercato interno e i servizi, Twitter ha deciso di ritirarsi dal codice rafforzato sulla disinformazione, giacché – come ha sostenuto il suo proprietario, Elon Musk – sulla piattaforma corre «meno disinformazione» rispetto al passato, avendo creato un *team* dedicato a combattere le campagne di disinformazione coordinate. Secondo esperti ed *ex* dipendenti, invece, i licenziamenti selvaggi attuati dalla nuova dirigenza e le molteplici dimissioni da parte degli stessi lavoratori hanno comportato una ridotta capacità di moderazione dei contenuti di Twitter con il conseguenziale aumento di diffusione di disinformazione sulla stessa piattaforma. Di recente la BBC ha scoperto che centinaia di *account* di propaganda statale russa e cinese prosperano su Twitter. Innanzi a queste contrastanti posizioni, il commissario UE ha affermato che «Gli obblighi rimangono. Si può scappare ma non ci si può nascondere»; e «se (Elon Musk) non prende sul serio il codice, allora è meglio che se ne vada». Cfr: B. SIMONETTA, *La Ue avverte Musk: Twitter rispetti le regole o sarà vietato*, in www.ilsole24ore.it (30.11.2022); F. GILLET, *Twitter pulls out of voluntary EU disinformation code*, in www.bbc.com (27.5.2023). Al riguardo, preme sottolineare che le dichiarazioni di Breton sono tutte supportate da quanto previsto dall'art. 45.4 del reg. DSA, secondo cui: «In caso di inottemperanza sistematica ai codici di condotta, la Commissione e il comitato possono invitare i firmatari dei codici di condotta ad adottare le misure necessarie».

società e sulla democrazia» (*considerando* 104) derivante da un uso intenzionalmente improprio dei servizi di intermediazione delle società dell'informazione. La disinformazione, dunque – sulla scia di quanto affermato dal gruppo di esperti costituito dalla Commissione europea nel 2018⁶¹ –, non si identifica solo con le notizie false, ma anche con quelle diffuse in modo inesatto o fuorviante, e il suo contenuto non è “illegale” bensì “legale”, sebbene dannoso. In altre parole, la disinformazione è una strategia creata a tavolino che, avvalendosi anche di artifici tecnici propri delle nuove tecnologie digitali⁶², può provocare «effetti negativi [sui] diritti fondamentali, in particolare [sulla] dignità umana, [sulla] libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, [...] sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica, [sulla] protezione della salute pubblica [e sul] benessere fisico e mentale della persona» (art. 34.1, lett. b), c) d), reg. DSA).

Attorno a questo concetto gli Stati UE e le piattaforme e motori di ricerca *on-line* di dimensioni molto grandi, in particolare, devono confrontarsi per adeguarsi al nuovo quadro normativo delineato dal regolamento DSA.

a)... degli Stati membri UE

Con riguardo ai Paesi europei, preme chiarire fin da subito che l'operazione giuridica che in questa sede si vuole svolgere è rivolta solo all'ordinamento tedesco e a quello francese, in quanto, al momento, sono gli unici due Stati UE dotati di una legislazione *ad hoc*⁶³ sulla disinformazione⁶⁴.

Entrambi gli ordinamenti⁶⁵ inquadrano il fenomeno *de quo* in modo differente e per alcuni versi più circoscritto rispetto a quanto elaborato dalla UE. L'ordinamento tedesco individua la disinformazione quando il contenuto è "manifestamente illegale", laddove invece per l'Unione europea la disinformazione

⁶¹ V. par. 2, nota 15, di questo saggio.

⁶² Cioè per via di sistemi algoritmici, creazione di *bot*, e così via.

⁶³ La *Netzwerkdurchsetzungsgesetz* (di seguito: NetzDG), adottata il 1° settembre 2017, è stata adottata con l'obiettivo di combattere anche le *fake news online*. Ciò viene chiaramente affermato nelle motivazioni della NetzDG «Nach den Erfahrungen im US-Wahlkampf hat überdies auch in der Bundesrepublik Deutschland die Bekämpfung von strafbaren Falschnachrichten („Fake News“) in sozialen Netzwerken hohe Priorität gewonnen».

