*Costituzionalismo.it*

Fascicolo 2 | 2022

# Libertà d'informazione e piattaforme digitali. Questioni aperte nei Paesi liberal-democratici e considerazioni sulle "misure di guerra" nella Federazione russa

di Simona Piva

Editoriale Scientifica

# LIBERTÀ D'INFORMAZIONE E PIATTAFORME DIGITALI. QUESTIONI APERTE NEI PAESI LIBERAL-DEMOCRATICI E CONSIDERAZIONI SULLE "MISURE DI GUERRA" NELLA FEDERAZIONE RUSSA

*di Simona Piva*
Dottoranda di ricerca in Diritto amministrativo
Università degli Studi di Modena e Reggio Emilia



## 1. Introduzione

*Internet*, negli ultimi vent'anni, ha assunto un ruolo sempre più rilevante e ha determinato la creazione di un "nuovo mondo", quello della rete, utilizzata ormai da quasi il 60% della popolazione mondiale, che, attraverso di essa, ha la possibilità di accedere ad ogni tipo di contenuto.

Dal momento che la rete è diventata il principale mezzo di comunicazione di massa e, quindi, di scambio di informazioni e «poiché l'informazione è parte integrante dell'intera attività umana» e «il nuovo medium tecnologico incide profondamente su tutti i processi della nostra esistenza collettiva e individuale»[1] si può parlare del nostro tempo come della "*era dell'informazione*".

[1] M. Castells, *La nascita della società in rete*, Milano, 2008, p. 75; L. Flori-

Col passare degli anni l'uso di *Internet* si è tanto diffuso che per molti individui una parte rilevante della loro vita privata, oltre che di quella lavorativa, si è trasferita in rete come evidenziato, già qualche anno fa, da un *report* dell'AGCOM[2].

Certamente *Internet* offre grandi opportunità da molti punti di vista, ad esempio, quello economico e quello socio-politico, nel quale i *social media* e i *social network*[3] facilitano le interazioni sociali tra gli individui e «la partecipazione dei cittadini alla società e alla democrazia»[4].

Anche durante il *lockdown*, che le autorità hanno imposto a causa della pandemia da Covid-19, *Internet* ha mostrato il suo grande potenziale, dal momento che, a seguito dell'obbligo di distanziamento, solo grazie alle piattaforme digitali e alla «capacità delle nuove tecnologie di ricreare uno spazio virtuale»[5] è stato possibile mantenere in essere tutta una serie di attività essenziali ed esercitare alcuni diritti di rilevanza costituzionale[6], tanto che ne è uscita notevolmente rafforzata la tesi di

---

DI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017. Sull'impatto dei *Big Data* sulla nostra vita, v. M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019; V.M. SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013.

[2] AGCOM, *Servizio economico-statistico, Big data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*.

[3] I termini *social media* e *social network* indicano rispettivamente le piattaforme per la diffusione delle informazioni e le piattaforme per comunicare gli uni con gli altri: P. MCMILLAN, *What's the difference between social media and social networking?*, in *SearchUnifiedCommunications*, 1 dicembre 2011.

[4] Comunicazione della Commissione Europea COM(2016) 288 *final* del 25 maggio 2016, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*, p. 3.

[5] Sul punto, v. P. STANZIONE, *Introduzione*, in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 3.

[6] Per citarne alcuni: il diritto al lavoro attraverso lo *smart working*, il diritto di libera manifestazione del pensiero, il diritto all'istruzione attraverso la Dad e il diritto ad avere rapporti sociali. Per quanto concerne il diritto di manifestazione del pensiero, art. 21 Cost., ormai è dato per scontato che esso sia costituito da tre fondamentali diritti: di informare, di essere informati e di non essere disinformati. A riprova dell'importanza attribuita dalle Autorità europee e nazionali al fenomeno estremamente pericoloso e pervasivo della disinformazione, v. *The Strengthened Code of Practice on Disinformation*, 16 giugno 2022, sottoscritto dalle principali piattaforme digitali e punto di arrivo di una lunga serie di prese di posizione della Commissione europea sul tema, che nel termine *disinformation* «*include misinformation, disinformation, in-*

coloro che da tempo sostengono che il diritto di accesso ad *Internet* sia un diritto fondamentale degli individui[7].

La necessità di riconoscere tale diritto è dovuta anche al fatto che

> «lo sviluppo tecnologico di questi ultimi anni sta cambiando le nostre società in maniera tanto profonda che la posizione sociale di una persona è definita anche (e non in misura trascurabile) dalle possibilità che questa ha di accedere alle nuove tecnologie e dalle competenze che ha per utilizzarle. Una tale constatazione conduce a ritenere che, nel ragionare di una società inclusiva e libera dalle discriminazioni, un aspetto su cui è opportuno soffermarsi attiene proprio all'accesso alle nuove tecnologie»[8].

L'accesso ad *Internet* è, infatti, funzionale all'uguaglianza sostanziale degli individui dal momento che favorisce «la partecipazione at-

---

*formation influence operations and foreign interference in the information space*» (I. *Preamble* (a)); AGCOM, *Rapporto tecnico. Le strategie di disinformazione online e la filiera dei contenuti fake*, 9 novembre 2018.

Per interessanti considerazioni sulla disinformazione in generale, v. A. Nicita, *Il mercato delle verità. Come la disinformazione minaccia la democrazia*, Bologna, 2021, pp. 217-225; C. O'Connor, J.O. Weatherall, *L'era della disinformazione. Come si diffondono le false credenze*, Milano, 2019.

[7] Sul diritto di accesso a *Internet* come diritto sociale, v. P. Passaglia, *L'accesso a Internet è un diritto (il Conseil Constitutionnel francese dichiara l'incostituzionalità di parte della c.d. "legge anti file-sharing")*, in *Il Foro Italiano*, 2009, IV, pp. 473 ss.; R. Pisa, *L'accesso ad internet, un nuovo diritto umano fondamentale?*, in *Treccani giuridica*, 7 gennaio 2010; T.E. Frosini, *Il diritto costituzionale di accesso ad Internet*, in *Rivista AIC*, n. 1/2011, pp. 1-17; G. De Minico, *Diritti Regole Internet*, in *Costituzionalismo.it*, n. 2/2011, ora in *Id.*, *Antiche libertà e nuova frontiera digitale*, Torino, 2016, pp. 43-63; S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, pp. 384 ss.; M. Pietrangelo, *Accesso ad Internet, diritto ancora diseguale? Aggiornamenti e ripensamenti*, in M.R. Allegri e G. D'Ippolito (a cura di), *Accesso ad Internet e neutralità della Rete fra principi costituzionali e regole europee*, Roma, 2017, pp. 25 ss.; D. Sassoli, *Il diritto al web sia una battaglia europea*, in *Repubblica.it*, 19 luglio 2020; A. Archer, N. Wildman, *Internet Access as an Essential Social Good*, in E. Aarts, H. Fleuren, M. Sitskoorn e T. Wilthagen (a cura di), *The new common*, 2021, pp. 29 ss. e, infine, gli scritti di G. De Minico, *Fundamental rights, European digital regulation and algorithmic challenge*; P. Tanzarella, *L'accesso a Internet è fondamentale, ma è davvero un diritto (fondamentale)?*; M.R. Allegri, *Il diritto di accesso a Internet: profili costituzionali*; A.M. Gambino, R. Giarda, *L'accesso ad Internet come diritto*, contenuti nella sezione monografica *Il diritto di accesso a Internet*, a cura di G. D'Ippolito, in *MediaLaws.eu*, n. 1/2021.

[8] P. Passaglia, *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni*, in *MediaLaws.eu*, n. 3/2021, p.1.

tiva dei cittadini alla società dell'informazione e [...] agendo da leva atta a sollevare gli ostacoli materiali ed economici al pieno sviluppo della persona, diventa l'occasione per l'effettivo esercizio delle libertà fondamentali – manifestazione del pensiero, comunicazione intersoggettiva – alle quali taluni, gravati dalle preoccupazioni del vivere quotidiano, sono spesso costretti a rinunciare»[9].

Inoltre, il riconoscere come un diritto la possibilità dell'accesso ad *Internet* implica in primo luogo il superamento del *digital divide*, che, causato dalla diversità del contesto socio-economico di partenza degli individui, si traduce in una diversa possibilità di utilizzo delle tecnologie *ICT* con significative conseguenze a livello conoscitivo e socio-economico.

Poiché, come abbiamo sottolineato, «l'accesso a *Internet* è diventato, per milioni di cittadini, parte integrante e condizione di esercizio di numerosi diritti e libertà di valore costituzionale»[10], il riconoscimento di questo diritto è stato ribadito nel corso degli anni da diverse fonti[11].

---

[9] G. De Minico, *Diritti Regole Internet*, cit., p. 2.

[10] T.E. Frosini, *op. cit*., p. 13.

[11] Sul punto, a livello nazionale, è opportuno ricordare che il diritto di accesso a *Internet*, che era stato autorevolmente propugnato da Stefano Rodotà, che, in un *Forum*, tenuto nel 2010, aveva proposto d'inserire il diritto di accesso a *Internet* all'interno dell'articolo 21 della Costituzione, in virtù anche del principio di uguaglianza contenuto nell'art. 3 Cost., è stato oggetto di una *Dichiarazione dei diritti in Internet* elaborata dalla Camera dei Deputati nel 2015. Tale documento, nei primi due commi dell'art. 2, dispone che «1. L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. 2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale».

A livello sovranazionale, è importante, innanzitutto, richiamare la *Declaration of Internet Freedom* del 1° luglio 2012, dichiarazione *online*, firmata da numerose organizzazioni, tra cui *Amnesty International*, e anche da singoli individui, che riconosce il diritto di accesso ad *Internet* e la libertà di espressione *online* come diritti umani fondamentali. A questa Dichiarazione ha aderito il Consiglio per i diritti umani delle Nazioni Unite con la Risoluzione del 5 luglio 2012. Qualche mese dopo, l'Unione europea, richiamandola espressamente, con la Risoluzione del Parlamento europeo dell'11 dicembre 2012, *Una strategia di libertà digitale nella politica estera dell'Ue (2012/2094(INI))*, ha affermato, in particolare, col Considerando B «che Internet è un elemento fondamentale per garantire l'accesso alle informazioni, la libertà di espressione, di stampa, di riunione e lo sviluppo economico, sociale, politico e culturale». In seguito, col Regolamento UE 2015/2120, l'UE ha sancito che il diritto ad *Internet* è un diritto fondamentale e il Considerando n. 1 dispone, segnatamente, che il testo di legge si pone l'obiettivo di «definire norme comuni per garantire un trattamento equo e non

Tuttavia, nonostante i suoi numerosi aspetti positivi, *Internet*, specialmente nel corso degli ultimi anni, ha mostrato, dal momento che espone gli internetnauti a rischi non irrilevanti, anche aspetti negativi. Tali negatività riguardano, in modo particolare, l'utilizzo da parte delle piattaforme dei dati di coloro che navigano in *Internet*, come, ad esempio, il trattamento dei dati personali[12] degli utenti, che sono raccolti e elaborati attraverso complessi, sofisticati e poco trasparenti algoritmi[13] per ottenere nuove informazioni che possono essere da esse utilizzate anche per finalità non legittime[14], i dati visti come «un asset di note-

discriminatorio del traffico nella fornitura di servizi di accesso a Internet e tutelare i relativi diritti degli utenti finali [...] e a garantire al contempo il funzionamento ininterrotto dell'ecosistema di Internet quale volano per l'innovazione». Per un corretto inquadramento delle fonti e del loro valore giuridico, v., per il diritto dell'Unione europea, G. Gaja, A. Adinolfi, *Introduzione al diritto dell'Unione europea*, Roma-Bari, 2013, per quello internazionale, v. A. Gioia, *Diritto internazionale*, Milano, 2019.