⁶⁴ La maggior parte dei Paesi UE impiega strumenti di *soft law* per gestire la disinformazione *online*. Cfr.: AA.VV., *Study for the “Assessment of the implementation of the Code of Practice on Disinformation” – Final Report*, Luxembourg 2020, p. 75 ss. ed European Parliament, *The Fight Against Disinformation and the Right to Freedom expression*, Bruxelles 2021, p. 62 ss. Quei pochi Paesi che hanno adottato misure di natura *hard* molte sono di natura penale. In linea di massima gli Stati affrontano ancora la diffusione di falsità, anche *online*, con le medesime leggi con cui vengono trattate la diffamazione, la frode, la pubblicità ingannevole e la falsa testimonianza. Per il caso italiano, v. M. MANETTI, *Freedom of Speech and the Regulation of Fake News*, in M. GRAZIADEI, M. TOSELLO (ed.), *Italian National Reports to the XXIst International Congress of Comparative Law*, ESI, Napoli, 2022, p. 417 ss.

⁶⁵ Per approfondimenti sulla legislazione tedesca e francese e cfr. T. GUERINI, *Fake News ...*, *cit.*, rispettivamente p. 79 ss. e p. 75 ss., S. SASSI, *Disinformazione ...*, *cit.*, rispettivamente p. 76 ss. e p. 86 ss.; ID., *Il contrasto alla disinformazione in Unione europea: una tutela per la tenuta della democrazia*, in A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze*, Napoli, 2022, rispettivamente p. 157 ss. e p. 162 ss.

ha contenuto “legale” ma dannoso. Il sistema francese inquadra questa categoria sulla base di una serie di criteri già stabiliti nella legge sulla libertà di stampa del 1881. Più specificamente l’art. 1 della loi n. 2018-1202⁶⁶ individua la manipolazione delle informazioni quando la notizia: 1) è palesemente falsa; 2) è diffusa in modo massiccio, artificiale o automatico; 3) mette in pericolo l’ordine pubblico o altri diritti individuali.

Quanto agli aspetti procedurali, in Germania la *Netzwerkdurchsetzungsgesetz* (di seguito: NetzDG), sembra essere stata in parte parametro di riferimento del regolamento DSA. Al pari di quanto previsto a livello europeo, anche questa legge responsabilizza in particolare le piattaforme digitali e i motori di ricerca di più grandi dimensioni⁶⁷. Tuttavia, essa differisce rispetto agli strumenti di contrasto. La NetzDG obbliga le *Big-Tech* a rimuovere o bloccare, entro ventiquattro ore dalla ricezione di un reclamo da parte di un utente, il contenuto “manifestamente illegale”. Se l’illegalità dei dati che circolano sulla rete è di dubbia interpretazione, la piattaforma digitale, prima di rimuoverli, dispone perlomeno di sette giorni per verificare e analizzare le informazioni. L’Unione europea solo a seguito di un *due process*⁶⁸ e solo in ultima istanza permette al prestatore del servizio di rimuovere il contenuto⁶⁹. Mentre con la Francia, le differenze si rilevano essenzialmente sotto due profili. Anzitutto, le norme sulla manipolazione delle informazioni si applicano solo in un dato temporale molto circoscritto, ovvero durante il periodo di campagna elettorale. In secondo luogo, si conferisce direttamente alla autorità giudiziaria il potere di ordinare entro 48 ore dal reclamo dell’utente la rimozione dei contenuti *online* ampiamente diffusi e ritenuti falsi.