[12] Per dato personale si deve intendere «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»: art. 4, par. 1, n. 1 del GDPR.

[13] Sull'importanza degli algoritmi è stato osservato che «l'ascesa delle piattaforme digitali è stata sostenuta dalla raccolta e dallo sfruttamento dei dati mediato dalla elaborazione da parte degli algoritmi che ne costituiscono e incrementano il valore. L'inarrestabile pervasività dei dati e dei meccanismi che li analizzano e li elaborano quali gli algoritmi ci mettono di fronte al fatto che i modi di acquisizione e gestione dei dati, nonché la loro natura e qualità, costituiscono un tema cruciale»: A. Ammannati, *I 'signori' nell'era dell'algoritmo*, in Diritto pubblico, fasc. 2/2021, p. 382.

[14] Sulla protezione dei dati personali, v. il *Regolamento UE 2016/679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (Regolamento generale sulla protezione dei dati), entrato in vigore il 25 maggio 2018. Sul Regolamento, cfr. P. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali, Il Regolamento europeo 2016/679*, II, Torino, 2016; L. Bolognini, E. Pelino, G. Bistolfi, *Il Regolamento Privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati in vigore da maggio 2016*, Milano, 2016; G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati personali*, in *Nuove leggi civ. comm.*, 2017; F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, pp. 369 ss.; J. Monducci, *La tutela della privacy alla luce del Regolamento (UE) 2016/679*, in C. Di Cocco, G. Sartor, *Temi di diritto dell'informatica*, Torino, 2017, p. 119 ss.; L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e*

vole valore economico»[15] di cui appropriarsi, da parte dei gestori delle grandi piattaforme, nelle mani dei quali si concentra un enorme potere economico[16] «con rischi anche per il mercato e la concorrenza»[17], l'impatto dei *Big Data* sulla *privacy* degli individui[18] e la manipolazione

*valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[15] M. Midiri, *Trasformazione digitale e riorganizzazione dei servizi pubblici alla luce del PNRR*, in *Studi parlamentari e di politica costituzionale*, vol. 54, n. 209/2021, p. 90. A proposito del valore dei dati, che sono stati definiti nel 2006 da Clive Humby «il nuovo petrolio», è stato osservato che «nell'ecosistema digitale i 'dati' rappresentano una essenziale fonte di ricchezza. Ma una fonte altrettanto importante è rappresentata dai 'profili', cioè dalle 'identità' di consumatori e utenti che gli algoritmi elaborano»: L. Ammannati, *La circolazione dei dati: dal consumo alla produzione*, in L. Ammannati, A. Canepa, G.L. Greco e U. Minneci (a cura di), *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione*, Torino, 2021, p. 145.

[16] [16] Sul potere dei "giganti del *tech*", tra cui si distinguono *Google*, *Apple*, *Facebook*, *Amazon* e *Microsoft*, conosciuti con l'acronimo *GAFAM*, v. E. Morozov, *Silicon Valley: i signori del silicio*, Torino, 2016; S. Galloway, *The Four: the hidden DNA of Amazon, Apple, Facebook and Google*, London, 2017; F. Foer, *I nuovi poteri forti – Come Google, Apple, Facebook e Amazon pensano per noi*, Milano, 2017.

[17] M. Midiri, *Trasformazione digitale e riorganizzazione dei servizi pubblici alla luce del PNRR*, cit., p. 88; *Id.*, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant, in* Federalismi.it, n. 14/2020*; Id., Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Il diritto dell'informazione e dell'informatica,* vol. 37, fasc. 2/2021, pp. 111 ss., pp. 112-113. In quest'ultimo articolo, l'Autore osserva che tra le cause che generano effetti anticoncorrenziali si possono indicare «la pluralità dei servizi offerti e l'attendibilità delle predizioni sulle preferenze degli utenti elaborate dalle piattaforme determinano "la formazione di avvolgenti 'ecosistemi digitali'"», che si basano su strategie di *lock-in*, da cui gli utenti faticano ad uscire, che possono produrre «esiti anticoncorrenziali, con riduzione della qualità dei servizi offerti ed esclusione dei concorrenti per effetto di blocco determinato dalle esternalità di rete»; H. Varian, M. Dolmans, G. Baird, *Digital challenges for competition policy*, *sept* 2018, in ec.europa.eu; J. Crémer, Y.A. De Montjoye, H. Schweitzer, *Competition Policy for the Digital Era*, Luxembourg, 2019; G. Colangelo, *Big data, piattaforme digitali e antitrust*, in Mercato Concorrenza Regole, fasc. 3/2016, pp. 425 ss.

[18] Sul punto, v. A. Montelero, *La privacy all'epoca dei big data*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 1181 ss.; M. Orefice, *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018; I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning*?, in *International Data Privacy Law*, n. 3/2013, pp. 74-87; A.M. Froomkin, *The Death of Privacy?*, in Stanford Law Review, vol. 52, n. 5/2000, pp. 1461-1545. Sull'impatto dei *Big Data* sulla tutela dei dati personali, v., anche, Consiglio d'Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasburgo, 2017.

dell'informazione attuata sui *social*, attraverso sofisticate tecniche di disinformazione, che lede la libertà di pensiero[19].

Su quest'ultimo punto, già nel decennio scorso, si è rilevata, a causa delle tecniche di disinformazione, delle *fake news* e della *post-truth*, l'emersione «del lato problematico di *Internet* e in particolare dei *social media*»[20], che ha ridimensionato l'iniziale clima di grande ottimismo nei confronti delle potenzialità di *Internet* anche in campo socio-politico. Ad esempio, nel caso delle "rivoluzioni colorate" o delle "primavere arabe"[21] si pensava che *Internet* potesse essere un mezzo in grado di favorire il processo democratico nei Paesi autoritari o, addirittura, di rovesciare i Governi non liberali (*cyber*-utopismo), speranza che si è dimostrata nella quasi totalità dei casi infondata, dal momento che quegli stessi Stati hanno utilizzato, oltre i tradizionali mezzi repressivi, anche la tecnologia informatica per combattere, neutralizzare e soffocare il dissenso interno[22]. Ma non solo: sta gradualmente entrando in crisi anche l'idea di *Internet* come architettura globale e aperta, in grado di realizzare le «magnifiche sorti e progressive» dell'umanità di leopardiana memoria e di essere l'asse portante della sostenibilità globale come affermato nella delibera del 27 giugno 2016 dello *Human Rights Council* dell'Assemblea Generale delle Nazioni Unite, trentaduesima sessione, che al punto n. 2 riconosce «*the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms, including in achieving the Sustainable Development Goals*»[23].

---

[19] J. Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, in *Fordham Law Review*, vol. 80, issue 4/2012, pp. 1525 ss.; K. Klonic, *The New Governors: The People, Rules, and processes Governing Online Speech*, in *Harvard law Review*, vol. 131, n. 6/2017, pp. 1598 ss.

[20] P. Costanzo, *La «democrazia digitale» (precauzioni per l'uso)*, in *Diritto pubblico*, fasc. 1/2019, pp. 71 ss., pp. 85-86.

[21] A questo proposito si possono ricordare "le rivoluzioni colorate" scoppiate negli anni 2000 nei territori prima appartenenti all'ex Urss ("la rivoluzione delle rose" in Georgia, quella "arancione" in Ucraina nel 2004/2005 e quella "dei tulipani" in Kirghizistan nel 2005), "le primavere arabe" del 2011 e le manifestazioni pro-europee del 2013/14, denominate *Euromaidan*, in Ucraina.

[22] A. Kendall-Taylor, E. Frantz, J. Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, in *Foreign Affair*, marzo/aprile, 2020.

[23] A/HRC/32/L.20, consultabile in undocs.org. Anche la Commissione europea ritiene che *Internet* sia uno strumento per favorire la sostenibilità sociale ed ambientale. Tale profilo è enunciato in numerosi documenti della stessa Commissione, come, ad esempio, il pacchetto di iniziative per l'attuazione del *Green Deal* europeo, in *europa.eu*.

Questa visione di un *Internet* globale e aperto, in grado di contribuire ad uno sviluppo sostenibile nelle sue varie forme, è stata ed è messa in crisi da scenari culturali e geopolitici globali che, nel corso degli anni e negli ultimi mesi, a causa del conflitto russo-ucraino, si sono e si stanno delineando sempre più e che hanno incrinato l'idea di un unico *Internet*, dando vita alla sua frammentazione, determinando, in questo modo, un *vulnus* di tutela della libertà di informare e di essere informati.

A riprova della crisi di *Internet* quale *open global society*, l'Unione europea, gli Stati Uniti, numerosi altri Paesi e diversi *partners* internazionali hanno proposto la *Declaration for the Future of the Internet*[24].

La Dichiarazione, dopo avere sottolineato la natura "rivoluzionaria" di *Internet*, come infrastruttura dalle rilevanti implicazioni, e riconosciuto la sua valenza "politica", punta il dito sul lato oscuro della rete e in particolare sull'"autoritarismo digitale", che, a causa di sofisticate campagne di disinformazione, pregiudica alcuni diritti fondamentali degli individui.

Da ciò discende, per la Dichiarazione, la necessità di intensificare, a livello globale, la cooperazione fra i Paesi firmatari per assicurare l'esistenza di un ambiente digitale inclusivo, aperto e sicuro, in contrapposizione alla tendenza registrata negli Stati autoritari, alcuni dei quali veramente di grande peso dal punto di vista geopolitico ed economico, in cui si attua la censura dei contenuti *online* ostili alla classe politica al potere regolamentando in maniera autoritaria la libertà di informazione e di parola, e si propende alla balcanizzazione della rete per isolarli dal *global free Internet*.

In sostanza, la Dichiarazione propone di continuare a mantenere in vita un *Internet* aperto, gratuito, globale, interoperabile, affidabile e sicuro, al fine di garantire sia lo sviluppo sostenibile della Rete che la protezione delle libertà fondamentali e dei diritti degli utenti[25], tra cui quella di potere accedere al "libero flusso delle informazioni" nell'ambito di un sistema aperto, ma, come vedremo, si può affermare che siamo in presenza, anche se per motivi diversi, di una "crisi" di *Internet* sia nei Paesi liberal-democratici che nei Paesi autoritari.

---

[24] *Declaration for the Future of the Internet*, 28 aprile 2022, tale dichiarazione fa seguito alla *Declaration on European Digital Rights and Principles*, 26 gennaio 2022.

[25] Sul tema della protezione dei diritti degli individui di fronte alla "censura privata" operata dalle piattaforme digitali, v. O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Oxford, 2021.

Nei Paesi liberal-democratici, tale crisi è determinata, in particolare, dalla manipolazione della libertà di informazione, che ha assunto un significativo "peso" negativo nel sistema informativo, tanto che si è ritenuto necessario, specie nell'Unione europea, passare dalla auto-regolamentazione delle piattaforme alla co-regolamentazione, per meglio tutelare i diritti fondamentali degli utenti europei.

Per quanto riguarda i Paesi non liberali, i loro Governi utilizzano la tecnologia informatica per rendere difficoltoso o addirittura, in qualche caso, impossibile ai loro cittadini accedere all'*Internet* globale ed entrare in contatto con idee diverse ed alternative alla narrazione *mainstream* al fine di impedire la loro diffusione e la possibile nascita o il rafforzamento del dissenso interno[26].

## 2. La manipolazione della libertà di informazione attraverso *Internet* nei Paesi liberal-democratici

La manipolazione della libertà di informazione è dovuta al fatto che i *social media* e i *social network* possono essere veicoli non solo di informazione, ma anche di disinformazione e di manipolazione al fine di influenzare e polarizzare l'opinione pubblica attraverso strategie «spesso alimentate da temi divisivi e da campagne di discriminazione o da espressioni d'odio (*hate speech*) nei confronti di gruppi o categorie di persone»[27].

Le piattaforme attraverso gli algoritmi[28] dei motori di ricerca elaborano grandi quantità di dati (*Big data*[29]), sia quelli che coloro che na-

[26] A. Kendall-Taylor, E. Frantz, J. Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, cit.

[27] M. Delmastro, A. Nicita, *op. cit*., p. 21. Per un approfondimento sugli *hate speech*, v. O. Pollicino, G. De Gregorio, *Hate speech, una prospettiva di diritto costituzionale comparato*, in Giornale di Diritto amministrativo, fasc. 4/2019, pp. 421-436; S. Sica, G. Giannone Codiglione (a cura di), *Security and Hate Speech. Personal Safety and Data Security: Rights in The Age of Social Media*, Bologna, 2019.

[28] Il potere degli algoritmi è tale che già dieci anni fa si è argomentato di "dittatura dell'algoritmo": S. Rodotà, *op. cit*., pp. 398 ss., mentre un altro Autore ha definito la società del nostro tempo «*Algorithmic Society*»: J.M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in U. C. Davis L. Rev., n. 51/2017-2018, pp. 1149 ss.

[29] I *Big Data*, in una prima accezione, sono quei dati che gli utenti immettono all'interno delle piattaforme *online* per poter usufruire dei servizi e dei beni offerti e

vigano sul *Web* lasciano volontariamente o involontariamente in rete[30], sia i dati dei dispositivi in relazione con gli utenti stessi[31], e, utilizzando la tecnica del *micro-targeting*, racchiudono ogni singolo utente in una "*filter bubble*"[32], elaborata in base agli interessi mostrati durante le sue precedenti navigazioni sul *Web*, «per cui, essendo esposte a contenuti selezionati, le persone hanno una percezione limitata, che è diversa dalla realtà»[33].

Tale tecnica, "confezionando" messaggi *ad hoc* sui vari destinatari, li espone a opinioni simili alle loro, che confermano quello che già pensano, sfruttando il fatto che quasi tutti gli individui, quando devono fare una scelta, tendono a privilegiare le informazioni in linea con le loro idee e ad evitare quelle che non lo sono[34], dal momento che «il

che transitano attraverso *Internet*, formando quella che è stata definita *datasphere*. In una seconda accezione, il termine è utilizzato in riferimento alla capacità di analizzare, per i più diversi fini, una massa di dati eterogenei, strutturati e non strutturati, attraverso sofisticati algoritmi. In particolare, si parla di *Big Data* nella prima accezione quando si ha una mole dei dati nell'ordine degli *zettabyte*, ovvero miliardi di *terabyte*. Per avere un'idea approssimativa della quantità di dati contenuti in uno *zettabyte* è stato affermato che uno «zettabyte corrisponde a una capacità di archiviazione pari a oltre 36.000 anni (in termini di durata) di video in HD ovvero una pila composta da 250 miliardi di DVD»: AGCOM, *Big data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 7.

[30] Frank Pasquale afferma che tutto ciò che facciamo *online* è tracciato e che il regime di "sorveglianza" sul *Web* per ragioni di sicurezza o per altri motivi è costante: F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard, 2015; S. Zuboff, *Il capitalismo della sorveglianza*, Roma, 2019. Tale situazione, a causa del fatto che, nell'epoca di *Internet*, la Rete conosce tutto di noi, ha portato ad affermare che «l'analogico, carta e penna, nell'era digitale, è l'unica cassaforte inviolabile»: J. D'Alessandro, *La rete sa tutto di te*, in *La Repubblica Scienze Tecnologia*, 12 settembre 2019, pp. 2-3.

[31] È stato osservato che anche l'*Internet* delle cose (*Internet of Things* (*IoT*)) determina un «flusso crescente di informazioni sulle persone che hanno rapporti con tali oggetti. Gli oggetti anzi "dialogano" tra loro, per accrescere e aggiornare continuamente i dati riguardanti le persone e per trasferirli ad apparati che, a loro volta, li elaborano e ne traggono conclusioni riguardanti la persona interessata»: S. Rodotà, *op. cit*., p. 322.

[32] Per il significato della locuzione *filter bubble*, cfr. E. Pariser, *The Filter Bubble. What The Internet Is Hiding From You*, London, 2011.

[33] S. Quintarelli, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Torino, 2019, p. 89. L'algoritmo dà agli individui, attraverso la profilazione, una «presentazione del reale modellata […] secondo la categoria (di consumatore, utente, elettore) cui esso ritenga di ascrivere il soggetto»: P. Stanzione, *op. cit*., p. 4.

[34] Questa tendenza è denominata *biased assimilation*, cfr. G.D. Hooke Pear-

fenomeno dell'*echo chamber* in cui vive il singolo utente lo porta ad accogliere senza spirito critico e a credere per vere le notizie che sono coerenti con i suoi pregiudizi»[35].

Poiché, col fenomeno appena citato, «l'informazione tendenzialmente viene adottata solo se è aderente al sistema di credenze già strutturato di un individuo»[36], ciò determina una «crescente polarizzazione delle opinioni in rete, che non ci aiuta a confrontarci con chi ha identità o posizioni diverse dalla nostra [ ]. Il risultato è una crescente autoreferenzialità dei processi di formazione dell'opinione pubblica via web»[37] e per questo «internet continua ad essere per molti un terreno fertile per l'estremismo»[38].

Inoltre le strategie di *micro-targeting*, tese alla disinformazione e alla manipolazione degli individui, ricorrono anche alle *fake news*[39],

---

son, S. Knobloch-Westerwick, *Is the Confirmation Bias Bubble Larger Online? Pre-Election Confirmation Bias in Selective Exposure to Online versus Print Political Information*, in Mass Communication and Society, n. 4, 2019, p. 467; A. Peruzzi, F. Zollo, A.L. Schmidt, W. Quattrociocchi, *From Confirmation Bias to Echo-Chambers: a data-driven approach*, in Sociologia e Politiche Sociali, n. 3/2018, p. 72.

[35] G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in G. Pitruzzella, O. Pollicino, S. Quintarelli, *Parole e potere, Libertà di espressione, hate speech e fake news*, Milano, 2017, p. 72. A questo proposito, Antonio Nicita parla di *assimilation bias* in quanto, quando ci troviamo davanti a nuove informazioni, accettiamo quelle che confermano ciò che già pensiamo e rigettiamo quelle che non sono in linea con esse, determinando una sorta di «solitudine cognitiva e autoreferenziale, chiamata non a caso echo chambers», che tende ad espandersi sempre più nell'era della comunicazione digitale: A. Nicita, *op. cit*., p. 96; v., anche, V. Visco Comandini, *Le fake news sui social network: un'analisi economica,* in MediaLaws.eu, n. 2/2018, pp. 191 ss.

[36] W. Quattrociocchi, A. Vicini, *Misinformation. Guida alla società dell'informazione e della credulità*, Milano, 2016, p. 50. Sulle *echo chambers*, cfr. C.R. Sunstein, *#Republic. La democrazia nell'epoca dei social media*, Bologna, 2017, pp. 39 ss.

[37] M. Calise, F. Musella, *Il Principe digitale,* Bari-Roma, 2019, p.11.

[38] C.R. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni*, Bologna, 2003, p. 87, in *Id.*, *The law of group polarization*, in Journal of political philosophy, vol. 10, n. 2/2002, pp. 175-195.

[39] Il termine, coniato nel 2016 da Sharyl Attkisson, racchiude sia il tipo di contenuto (falso) che la modalità attraverso cui esso raggiunge i destinatari (la rete). Tuttavia, è opportuno puntualizzare che «le fake news possono nascere ed essere propagate su uno qualsiasi dei vettori di informazione, da Internet, alla radio, alla televisione o alla carta stampata e riverberare diffondendosi sugli altri»: S. Quintarelli, *Content moderation: i rimedi tecnici*, in G. Pitruzzella, O. Pollicino, S. Quintarelli, *Parole e potere, Libertà di espressione, hate speech e fake news*, cit., p. 100. Sul tema delle

che «non hanno niente a che vedere con le opinioni, ma sono delle vere e proprie menzogne»[40], per modificare o radicare ancora di più il pensiero delle persone.

Tale prassi, poiché contribuisce a polarizzare gli individui, ostacola il pluralismo informativo[41], che costituisce un elemento essenziale della comunicazione in una società democratica[42], impedendo il *free marketplace of ideas*, in base al quale dovrebbe emergere l'opinione migliore, e lo sostituisce col mercato delle verità in cui viene a mancare il confronto aperto e ogni gruppo pensa di essere portatore della verità che cerca di imporre agli altri[43].

La polarizzazione degli individui è un fenomeno particolarmente pericoloso come è stato ed è possibile vedere nei Paesi liberal-democratici sia in occasione della pandemia da Covid-19 che della guerra russo-ucraina in quanto l'opinione pubblica si è divisa in due fazioni contrapposte.

Nei due casi appena richiamati si è innescato un "paradigma binario"[44] in cui anche le autorità pubbliche, invece di incoraggiare «il dibattito e la trasparenza nelle decisioni pubbliche», hanno assunto il ruolo di portatrici di una verità ufficiale da opporre a coloro che sollevavano e sollevano critiche nei confronti della stessa, impedendo il pluralismo informativo di cui gli individui hanno bisogno per arrivare a conoscere i fatti.

Questo orientamento si inserisce in un *trend* che caratterizza dall'inizio di questo secolo anche i Paesi occidentali, dove si è registrata in maniera sistematica da parte dei Governi un'espansione dei sistemi di

---

*fake news,* v. P. Passaglia, *Fake news e fake democracy: una convergenza da scongiurare*, in Federalismi.it, n. 11/2020, pp. 126 ss.; E. Lehner, *Fake news e democrazia*, in MediaLaws.eu, n. 1/2019; V. Visco Comandini, *op. cit.*; F. Pizzetti, *Fake news e allarme sociale: responsabilità, non censura*, in MediaLaws.eu, n. 1/2017; AGCOM, *News vs. fake nel sistema dell'informazione – Interim report nell'ambito dell'Indagine conoscitiva su Piattaforme digitali e sistema dell'informazione,* delibera n. 309/16/CONS, 2018.

[40] G. Pitruzzella, *La libertà di informazione nell'era di Internet*, cit., p. 72.

[41] R. Borrello, *Alcune riflessioni preliminari (e provvisorie) sui rapporti tra i motori di ricerca ed il pluralismo informativo*, in MediaLaws.eu, n. 1/2017, pp. 74 ss.

[42] «La democrazia deve essere il regime della verità, nel senso della piena possibilità della conoscenza dei fatti da parte di tutti»: S. Rodotà, *op. cit*., p. 224.

[43] A. Nicita, *op. cit*., pp.189 ss.

[44] N. Urbinati, *La guerra guerreggiata della logica binaria*, in Domani.it, 5 marzo 2022.

sorveglianza, in particolare dopo gli attacchi terroristici dell'11 settembre 2001 alle Torri gemelle del *World Trade* Center e al Pentagono, per motivi di sicurezza nazionale[45] o, negli ultimi anni, a causa dello scoppio della pandemia da Covid-19, di salute pubblica, determinando spesso, come già accennato, una significativa contrazione del pluralismo informativo e gravi ripercussioni sull'effettivo esercizio dei diritti fondamentali da parte degli individui.

## 3. Dalla *self-regulation* delle piattaforme alla *co-regulation*: la svolta del legislatore europeo con il *Digital Service Act*

In questo paragrafo verrà preso in considerazione come, da un punto di vista diacronico, è stato affrontato il problema della regolamentazione delle piattaforme nei Paesi liberal-democratici e, in particolare, nell'Unione europea.