Due, di contro, i tratti comuni sottesi alle discipline nazionali ed europea. Il primo è relativo alla richiesta ai servizi di intermediazione di dimensioni molto grandi di agire in modo trasparente. Per conseguenza, in linea di massima, e con le ovvie differenze del caso, queste legislazioni prevedono sistemi di segnalazioni interni, e qualsiasi decisione assunta in merito a un reclamo deve essere comunicata al reclamante e all’utente interessato senza ritardi ingiustificati. Si prevede inoltre che i prestatori dei servizi di intermediazione debbano pubblicare, con tempistiche scadenze, relazioni dettagliate che illustrino la gestione dei reclami ricevuti e le rispettive pratiche di moderazione. Il secondo elemento è dato dalla possibilità di comminare sanzioni pecuniarie proporzionali alla violazione commessa dal fornitore di servizi di intermediazione. Multa che: in Germania può essere disposta dall’autorità amministrativa competente fino a un importo massimo di cinque milioni di euro, con la possibilità di ricorrere al giudice

⁶⁶ Loi n. 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information. Il medesimo giorno, il Parlamento francese ha varato anche la relativa legge organica – Loi n. 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information – che estende le sue norme alle elezioni presidenziali.

⁶⁷ La cui dimensione viene quantificata nella soglia di utenti registrati dagli stessi utenti nel territorio tedesco, che non deve essere inferiore a due milioni (art. 1(2), NetzDG).

⁶⁸ Cfr. artt. 14 ss. e art. 49 ss., reg. DSA.

⁶⁹ Cfr. artt. 20 ss. e artt. 35 ss., reg. DSA.

competente, la cui sentenza vincola la stessa autorità amministrativa; in Francia, dall'autorità giudiziaria; e nell'ordinamento europeo, dalla Commissione europea (artt. 74 ss. reg. DSA) fino al 6% del fatturato globale dell'azienda digitale, cui è possibile ricorrere presso la Corte di Giustizia dell'Unione europea (artt. 81-82, reg. DSA).

Infine, la Francia, al pari della UE, e a differenza della Germania, prevede una autorità regolatoria⁷⁰ con poteri di vigilanza sull'operato delle piattaforme digitali e motori di ricerca *online*.

Più radicali, come vedremo qui in appresso, sembrano essere i cambiamenti cui dovranno attenersi i prestatori dei servizi intermediari.

b) ... delle piattaforme e dei motori di ricerca online di dimensioni molto grandi

Per capire la portata del paradigma cui sono costretti in particolare le piattaforme e motori di ricerca *online* di dimensioni molto grandi basti solo ricordare la libertà con cui da sempre hanno agito. Fin dai loro esordi, essi hanno avuto il potere di individuare quali contenuti caricare e quali condividere; quali contenuti potevano rimanere disponibili e quali rimossi; chi poteva partecipare e assistere alla conversazione *online* e chi doveva rimanere escluso. Ciò era, ed è, tecnicamente possibile perché ognuno dei *social media* si è dotato, nel tempo, di rispettivi termini e condizioni di servizio che definiscono in chiaro-oscuro le regole che gli utenti devono accettare per iscriversi ai relativi servizi. Sicché gli internauti possono rimanere nello spazio messo a loro disposizione e usufruire dei servizi offerti dai *social network* solo se rispettano gli *standard community* dagli stessi stabiliti autonomamente. I *social media*, soprattutto quelli di dimensioni molto grandi, hanno da sempre goduto di un indiscusso potere privato, giacché si pongono in una posizione di dominio rispetto agli individui. È il comitato direttivo delle aziende digitali che regola e decide in modo indipendente e massiccio i contenuti generati dagli internauti. Internauti che, ricordiamo, non hanno un benché minimo diritto di partecipare né alla loro elaborazione né al loro *enforcement*.