A differenza dei Paesi illiberali, come si vedrà nella seconda parte dell'articolo, in cui i diritti delle persone non sono garantiti, il principio dello Stato di diritto costituisce «il principio strutturale forse maggiormente significativo, caratterizzante ed identificante l'Unione come comunità di diritto»[46], e, pertanto, il legislatore europeo si è posto e si pone con grande sensibilità il problema della tutela dei diritti degli utenti di *Internet*.

Come osservato, tra le grandi questioni dibattute nel nostro tempo c'è quella del ruolo centrale che le piattaforme digitali hanno progressivamente assunto nelle nostre società[47] sotto molti punti di vista, tra cui quello economico.

---

[45] Sul tema dell'inasprimento della sorveglianza da parte degli Stati liberal-democratici (in particolare degli Stati Uniti d'America) dopo gli attentati appena richiamati, v. D. Lyon, *Surveillance After September 11*, Cambridge, 2003; K. Ball, F. Webster (a cura di), *Crime, Terrorism and Warfare in the Information Age*, London, 2003; T. Monahan (a cura di), *Surveillance and Security: Technological Politics and Power*, in *Everyday Life*, New York, 2006.

[46] E. Gianfrancesco, *Un approccio costituzionalistico alla Commissione europea. Alcuni profili rilevanti*, in *Diritto e Società*, n. 1/2021, p. 4.

[47] L'importanza delle piattaforme al giorno d'oggi è tale che «una delle tante definizioni della società attuale è quella di "società delle piattaforme". Pur con tutti i limiti propri di ogni generalizzazione, tra le tante proposte questa è quella che coglie, più di ogni altra, un dato caratterizzante il contesto attuale: la centralità del potere assunto dalle piattaforme, in un ambito che non si limita più soltanto al mercato ma investe,

Il potere economico degli "*over the top*", ossia dei giganti tecnologici USA, la cui ricchezza è superiore a quella del PIL di molti Paesi, è tale che essi si sono attribuiti il ruolo di *gatekeeper* che dettano le regole del mercato, ne orientano le dinamiche e controllano l'accesso al mercato stesso alle aziende concorrenti a danno della concorrenza.

Le grandi multinazionali *tech*, in virtù del loro peso economico e della loro prassi monopolista, esercitano, come le grandi industrie tradizionali, ma in misura ancora maggiore, anche una notevole influenza sociale e politica dal momento che sono in grado di orientare «le forme e i modi del dibattito pubblico online»[48] e di fare pressioni sui Governi dei Paesi in cui operano per indirizzare la legislazione a favore dei loro interessi specifici.

In questo modo i *Tech Giant* spesso riescono a "frenare" i tentativi degli organismi *antitrust* di regolare e perseguire le distorsioni concorrenziali da essi poste in essere a scapito della concorrenza, dei consumatori, dell'innovazione.

Un altro punto di vista è quello, molto importante ai fini del nostro discorso e su cui ci soffermeremo più a lungo, che riguarda la libertà di parola e il pluralismo dell'informazione, che sono l'essenza della coesistenza civile in una società democratica[49], minacciata dall'*hate speech* e dalle *fake news*, che costituiscono un aspetto fondamentale della disinformazione[50] e sono spesso «intrinsecamente politiche nei loro effetti e nelle loro intenzioni»[51].

Visto che i messaggi, che vengono pubblicati in rete, possono contenere discorsi d'odio o avere l'obiettivo di disinformare gli utenti, le piattaforme *online* per ovviare a tali aspetti negativi si sono autolegitti-

più in generale, i diritti civili, sociali e politici»: P. Stanzione, *op. cit.,* p. 1; B. Obama, *Disinformation is a threat to our Democracy. Tech platforms need to recognize that their decisions have an impact on every aspect of society*, discorso tenuto il 22 aprile 2022 all'Università di Standford; A. Canepa, *I mercanti dell'era digitale. Un contributo allo studio delle piattaforme,* Torino, 2020.

[48] M. Delmastro, A. Nicita, *op. cit*., p. 49.

[49] R. Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered?*, in MediaLaws.eu, n. 1/2022, pp. 2-4.

[50] C. Pinelli, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in Diritto pubblico, fasc. 1/2022; C. O'Connor, J.O. Weatherall, *L'era della disinformazione Come si diffondono le false credenze*, Milano, 2019; AGCOM, *Rapporto tecnico. Le strategie di disinformazione online e la filiera dei contenuti falsi*, 9 novembre 2018.

[51] A. Nicita, *op. cit.,* p. 7.

mate a tutelare le libertà di espressione e di informazione, sindacando in maniera autonoma i contenuti sui loro *social* attraverso *policy* di autoregolamentazione, dando così vita al fenomeno della c.d. "privatizzazione della giustizia digitale"[52].

In questo modo le piattaforme digitali, incentivate dal fatto che all'inizio della loro diffusione si era pensato di demandare ad esse il compito di valutare ed eventualmente bannare i contenuti inappropriati postati dagli internetnauti sui *social network*, si sono attribuite poteri censori, che hanno determinato la comparsa di nuovi poteri privati relativi alla censura sulla rete, che tendenzialmente hanno cercato di sostituirsi ai poteri pubblici.

Il fatto che le piattaforme abbiano pensato, attraverso le loro *policies*, di poter riservare a se stesse la moderazione dei contenuti denota l'importanza e il potere che hanno acquisito nel nostro tempo[53], ma ciò ha determinato spesso problemi, dovuti alla poca trasparenza e alla discrezionalità della loro azione, che hanno dato adito a numerose critiche[54] a volte fondate, a volte no.

---

[52] O. Pollicino, *Facebook e il pericoloso passo in avanti verso la privatizzazione della giustizia digitale*, in *Diritto e web*, 18 settembre 2019. Sui problemi dovuti alla autoregolazione delle piattaforme, v. F. Donati, *Verso una nuova regolazione delle piattaforme digitali*, in *Rivista della regolazione dei mercati*, fasc. 2/2021; L. Ammannati, *Per una "nuova" regolazione delle piattaforme digitali*, in L. Ammannati e A. Canepa (a cura di), *Tech law: il diritto di fronte alle nuove tecnologie*, Napoli, 2021; G. D'Acquisto, *Nuove tecnologie e regolamentazione: storia di una convivenza necessaria*, in L. Ammannati e A. Canepa (a cura), *Tech law: il diritto di fronte alle nuove tecnologie*, cit.; M. Manetti, *Regolare Internet*, in *MediaLaws.eu*, 2, 2020; G. De Gregorio, *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *MediaLaws.eu*, n. 1/2017, p. 97; F. Cafaggi, *New Foundations of Transnational Private Regulation*, in E. Palmerini e E. Stradella (a cura di), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, 2013.

[53] Come è stato sottolineato dal Presidente dell'Autorità garante per la protezione dei dati personali quando afferma che «Il ruolo centrale assunto dalle piattaforme nel sistema attuale (emerso in maniera deflagrante con la sospensione degli account Facebook e Twitter di Donald Trump sino al termine del mandato, a seguito dell'assalto al Congresso), è tale da configurarle quali veri e propri poteri privati»: P. Stanzione, *op. cit*., p.1. Sul punto, è stato giustamente osservato che i giganti digitali «tendono a produrre 'in proprio' le regole essenziali del loro funzionamento»: L. Ammannati, *I 'signori' nell'era dell'algoritmo*, cit., p. 385.

[54] Per evitare le critiche sollevate nel caso di rimozione o di non rimozione di contenuti dal *social* («Sappiamo che non sempre abbiamo ragione quando decidiamo di rimuovere o lasciare pubblicato un contenuto su Facebook»), *Facebook* ha costitu-

Non poche volte, infatti, esse sono intervenute per limitare o rimuovere dalla rete contenuti ritenuti pericolosi, ma che in realtà non lo erano, per attuare il cosiddetto *deplatforming* degli *account* non solo di persone comuni, ma, anche, di personaggi pubblici importanti, come nel caso dell'*ex* Presidente degli Stati Uniti, Donald Trump, dopo l'assalto, il 6 gennaio 2021, a *Capitol Hill*[55], o di Associazioni politiche come CasaPound e Forza Nuova[56].

La discrezionalità delle piattaforme nella moderazione dei contenuti è emersa in maniera eclatante anche nel caso, che presenta aspetti quantomeno dubbi, come vedremo nel paragrafo 5.1, in cui *Meta* ha deciso, contrariamente a quanto previsto dalla sua *policy*, di consentire

ito un *Indipendent Oversight Board* (Comitato per il controllo). *L'Oversight Board* è un organismo paragiurisdizionale costituito da esperti indipendenti di tutto il mondo, che ha il compito di riesaminare *ex post* le decisioni più difficili e più importanti di rimozione o di non rimozione dal *social* di casi segnalati dagli utenti e decidere sulla loro correttezza. È possibile ricorrere al Comitato *versus* due tipi di decisioni di *Facebook*: se un utente non concorda con la rimozione di un suo contenuto dal *social* o se un utente ha segnalato a *Facebook* (e *Instagram*) contenuti che, a suo parere, dovevano essere rimossi ma che non lo sono stati. È importante sottolineare l'importanza riconosciuta all'*Oversight Board* dal momento che «la risoluzione del comitato di ogni caso sarà vincolante e *Facebook* la attuerà tempestivamente, a meno che l'attuazione di una risoluzione possa violare la legge»: art. 4 dello Statuto. Sull'*Oversight Board*, v. L. Ammannati, *I 'signori' nell'era dell'algoritmo*, cit., p. 408; A. Iannotti della Valle, *La giurisdizione privata nel mondo digitale al tempo della crisi della sovranità: il 'modello' dell'Oversight Board di Facebook*, in Federalismi.it, n. 26/2021, pp. 153-164; R. Natoli, *Il diritto privato regolatorio*, in *Rivista della Regolazione dei Mercati*, 2020 (1), p. 143. Sulla privatizzazione della censura in generale, v. 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, fasc. 1/2019.

[55] L'assalto a *Capitol Hill* a causa della sua gravità è stato definito «il giorno più cupo della democrazia americana»: A. Nicita, *op. cit*., p. 43.

[56] G. Pitruzzella, *Fake news e odio in rete. Dopo il caso Facebook-CasaPound*, in Il Foglio, 22 settembre 2019; C. Melzi D'Eril, G.E. Vigevani, *Odio in rete e rimozione della pagine Facebook: giudice che vai, soluzione che trovi*, in *Il Sole 24 Ore*, 27 febbraio 2020; C. Caruso, *La libertà di espressione presa sul serio. Casa Pound c. Facebook, atto I*, in SidiBlog, 20 gennaio 2020; P. De Sena, M. Castellaneta, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, in SidiBlog, 20 gennaio 2020; P. Villaschi, *La (non) regolamentazione dei social network e del web,* in M. D'Amico e C. Siccardi (a cura di), *La Costituzione non odia. Conoscere, prevenire e contrastare l'hate speech on line*, Torino, 2021, pp. 113-126. Resta qui aperta la questione, che si ritiene comunque di richiamare, se la regolazione giuridica – per quanto ben calibrata – possa effettivamente frenare le tendenze profonde alla polarizzazione dell'opinione pubblica.

agli utenti dei suoi due *social network* di postare discorsi d'odio quando sono indirizzati verso gli invasori russi e i loro sostenitori.

Il tentativo delle piattaforme, che sono di proprietà privata, di riservare a sé stesse funzioni para-giurisdizionali ha sollevato fin dall'inizio «un problema nella misura in cui grava soggetti privati, orientati verso finalità di business, del compito di assicurare il bilanciamento tra interessi di segno diverso, generalmente affidato alle autorità giurisdizionali»[57].

Di conseguenza, a livello di Unione europea, si è cercato di passare dalla autoregolamentazione delle piattaforme alla co-regolamentazione, attraverso strumenti di *soft law*, con il primo *Code of Conduct on countering illegal hate speech online*, che è stato adottato nel 2016 dalla Commissione Europea insieme ai principali *network: Facebook*, *Microsoft, Twitter* e *YouTube*, ai quali si sono aggiunti successivamente *Instagram, Google*, *Snapchat*, *Dailymotion* e *jeuxvideo.com*, e che affida ai *social* stessi il compito di rimuovere i discorsi d'odio diffusi *online* dai loro utenti.

In seguito, nel 2018, le principali piattaforme digitali hanno sottoscritto il *EU Code of Practice on Disinformation*[58], che, elaborato insieme agli organi politici dell'Unione europea, assegna loro il compito di rimuovere i contenuti ingannevoli o fuorvianti e prevede la figura dei *fact-checkers*, il cui compito è quello di verificare le informazioni che sono postate sui *social*, dal momento che, nel caso delle *fake news* e dell'*hate speech*, il problema principale è quello «di asseverare la correttezza o meno di un contenuto»[59].

Nello stesso tempo, in modo crescente, si è fatta strada, a livello europeo, l'«esigenza di normare, circoscrivendoli, i poteri sempre più estesi delle piattaforme, ascrivendo loro corrispondenti responsabilità

[57] O. Pollicino, *La prospettiva sulla libertà di espressione nell'era di Internet*, in G. Pitruzzella, O. Pollicino, S. Quintarelli, *Parole e potere, Libertà di espressione, hate speech e fake news*, cit., p. 45; G.L. Conti, *Manifestazione del pensiero attraverso la Rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?,* in Rivista AIC, n. 4/2018, pp. 200 ss.; A. Ciancio, *La libertà di informazione, internet ed il terrorismo internazionale*, in Federalismi.it, n. 12/2015, pp. 5 ss.

[58] Sul *Code*, v. G. Pagano, *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in Federalismi.it, n. 11/2019; M. Monti, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in Federalismi.it, n. 11/2020.

[59] S. Quintarelli, *Content moderation: i rimedi tecnici*, cit., p. 100.

funzionali alla garanzia dei diritti fondamentali incisi, in varia misura, dalla loro azione»[60], attraverso una regolamentazione specifica per le piattaforme digitali valida per tutti gli Stati membri dell'Unione europea.

In questo quadro si sono inserite le due iniziative presentate nel dicembre del 2020 dalla Commissione europea[61]: il *Digital Services Act* e il *Digital Markets Act*[62], previsti nell'ambito della strategia digitale europea, *Shaping Europe's Digital Future*, con l'obiettivo di migliorare la normazione sui servizi digitali nell'UE in attuazione del piano, più generale, d'azione per la democrazia europea (*European Democracy Action Plan*).

La proposta di regolamento relativo a un Mercato unico dei servizi digitali (*Digital Services Act*), presentata dalla Commissione, è stata approvata con alcune modifiche e integrazioni del testo a seguito dell'accordo, in data il 23 aprile 2022, tra il Consiglio e il Parlamento europeo, e la votazione della Plenaria del Parlamento europeo del 5 luglio 2022[63].

---

[60] P. Stanzione, *op. cit*., p. 2.

[61] Sul potere di iniziativa legislativa della Commissione europea, v. E. Gianfrancesco, *La Commissione nel quadro istituzionale dell'Unione: una ricognizione*, in *Forum di Quaderni Costituzionali*, n. 9/2012, pp. 14-20.

[62] G. D'Agostino *Le piattaforme digitali come nuove forme di mercato. Alcune considerazioni in merito ai profili economico-giuridici alla luce del processo normativo in UE,* in L. Ammannati, A. Canepa, G.L. Greco e U. Minneci (a cura di), *Algoritmi, Big Data, piattaforme digitali*, cit., pp. 119-133; M. Leistner, *The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital services Act – A critical primer*, pp. 3-4. Il *Digital Market Act*, che tratta, in funzione *antitrust*, le tematiche come l'abuso di posizione dominante e la pratica di attività anticoncorrenziali da parte delle grandi multinazionali digitali, è stato approvato in via definitiva il 24 Marzo 2022.

[63] Il *DSA* entrerà in vigore 20 giorni dopo la sua pubblicazione nella Gazzetta ufficiale europea e sarà applicato 15 mesi dopo. Ma, per quanto riguarda le piattaforme e i motori di ricerca *online* molto grandi, il *DSA* sarà applicato da una data precedente, ovvero quattro mesi dopo che le *very large online platforms* (*VLOPs*) saranno individuate. L'Unione Europea riconosce molta importanza all'approvazione del *DSA*, tanto che la Presidente della Commissione Europea, Ursula von der Leyen, ha scritto su *Twitter*, il 23 aprile, che «*Today's agreement on #DSA is historic. Our new rules will protect users online, ensure freedom of expression and opportunities for businesses. What is illegal offline will effectively be illegal online in the EU. A strong signal for people, business & countries worldwide*». Da richiamare, anche, quanto deciso dal Consiglio europeo, che, «nel contesto dell'aggressione Russa in Ucraina e delle particolari conseguenze sulla manipolazione delle informazioni online», ha introdotto nel DSA

Il legislatore europeo col *Digital Service Act*, riconoscendo il ruolo strategico e centrale delle piattaforme *online* nell'informare i cittadini e nel contribuire a dar vita alla formazione di un dibattito pluralista, ma allo stesso tempo consapevole dei rischi in merito all'*hate speech* e alle pratiche di disinformazione mediante le *fake news* che possono essere diffuse sul *Web*, si pone l'obiettivo di «stabilire regole uniformi per un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta siano effettivamente protetti».

A tal fine esso tende opportunamente a chiarire e rafforzare gli obblighi delle piattaforme digitali in tema di contenuti illegali, che, però, non specifica[64], lasciando alle autorità giudiziarie o amministrative nazionali, il compito di individuarli, «a seconda dell'ordinamento giuridico di ciascuno Stato membro»[65], e di attivarsi per la loro rimozione[66], introducendo regole e procedure, che prevedono sia il ricorso a sistemi di intelligenza artificiale sia al controllo umano, di contrasto ai contenuti illegali *online* per evitare che gli utenti siano esposti a contenuti che li racchiudano in *filter bubbles* ostacolando il libero mercato delle idee.

Inoltre, dal momento che il *DSA* ritiene che gli utenti *internet* debbano avere un maggior controllo della dimensione digitale[67], esso pre-

un nuovo articolo al fine di istituire un meccanismo di reazione in caso di crisi» per consentire l'adozione di misure "proporzionate ed efficaci" nei confronti delle *very large online platforms*, che diffondono disinformazione. Non essendo possibile in questa sede un compiuto approfondimento del DSA, si vedano comunque, i seguenti documenti e articoli consultabili in *consilium.europa.eu*, *ec.europa.eu*, *garanteprivacy.it*, *agendadigitale.eu*, *infondata.ilsole24ore.com*.

[64] A. Nicita, *op. cit*., p. 233: la «decisione della Commissione di non proporre una regolamentazione diretta dei contenuti illegali non sorprende. Come i legislatori degli Stati membri essa si è trovata di fronte alla difficoltà, da un lato, di definire più dettagliatamente le fattispecie, dall'altro, di non limitare la libertà di espressione, e alla fine la scelta è stata di non intervenire sul punto».

[65] Considerando n. 29 del *DSA*.

[66] La Commissione europea per contrastare la disinformazione *online* ha redatto due importanti documenti: la Comunicazione *Contrastare la disinformazione online: un approccio europeo, COM(2018) 236 final* del 26 aprile 2018 e la *Relazione della Commissione sull'attuazione della comunicazione "Contrastare la disinformazione online: un approccio europeo", COM(2018) 794 final* del 5 dicembre 2018.

[67] Il *DSA* istituisce un meccanismo c.d. "*notice and action*", che riguarda le segnalazioni, da parte degli utenti dei *social*, dei contenuti illegali *online*, che devono essere trattate dalle piattaforme in modo non discriminatorio e nel rispetto dei diritti fondamentali, compresa la libertà di espressione, che rappresenta uno degli aspetti più difficili da bilanciare in vista di una possibile rimozione.

vede che le piattaforme tengano in debito conto le segnalazioni degli utenti, così come include la possibilità per gli utenti di appellarsi contro le rimozioni decise dalle piattaforme qualora le ritengano ingiustificate, «con possibile gravame davanti ad un organismo imparziale per la risoluzione extragiudiziale delle controversie»[68] e di ottenere un risarcimento nel caso di violazioni delle norme da parte delle piattaforme nei loro confronti.

Il DSA stabilisce, in particolare, che le *very large online platforms*[69], come *Google* e *Facebook*, siano soggette a specifici e più severi obblighi di controllo e moderazione dei contenuti, a causa dei peculiari rischi che si presentano in ragione della loro grande diffusione, partendo dal principio che «maggiori sono le dimensioni, maggiori sono le responsabilità delle piattaforme online».

Le piattaforme saranno, dunque, responsabili dei contenuti pubblicati e, nel caso delle *VLOPs*, la Commissione avrà il potere esclusivo di chiedere l'osservanza delle norme come affermato dal Commissario per il mercato interno Thierry Breton, poiché il *DSA* «affida alla Commissione la supervisione delle grandi piattaforme online, inclusa la possibilità di imporre sanzioni fino al 6% del fatturato globale o addirittura il divieto di operare nel mercato unico dell'UE in caso di ripetute e gravi violazioni».

Per attuare l'applicazione del *DSA*, l'art. 38 stabilisce l'istituzione, negli Stati membri, della figura dei *Digital Services Coordinators*, e le modalità di cooperazione degli stessi sia con i coordinatori dei servizi digitali degli altri Stati membri sia con la Commissione europea[70].

A proposito dei *Coordinators* è previsto, in particolare, che

---

[68] M. Midiri, *Le piattaforme e i poteri dei dati (Facebook non passa il Reno),* cit., p. 177.

[69] Le *very large online platforms* (VLOPs) sono quelle piattaforme digitali che hanno in media oltre 45 milioni di utenti attivi mensili nell'Unione europea, pari al 10% della popolazione europea. Il *DSA* suddivide le piattaforme intermediarie di servizi in quattro categorie: *intermediary services*, *hosting*, *online platform* e *very large platform*.

[70] *P9 TA(2022)0014 Legge sui servizi digitali Emendamenti del Parlamento europeo, approvati il 20 gennaio 2022, alla proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE(COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).* Il testo della Legge è stato sottoposto in seguito ad un'ulteriore revisione e la sua versione definitiva sarà pubblicata sulla Gazzetta Ufficiale europea.

> «*Member States should ensure that Digital Services Coordinators can take measures that are effective in addressing and proportionate to certain particularly serious and persistent infringements of this Regulation. Especially where those measures can affect the rights and interests of third parties, as may be the case in particular where the access to online interfaces is restricted, it is appropriate to require that the measures be ordered by a competent judicial authority at the Digital Service Coordinators' request and are subject to additional safeguards*»[71].

Dunque, per implementare il funzionamento del *DSA* è stabilita la creazione di una struttura a rete, che comporta il coinvolgimento «di diversi attori interessati alle decisioni di regolazione»[72], in questo caso i *Digital Services Coordinators* dei Paesi membri, supportati dalle Autorità amministrative indipendenti nazionali, dai cittadini e dalle autorità giurisdizionali, e la Commissione europea, dal momento che la regolazione delle piattaforme, data la complessità delle situazioni che deve affrontare, richiede una visione olistica e uno sforzo comune per dare vita ad un sistema in grado di tutelare la certezza del diritto nell'ecosistema digitale.