Ora, questa dimensione di esercizio di potere da parte di privati all'interno del loro spazio privato, che, in ragione delle loro decisioni sulla moderazione dei contenuti diffusi sulle loro piattaforme, influisce sullo spazio e sul dibattito pubblici, sulle scelte democratiche, sull'accesso alle informazioni e sulla libertà

⁷⁰ Trattasi dell'Autorità di regolazione della comunicazione audiovisiva e digitale (ARCOM), che subentra al *Conseil supérieur de l'audiovisuel*, alla quale l'articolo 12 *loi* n. 2018-1202 gli conferisce la possibilità di formulare raccomandazioni agli operatori delle piattaforme digitali sulla lotta alla diffusione di informazioni false. Riconosciuta è l'efficacia operativa del *Conseil supérieur de l'audiovisuel* nel combattere la diffusione di informazioni false per il tramite di servizi di media audiovisivi (al riguardo v. P. MOURON, *De la rumeur aux fausses informations. Remarques sur la proposition de la loi relative à la lutte contre la manipulation de l'information*, in *Légicom*, n. 60, 2019, in part. p. 14 ss.). Diversi sono stati gli avvisi o le sanzioni comminate dal *Conseil* contro i servizi che hanno trasmesso *fake news*. Peraltro la *Recommandation* n. 2019-03 *du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations*, ha adottato alcune misure simili a quelle previste dal Codice di buone pratiche europeo del 2018 e ha definito le condizioni per elaborare un meccanismo di segnalazione.

di espressione, sembra ridimensionarsi con l'entrata in vigore del regolamento DSA. Le intenzioni del DSA sono quelle di passare da un regime che esenta tutti questi soggetti da responsabilità a uno che li fa soggiacere a obblighi di diligenza. Sia di esempio la regolamentazione sulla gestione dei rischi sistemici che possono sorgere dall'impiego improprio dei servizi dei *social networks* e motori di ricerca *online* di dimensioni molto grandi. Essa comporta una disciplina che si sovrapporrà a quella adottata in regime di *self-regulation*. Un cambiamento che porta a una responsabilità della progettazione dei servizi, la cui inosservanza non comporta una responsabilità per l'azione degli utenti, bensì dei prestatori dei servizi di intermediazione. Peraltro il loro potere di decidere sull'applicazione e sull'osservanza delle restrizioni in relazione all'uso dei loro servizi deve d'ora innanzi parametrarsi al rispetto dei diritti fondamentali previsti dalla Carta dei diritti fondamentali dell'UE, da inserire nelle loro rispettive condizioni generali. In questo modo le eventuali restrizioni poste dai *social media* alla libera espressione nello spazio digitale saranno perlomeno adottate sulla base di regole certe, prevedibili e giustificate, ovvero sulla base dello Stato di diritto⁷¹.

In ragione di tutto ciò, l'ordinamento giuridico europeo, per il tramite di una regolamentazione organica, sta cercando di costruire un quadro comune di regole attorno alle quali si forza e si forgia una cooperazione leale tra i diversi attori (privati e/o pubblici che siano) capace di combattere la manipolazione delle informazioni a tutela della libertà di espressione e quindi a tutela dei valori democratici.

In altri termini, e al di là delle diverse difficoltà riscontrate, e che si produrranno, sembra che in materia si stia delineando a livello europeo un nuovo regime giuridico per le piattaforme digitali che ruota attorno ai principi di trasparenza, cooperazione e responsabilità.

L'idea che l'attuazione effettiva del principio per cui ciò che è legittimo nel mondo analogico deve esserlo anche in quello digitale, per un esercizio effettivo delle libertà democratiche in spazi i cui confini sono sempre più sfumati, sembra stia facendo cadere uno degli ultimi tabù, ossia che Internet debba essere esente da forme di regolamentazione. Soprattutto nel suo sillogismo tra democrazia e trasparenza. Laddove l'autorità pubblica pretende di monitorare il comportamento delle piattaforme digitali per conoscere i loro processi decisionali, sia nella fase ascendente che in quella discendente, per un duplice scopo. In primo luogo, perché ciò consente una valutazione accurata, tempestiva e completa dell'impatto delle azioni delle piattaforme. In secondo luogo, perché tutte queste informazioni possano essere diffuse agli utenti-interni in modo da garantire loro meccanismi di reclamo semplici, chiari e immediati e da rendere evidente agli stessi utenti-interni da quali inganni devono essere protetti.

⁷¹ Di recente sul tema v. T. FROSINI (a cura di), *Rule of Law come costituzionalismo*, il Mulino, Bologna, 2023.