## 4. Il ruolo delle piattaforme digitali e dei *social network* nei Paesi autoritari

Nel mondo i cittadini godono di una libertà di informazione che cambia da Stato a Stato[73], in alcuni la censura è praticamente assente,

---

[71] *Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)). Committee on the Internal Market and Consumer Protection. Rapporteur: Christel Schaldemose*.

[72] D. Bevilacqua, *Il free-trade e l'agorà. Interessi in conflitto, regolazione globale e democrazia partecipativa*, Napoli, 2012, p. 93. In generale, per il concetto di rete, v., *ex multis*, S. Cassese, *Le reti come figura organizzativa della collaborazione,* in *Id., Lo spazio giuridico globale*, Roma-Bari, 2003, pp. 21 ss.; A. Lippi, *Il policy making europeo come "rete"*, in A. Predieri e M. Morisi (a cura di), *L'Europa delle reti*, Torino, 2001, pp. 10 ss.; L. Ammannati, *Governance e regolazione attraverso reti*, in L. Ammannati e P. Bilancia (a cura di), *Governance dell'economia e integrazione europea. Governance multilivello regolazione reti*, vol. II, Milano, 2008, pp. 181 ss.

[73] Nonostante la globalizzazione, infatti, «la società mondiale non è una megasocietà nazionale che contiene e annulla in sé tutte le società nazionali, ma un orizzonte

mentre in altri limita gravemente l'informazione e la possibilità di accedere a fonti alternative che non siano quelle del regime insediato al potere.

Negli Stati autoritari *Internet* è uno degli strumenti più potenti in mano ai governanti, dal momento che possono utilizzare, insieme alla radio, alla televisione e ai giornali, le piattaforme e i *social* come mezzi per influenzare, disinformare e manipolare l'opinione pubblica.

Tali tecnologie, inoltre, possono essere impiegate sia come strumenti di controllo politico e sociale delle persone, che come mezzi di legittimazione del potere politico in quanto utilizzano tecniche innovative basate sull'intelligenza artificiale[74].

Il problema dell'uso strumentale della rete da parte dei regimi autoritari è molto diffuso, come è emerso in maniera evidente anche in questo periodo nel caso del conflitto russo-ucraino, che, accanto ad aspetti tradizionali, come le strategie di informazione e disinformazione effettuate attraverso la televisione, la radio e la stampa, presenta anche strategie caratterizzate dal ricorso ad *Internet.*

I Paesi con sistemi politici non democratici si sono impegnati, nel corso degli anni, nella creazione di piattaforme nazionali da opporre a quelle straniere, che spesso sono *Internet company* statunitensi, per il fatto che esse (le piattaforme nazionali) sono più facilmente controllabili e danno la possibilità, attraverso la propaganda di regime, di influenzare e orientare l'opinione pubblica in senso favorevole nei confronti di chi detiene il potere politico.

Di frequente le popolazioni di questi Paesi sono oggetto di vere e proprie campagne di manipolazione delle informazioni, che costituiscono un ostacolo al discorso democratico, attraverso i *trolls*[75], i *bots*, programmi *software* automatizzati che interagiscono sui *social* facendo credere agli utenti di comunicare con una persona reale, e i *deepfakes*[76],

---

mondiale, caratterizzato dalla molteplicità e dalla non-integrazione»: U. Beck, *Che cos'è la globalizzazione*, Roma, 1999, p. 23.

[74] I Paesi che nel 2021 attuavano una censura particolarmente stringente su *Internet* erano: Cina, Iran, Bielorussia, Qatar, Siria, Thailandia, Turkmenistan, Emirati Arabi, v. *Internet Censorship 2021: A Global Map of Internet Restrictions, in comparitech.com.* A questi Paesi si dovrebbe aggiungere la Federazione russa per le ulteriori restrizioni che ha adottato, nell'ultimo periodo, a seguito del conflitto con l'Ucraina.

[75] I *Trolls*, che spesso operano all'interno delle *troll farm*, siti coordinati in attività di disinformazione per influenzare l'opinione pubblica, sono coloro che intervengono in modo provocatorio al fine di disturbare le normali interazioni tra internetnauti.

[76] Uno di primi esempi di *deepfake* è stato quello presentato nel 2017 da un grup-

video e audio falsi, realizzati utilizzando l'intelligenza artificiale, che servono per diffondere disinformazione.

Per esemplificare la situazione che caratterizza molti regimi autoritari possiamo prendere in considerazione la Repubblica Popolare Democratica di Corea (Corea del Nord), la Repubblica popolare cinese e la Repubblica Islamica dell'Iran.

Nella Corea del Nord, le persone comuni, che non hanno accesso alla rete *Internet* globale, utilizzata soltanto dagli organi legati a vario titolo al governo, devono servirsi di un'unica rete locale, denominata *Kwangmyong*, che permette al Governo di operare una capillare censura sul traffico *online* ed evitare il diffondersi di idee diverse da quelle governative.

Lo stesso discorso può essere fatto nei confronti della Repubblica popolare cinese, dove da decenni viene attuata la censura e la sorveglianza degli individui.

A proposito di questo Paese è importante, innanzitutto, rilevare che la "liberalizzazione" dell'economia non ha comportato un cambiamento politico, dal momento che, anche se la Repubblica popolare cinese ha visto una graduale liberalizzazione dell'economia, che l'ha portata a integrarsi nel mercato mondiale[77] ed esserne uno dei maggiori protagonisti, il Governo cinese ha continuato a sostenere un orientamento politico che rifiuta i valori occidentali come la libertà di parola e la democrazia, a tenere sotto stretto controllo ogni tentativo di mutamento politico e a soffocare il dissenso.

po di ricercatori dell'Università di Washington, nell'ambito di una ricerca finanziata da *Samsung*, *Google*, *Facebook* e Intel, alla conferenza del *SIGGRAPH* (*Special Interest Group on GRAPHics and interactive Techniques*), la più grande conferenza al mondo riguardante la *computer* grafica, in cui si vede Barack Obama pronunciare un discorso mai fatto. Un caso recente di *deepfake* è un video, apparso sui *social media* il 16 marzo scorso, che mostra il Presidente ucraino Zelensky, che si rivolge alla sua Nazione e invita il suo popolo a deporre le armi e a cessare le ostilità. Lo stesso Zelensky ha dovuto dichiararlo falso in un video apparso su *Instagram* e, in seguito, *Facebook* e *YouTube* lo hanno rimosso dalla rete. Il video ha rappresentato un momento storico nell'evoluzione delle tecniche di disinformazione virtuali dal momento che si tratta del primo tentativo di impiegare questa tecnica in un contesto bellico, tuttavia questa evoluzione era del tutto prevedibile poiché già nel video di Barack Obama profeticamente si affermava: «*We're entering an era in which our enemies can make anyone say anything at any point in time*».

[77] Nel dicembre 2001 la Repubblica popolare cinese, dopo un lungo negoziato, è entrata nella *World Trade Organization* (*Wto*).

In particolare in questo Paese, dove dalla metà del secolo scorso viene effettuato un controllo centralizzato costante e pervasivo sugli individui, in seguito alla diffusione di *Internet*[78], al fine di rafforzare la sorveglianza governativa sul traffico *online*, è stato dato vita nel 1998, dopo che il Consiglio di Stato cinese aveva approvato un "ordine" amministrativo intitolato *Metodi di gestione per i servizi di informazione su Internet*, al *Golden Shield Project.*

Il *Golden Shield Project*, conosciuto, facendo riferimento ad un suo sottosistema, anche come *Great Firewall of China*[79], è stato testato nel 2003 dal Ministero della Pubblica Sicurezza cinese (MPS) ed è pienamente funzionante dal 2006.

Il *Great Firewall* ha il compito di bloccare l'accesso agli indirizzi *internet* stranieri considerati "pericolosi" dal Governo e realizza l'isolazionismo informatico, impedendo ai cittadini cinesi di avere accesso al *global free Internet*, al fine di rendere il Paese impermeabile alle idee e ai valori dei Paesi liberal-democratici occidentali[80].

Il *Great Firewall*, in sostanza, è un sistema che si basa sulla censura operata dal Governo cinese per impedire agli internetnauti cinesi l'accesso ai servizi digitali stranieri monitorando, sorvegliando e bloccando il traffico *internet* in entrata e uscita dal Paese per impedire la diffusione di contenuti ritenuti politicamente indesiderati dal Governo, perché, dando voce agli oppositori interni, che potrebbero potenzialmente dar vita ad azioni collettive, potrebbe essere messa in pericolo la stabilità politica e sociale del Paese[81].

Contemporaneamente al posto dei siti *web* stranieri maggiormente diffusi, in Cina ne sono stati creati altri, come il motore di ricerca e

[78] *Internet* si è diffuso in Cina all'inizio del 1996 e già nella seconda parte di quell'anno il Governo cinese ha iniziato a bloccare i siti stranieri che riteneva diffondessero idee non in linea con i suoi orientamenti politici e fossero critici nei suoi confronti.

[79] La denominazione "*Great Firewall*" fu coniata dalla rivista *Wired* nel 1997.

[80] Sul punto, v. M. Ferraro, *Cina, il Grande Fratello che controlla un miliardo e mezzo di cittadini*, in *La Repubblica*, 29 dicembre 2017; R. MacKinnon, *Flatter world and thicker walls? Blogs, censorship and civic discourse in China*, in *Public Choice*, Vol. 134/2008, pp. 31-46; X. Xu, Z.M. Mao, J.A. Halderman, *Internet Censorship in China: Where Does the Filtering Occur?*, in *Passive and Active Measurement Conference*, 2011, pp. 133-142; S. Denyer, *In Cina la censura di Internet va benone*, in *The Washington Post*, 28 maggio 2016.

[81] G. King, J. Pan, M.E. Roberts, *How Censorship in China Allows Government Criticism but Silence Collective Expression*, in *American Political Science Review*, vol. 107, n. 2 (May 2013), pp. 1-18.

il sito *web* più visitato *Baidu*[82], il "*Google* cinese", e i *social network Sina Weibo* e *WeChat*, che il Governo cinese è in grado di controllare per monitorare, controllare e filtrare le principali notizie presenti sulla rete.

Sul punto è, però, importante ricordare che l'attività del governo cinese è in parte facilitata da due fattori: il primo riguarda il fatto che nelle maggior parte dei casi i "*netizens*" (cittadini della Rete) o "*cyber citizens*" «si considerano, consciamente o inconsciamente, membri di sottosistema di governo»[83], ragione per la quale molti di essi si comportano da censori segnalando contenuti non in linea con la narrazione del Governo; il secondo concerne la distanza culturale che separa gli internetnauti cinesi dai cittadini occidentali[84], per la maggioranza dei quali la libertà di espressione rappresenta un valore fondamentale.

Ancora diverso è il caso della Repubblica Islamica dell'Iran: mentre quasi tutti i regimi autoritari hanno realizzato, pur essendo formalmente collegati ad *Internet*, dei *Firewall*, che permettono loro di "filtrare" il traffico dell'infosfera o cyberspazio al fine di controllare i propri cittadini per garantire la stabilità sociale e politica necessaria alla loro sopravvivenza, l'Iran rappresenta una situazione unica in quanto non è connesso ad *Internet*, ma ha una rete interna parallela completamente scollegata e isolata dal *World Wide Web* globale.

Tuttavia, nonostante l'isolamento dall'*Internet* globale voluto dalle Autorità iraniane, le immagini e le notizie, apparse sui *mass media* dei Paesi liberal-democratici e relative alle proteste, che stanno accadendo dal 16 settembre in quel Paese a seguito della morte di Mahsa Amini[85], dimostrano che è impossibile impedire totalmente l'uscita di informazioni e di video su quanto sta accadendo in Iran.

La loro diffusione è stata resa possibile perché i dissidenti iraniani, per eludere la censura *on-line* imposta dal Governo degli *ayatollah*,

---

[82] *Baidu* insieme con quattro grandi imprese cinesi (*Alibaba*, *Tencent*, *Huawei* e *Xiaomi* fa parte di un gruppo conosciuto con l'acronimo *BATHX*. Tra queste imprese, *Alibaba* è un gigante dell'*e-commerce*, *Tencent* è una società di videogiochi e *social media*.

[83] K. Kuo, *Rete e social media in Cina*, Milano, 2014, p. 41.

[84] M.G. Mattei, *Il dragone digitale*, in K. Kuo, *Rete e social media in Cina*, cit., p.17.

[85] Mahsa Amini era una giovane curda che è deceduta per le violenze subite dalla "polizia morale" iraniana, mentre era in stato di arresto per non aver indossato correttamente l'*hijab*.

utilizzano la *VPN*[86] e altri servizi di *relay* per poter comunicare con gli internetnauti del *Web* globale.

In questo modo l'opinione pubblica mondiale ha potuto anche vedere che sono stati specialmente i giovani iraniani, appartenenti alla Generazione Z, ovvero coloro che sono nati tra il 1997 e il 2010, a dar vita a numerose manifestazioni anti-velo, che durano tuttora in molte città del Paese, nei confronti del potere politico che ha deciso di soffocarle con la forza.

Riprendendo il filo principale del discorso, si può affermare che nel caso dell'Iran, che ha deciso di staccare la propria rete da *Internet* creando una nuova rete che copre solo il suo territorio, si può parlare di *splinternet*[87].

Se numerosi Paesi autoritari si metteranno sulla strada di isolarsi dall'*Internet* globale (è questo il caso della Federazione russa come vedremo nel paragrafo 5.2.), ciò determinerà un'ulteriore "balcanizzazione" della rete, causando un cambiamento radicale di *Internet*, che cesserebbe di essere una singola rete, caratterizzata da una tecnologia di comunicazione globale in grado di connettere tutto il mondo, per essere frammentato in diverse reti regionali chiuse in se stesse, che costituirebbero, a ben guardare, delle bolle tese a rafforzare sempre più, mettendo *offline* le idee che circolano nei Paesi liberal-democratici, l'isolamento degli individui che abitano in quegli Stati.

Tuttavia, per il momento, nonostante i *Firewall*, la tecnologia digitale è in grado di offrire ai dissidenti degli Stati illiberali i mezzi per evitare la loro completa disconnessione dalla rete globale e a avere accesso a fonti di informazione alternative alla narrazione *mainstream*.

Ciò può essere fatto ricorrendo alla *Virtual Private Network* (*VPN*), ossia alla "rete privata virtuale", che «permette di rendere invisibili le proprie attività in rete a occhi indiscreti e di mascherare l'indirizzo *IP* da cui si accede a *Internet*»[88], consentendo in questo modo di dar vita ad un canale di comunicazione con la rete globale in grado

[86] Sul punto, v. *Macinety.it*; *nytimes.com*.

[87] Il termine è stato coniato nel 2001 da Clyde Wayne Crews in un editoriale su *Forbes* per descrivere la sua visione sulla creazione di *Internet* paralleli che vengono gestiti come «*distinct, private, and autonomous universes*».

[88] M. Cochi, *Come i russi aggirano la severa censura governativa su Internet*, in *startinsight.eu*, 2022, p. 1.

di sfuggire alla censura dei Governi[89] dal momento che il "traffico" su *Internet* di questi utenti risulta criptato.

## 5. Il caso della Federazione russa

Per approfondire concretamente il discorso sulla volontà di impedire la libertà di informare, di essere informati e di non essere disinformati[90] e di limitare il pluralismo informativo da parte dei Paesi autoritari è possibile prendere in considerazione ciò che sta accadendo dalla fine dello scorso febbraio nella Federazione russa.

### *5.1. L'incremento della disinformazione e della censura nella Federazione russa dopo il 24 febbraio 2022*

La notte fra il 23 e il 24 febbraio, dopo che la Federazione russa aveva riconosciuto le repubbliche separatiste di Luhansk e Donetsk nel Donbass controllate dai filorussi, l'esercito russo ha dato inizio nella parte orientale dell'Ucraina a quella che Putin ha definito "operazione militare speciale"[91] per proteggere i separatisti del Donbass e

[89] Sulla VPN, v. S. Lombardo, *VPN: cos'è, come funziona e a cosa serve una Virtual Private Network*, in *CyberSecurity360*, 5 settembre 2022.

[90] Il diritto a non essere disinformati consiste nel diritto «a non ricevere sistematicamente, prioritariamente o esclusivamente notizie false, incomplete o comunque idonee a veicolare una informazione non imparziale»: A. Nicita, *op. cit*., p. 218.

[91] Nel marzo 2019 è entrata in vigore nella Federazione russa una legge che vieta la diffusione *online* di *fake news* sia da parte dei mezzi di comunicazione di massa, sia di singoli cittadini. Tale legge è applicabile non solo alle notizie false che vengono diffuse su *Internet*, ma anche a qualsiasi informazione falsa, ma riportata come affidabile; inoltre vengono puniti anche coloro che dimostrano una "palese mancanza di rispetto" nei confronti dello Stato. La Duma il 4 marzo 2022 ha, inoltre, approvato all'unanimità una legge tesa ad impedire la diffusione di false informazioni sulle operazioni militari in corso in Ucraina. Tale legge, approvata dalla camera bassa del Parlamento russo, prevede, in particolare, fino a tre anni di carcere e una multa da 1,5 milioni di rubli per coloro che pubblicano informazioni false (in realtà vengono classificate come *fake news* tutte le informazioni non allineate con quelle diffuse dalla propaganda di Stato sulla guerra in Ucraina), pene estensibili fino a 5 milioni di rubli e quindici anni di reclusione a seconda delle conseguenze e dell'entità delle notizie diffuse. Ad esempio, poiché il Presidente Putin ha definito l'intervento armato russo contro l'Ucraina "operazione militare speciale" per proteggere i separatisti del Donbass, definire "guerra" il conflitto russo-ucraino è considerato disinformazione e come tale punibile.

annettere le due repubbliche e, nello stesso tempo, conquistare la città di Odessa[92].

Per condurre con successo le operazioni militari la Russia non si è affidata solamente alle armi, ma anche ad una articolata campagna di disinformazione e propaganda, in cui le piattaforme digitali e i *social media* hanno un ruolo importante[93].

Per sostenere l'intervento bellico ed attuare tecniche di disinformazione e di propaganda, il Governo russo utilizza per influenzare l'opinione pubblica interna i più seguiti *media* nazionali, che sono statali o appartengono a grandi società private, di proprietà di un ristretto numero di oligarchi, con forti legami col Governo e vicini al potere politico a cui devono la loro fortuna economica, che hanno dato vita ad una sorta di "capitalismo oligarchico" sottoposto ad uno stretto controllo politico, che interviene con prontezza «quando i singoli capitalisti guidano le loro imprese in direzioni non gradite al partito-Stato»[94].

[92] Nelle settimane successive il teatro delle operazioni militari russe si è via via allargato a tutto il territorio nazionale ucraino, per poi, all'inizio del mese di aprile, restringersi nuovamente in vista di un riposizionamento delle forze militari russe nei territori orientali dell'Ucraina. Dopo che nei mesi successivi l'esercito russo ha occupato gran parte dei territori delle due repubbliche popolari separatiste del Donbass e delle regioni di Zaporizhzhia e di Kherson, nel mese di settembre in questi territori è stato indetto per volere del governo russo un *referendum*, che si è svolto tra il 23 e il 27 settembre e ha avuto come esito la loro annessione alla Federazione russa. Nonostante che il *referendum* e i risultati dello stesso non siano stati riconosciuti validi dagli USA e dall'Unione Europea, apertamente schierati a fianco dell'Ucraina, e da gran parte della comunità internazionale, il giorno 30 settembre Vladimir Putin ha firmato i trattati di annessione di questi territori, che è stata formalmente ratificata il 3 ottobre dalla Duma di Stato e il 4 ottobre dal Consiglio della Federazione. Il 5 ottobre Putin ha firmato le quattro leggi che ratificano l'annessione delle regioni ucraine occupate, di cui, però, non ha il pieno controllo. Dal punto di vista militare l'annessione di questi territori ha un'importanza capitale: l'operazione militare speciale, nella logica del Cremlino, si è trasformata in una guerra difensiva e, stando alla dottrina militare russa, la controffensiva ucraina, che in queste ultime settimane sta registrando significativi successi nei territori annessi alla Federazione, è diventata "un'aggressione alla sovranità russa" e Mosca potrà usare ogni mezzo "per difendere il territorio nazionale", compreso il ricorso all'impiego dell'arsenale nucleare.

[93] M. Veneziano, *Arene informative e attori geopolitici: il duplice ruolo delle piattaforme digitali nel conflitto tra Federazione russa e Ucraina*, in Geopolitica.info, 3 marzo 2022.

[94] G.P. Caselli, *Eredità sovietica e terapia shock impiombano l'economia russa*, in *Limes – Rivista italiana di geopolitica*, n. 11/2011, p. 159.

Se prendiamo le tre principali reti televisive, vediamo che due di esse *Rossiya Tv* (Russia Tv) e *Pervyj kanal* (Primo canale) sono controllate dal Governo, la prima interamente, la seconda per il 51%, mentre *NTV*, il terzo canale televisivo più importante, è posseduto dal colosso energetico *Gazprom*.

La stessa situazione riguarda le radio più diffuse, anch'esse, in un modo o nell'altro, sotto la supervisione dello Stato, così come la carta stampata e i siti *web* nazionali maggiormente utilizzati.

Per quanto riguarda l'informazione interna, *TV Rain* è stata sospesa a tempo indeterminato, la radio "Eco di Mosca" è stata chiusa, il giornale *Novaya Gazeta*, uno dei più noti giornali di opposizione della Federazione russa, diretto da Dimitrij Muratov, premio Nobel per la pace 2021 insieme alla giornalista filippina Maria Ressa, è stato sottoposto, fin dall'inizio delle ostilità, ad un'attenta sorveglianza [95].

A partire dall'inizio della guerra con l'Ucraina, la Federazione russa ha, inoltre, intensificato le misure repressive nei confronti delle fonti di informazione internazionali non allineate con le tesi del Governo e critiche nei confronti dell'intervento militare contro l'Ucraina.

I provvedimenti governativi hanno, infatti, silenziato numerose emittenti radio straniere (*Bbc*, *Voice of America*, *Radio Free Europe* e *Deutsche Welle*) e gradualmente bloccato l'accesso alle piattaforme tecnologiche, come *Facebook* (oscurato il 4 marzo) e *Instagram* di *Meta*[96], *Twitter*, *YouTube*, mentre altre, come *Apple*, *Microsoft*, *Netflix*

[95] Muratov il 3 marzo scorso ha presentato un ricorso alla Corte EDU con cui ha chiesto che venissero adottate delle misure d'urgenza nei confronti della Federazione russa accusata di impedire l'attività di informazione dei *media* russi indipendenti sulla guerra in Ucraina, perché non in linea con l'orientamento ufficiale. La Corte, in attesa di pronunciarsi nel merito, ha emesso il 10 marzo un provvedimento cautelare urgente a tutela della libertà di espressione, garantita dall'art. 10 della Convenzione europea dei diritti dell'uomo, con cui ha intimato alla Russia di non interferire e di non impedire l'attività di *Novaya Gazeta*.

[96] Come ha annunciato Mark Zuckerberg, durante una conferenza tenutasi il 28 ottobre scorso, *Meta* è la società, costituita da *Facebook*, *Messenger*, *Instagram*, *WhatsApp* e *Oculus* (società specializzata in visori per la realtà virtuale), che ha deciso di investire sulla creazione del metaverso, uno spazio virtuale tridimensionale in cui sarà possibile effettuare le attività quotidiane e interagire in maniera molto coinvolgente con gli *avatar* dei *digital twin*, ossia rappresentazioni digitali e tridimensionali delle persone reali. Mark Zuckerberg, dopo aver creato la prima piattaforma globale di *social media*, intende ripetere la stessa cosa nella realtà virtuale col metaverso. Secondo i suoi programmi, *Meta* rappresenterà la nuova rivoluzione della tecnologia mondiale, capace di sostituire *Internet*, che si evolverà in un mondo virtuale come strumento di

e *TikTok*, a causa della censura, di propria iniziativa hanno gradualmente sospeso le loro attività.

In questo modo la Federazione russa ha incominciato ad innalzare un *firewall*, una cortina di ferro digitale, che isola i suoi abitanti dalle fonti informative occidentali[97] e a dar vita ad un'intensa attività di propaganda, di disinformazione e di manipolazione delle informazioni sull'invasione e sull'andamento delle operazioni militari attraverso i *media* russi, in particolare il quotidiano governativo *online Sputnik* e il canale televisivo statale multilingue *RT* (*Russia Today*). A proposito di questi ultimi due *media* russi, è bene ricordare che il Consiglio dell'Unione Europea il 1° marzo scorso ha deciso, dopo l'inserimento dell'articolo 2 *septies*[98] nel Regolamento (UE) n. 833/2014[99], di bandire, a partire dal 2 marzo, le trasmissioni in Europa sia di *Russia Today* che di *Sputnik* perché, come recita il Considerando 9 dello stesso Regolamento, «tali organi di informazione […] svolgono un ruolo essenziale,

comunicazione e svago. Il metaverso sarà, in sostanza, una nuova dimensione, in cui lo spazio fisico e quello digitale coesisteranno dando vita ad una realtà *phygital*, che potrà essere interessante e coinvolgente, ma che porrà prima di tutto il problema dei veri fini cui tenderà chi ne deterrà il controllo e, immediatamente dopo, il problema della necessità di regolamentarla, da un lato, per tutelare la *privacy* e la sicurezza dei suoi utenti e, dall'altro lato, per tutelare le regole della concorrenza in quanto, dopo *Meta*, altre piattaforme potrebbero proporre il loro metaverso e ricorrere a strategie di *lock-in* per assumere una posizione dominante sul mercato.

[97] Per ovviare a tale situazione, al fine di permettere ai cittadini russi o, comunque, a quelli che sono diffidenti o contrari alla narrazione di Stato, l'accesso a fonti di notizie maggiormente affidabili o diverse da quelle governative, si sta cercando di sviluppare sistemi di comunicazione basati sulla crittografia *end-to-end* in grado di aggirare il *firewall* censorio russo. *Twitter*, ad esempio, dall'8 marzo è nuovamente disponibile in Russia, nonostante il *ban*, non dal suo sito tradizionale, ma adottando gli #*OnionServices* e #*OnionNetworking* attraverso il progetto *Tor*, una piattaforma che consente di accedere ad *Internet* in modo anonimo e sicuro aggirando la censura del Governo.

[98] Articolo 2 *septies*: 1. È vietata agli operatori la radiodiffusione, ovvero il conferimento della capacità di diffondere, l'agevolazione della radiodiffusione o altro concorso a tal fine, dei contenuti delle persone giuridiche, delle entità o degli organismi elencati nell'allegato XV, anche sotto forma di trasmissione o distribuzione tramite mezzi quali cavo, satellite, IP-TV, fornitori di servizi internet, piattaforma o applicazione di condivisione di video su internet, siano essi nuovi o preinstallati. 2. Sono sospesi qualsiasi licenza o autorizzazione di radiodiffusione e qualsiasi accordo di trasmissione e distribuzione con le persone giuridiche, le entità o gli organismi elencati nell'allegato XV.

[99] Regolamento (UE) 2022/350 del Consiglio, del 1° marzo 2022, *che modifica il regolamento (UE) n. 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina.*

strumentale ai fini della promozione e del sostegno dell'aggressione nei confronti dell'Ucraina e della destabilizzazione dei Paesi ad essa limitrofi».

Anche i grandi *social*, come *Facebook* e *Instagram*, *Twitter*, *TikTok* e *YouTube*, si sono attivati autonomamente per contrastare e limitare la diffusione di contenuti inattendibili e palesemente frutto di pratiche di propaganda e di disinformazione che circolano a proposito della guerra russo-ucraina[100].

*Meta*, ad esempio, ha formato un "centro operativo speciale" per arginare la divulgazione di notizie false postate su *Facebook* sul conflitto militare in corso in Ucraina dai fautori di entrambi gli schieramenti e, in particolare, da organizzazioni controllate dallo Stato russo, che, come contromisura, ha ordinato al *social network* in questione, senza ottenere, però, alcun risultato, la cessazione di *fact-checking* del suo centro.

Un importante aspetto, su cui è necessario richiamare nuovamente l'attenzione, è quello che *Meta* ha concesso ai suoi utenti di postare messaggi, che violano le regole di *Facebook* e *Instagram* contro i discorsi d'odio, non censurando i *post* degli iscritti a *Facebook* e *Instagram* di numerosi Paesi[101] contro la Federazione russa, l'esercito russo invasore, il Presidente Vladimir Putin e il Presidente della Bielorussia, Alexander Lukashenko.

La decisione di *Meta* ha spinto la Federazione russa a reagire limitando l'accesso anche a *Instagram* a partire dal 14 marzo, accusando il *social network* di diffondere, dopo l'invasione dell'Ucraina, appelli alla violenza contro i russi, e a ordinare alla sua ambasciata negli Stati Uniti di chiedere al Governo americano di fermare le «attività terroristiche» di *Meta* e di «assicurare i colpevoli alla giustizia».

Anche l'Ufficio dell'Alto Commissariato per i diritti umani delle Nazioni Unite si è dichiarato preoccupato per il cambio di *policy* di *Meta*.

Il cambiamento di *policy* da parte di *Meta* ci offre l'occasione per prendere brevemente in considerazione un'importante problematica

[100] L'attività di contrasto al propagarsi di false notizie su *Internet* ha visto anche l'intervento dei *debunker*, individui o organizzazioni, che cercano di trovare conferme alla credibilità di notizie o di filmati relativi al conflitto in questione, nel tentativo di stabilirne la verità dal momento che non mancano, ad esempio, video riguardanti operazioni cosiddette di "*false flag*".

[101] Armenia, Azerbaigian, Estonia, Georgia, Ungheria, Lettonia, Lituania, Polonia, Federazione russa, Slovacchia, Ucraina.

che riguarda l'azione delle piattaforme digitali e cioè il controllo dei contenuti in rete predisposto in maniera autonoma dalle piattaforme stesse attraverso condizioni d'uso che determinano quali contenuti possono essere pubblicati e quali devono essere rimossi.

Il tema del controllo operato dalle piattaforme sui contenuti comprendenti discorsi d'odio è di grande rilevanza[102] e ha posto il delicato problema della sua qualificazione: infatti, mentre una parte della dottrina afferma espressamente che si tratta di un'attività censoria *tout court*[103], le piattaforme digitali e la Commissione europea parlano di attività di moderazione dei contenuti o *Content Moderation.*

In ogni caso, al di là di questa questione che non è di certo trascurabile, non sembra opportuno affidare ai *social media*, che appartengono a società private, senza imporre loro una regolamentazione pubblica, il potere di moderare il discorso politico sul *Web*, in quanto ciò può dar vita ad importanti aspetti negativi tra cui la cancellazione arbitraria di contenuti postati, il cosiddetto *deplatforming* o, come appena visto nel caso di *Meta*, la possibilità di lasciare circolare liberamente, anche se per un periodo limitato e per un circoscritto numero di Paesi, discorsi d'odio sui suoi *social network.*

La decisione di *Meta* può rappresentare un pericoloso precedente perché potrebbe essere replicato, in quanto, se le regole che "valgono" sono quelle dei proprietari delle piattaforme, questi ultimi, attribuendosi «il diritto di determinare i criteri di verità», possono cambiare, a loro discrezione, bersaglio, esercitando un potere reale nel discorso pubblico e, di conseguenza, incidere in modo profondo sulle dinamiche democratiche.

Questo è un effetto della complessità giuridica che caratterizza l'era di *Internet*, in cui soggetti privati, nella fattispecie le piattaforme

[102] P. Falletta, *Controlli e responsabilità dei social network sui discorsi d'odio online*, in *MediaLaws.eu*, n. 1/2020.

[103] V. M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'Agorà digitale*, cit. L'Autore, a p. 39, distingue due tipologie di censura: la "censura *de facto*", effettuata dalle piattaforme in maniera autonoma in base alle loro *policies* e condizioni d'uso, e la "censura *de jure*". A proposito di quest'ultima, poi, si deve «rilevare la sussistenza di due species di questo genus: la censura privata funzionale, ossia quella imposta dallo Stato a seguito di un controllo di natura giudiziale/amministrativo, e la censura privata sostanziale, ossia quella in cui il bilanciamento fra libertà di espressione e altri beni giuridici viene delegato dallo Stato direttamente alle piattaforme digitali». Con la censura privata sostanziale, in definitiva, si può parlare di privatizzazione della giustizia su delega statale.

*online*, attuano una censura privata, che, a volte, limita in modo ingiustificato la libertà di espressione degli individui.

### *5.2. Un ulteriore passo verso la balcanizzazione della Rete globale: la* RuNet*, l'*Internet *sovrano russo*

Premesso che la Federazione russa già da diversi anni sta portando avanti, per vari motivi, il controllo di *Internet* attraverso una nutrita «serie di interventi regolatori»[104], nei primi mesi del 2019 sono stati discussi tre progetti di legge riguardanti «la libera circolazione delle informazioni su Internet e il funzionamento delle rete»[105].

Dei tre progetti, due, riguardanti la circolazione delle informazioni su *Internet*, che hanno affrontato

> «la responsabilità per la diffusione delle "fake news" […] e delle pubblicazioni che esprimono una "palese mancanza di rispetto per l'autorità" […], hanno apportato rilevanti correzioni e integrazioni alla legge federale n. 149 "*Sull'informazione, sulle tecnologie dell'informazione e sulla difesa dell'informazione*" del 2006 e al Codice degli illeciti amministrativi del 2001 (nella parte che stabilisce la responsabilità amministrativa per la diffusione delle informazioni proibite nelle reti di informazione)»[106].

Questi due disegni di legge sono stati discussi e approvati in tempi brevissimi, prima dai deputati della *Duma* in tre sedute e, in seguito, dal Consiglio federale in una sola seduta, e le due leggi, dopo la firma del Presidente Putin[107], sono entrate in vigore il 29 marzo 2019.

---

[104] Sul tema, v. I. Galimova, *La Duma introduce nuove restrizioni alla rete*, in *Nomos. Le attualità del diritto*, n. 1-2019, pp. 1-18.

[105] *Ivi*, p. 3.

[106] *Ivi*, pp. 3-4. Le sanzioni amministrative prevedono, per gli utenti russi che diffondono in rete contenuti che esprimono «"in una forma indecente ... una chiara mancanza di rispetto verso la società, lo Stato, i simboli ufficiali dello Stato, la Costituzione o gli organi del potere statale (…)" oppure "informazioni false di pubblico interesse presentate come veritiere", se portano a gravi conseguenze per la salute di una persona o la stabilità sociale», una multa anche superiore a 30 mila rubli o la reclusione fino a 15 giorni in caso di violazione ripetuta: *ivi*, pp. 4-5.

[107] Nella Federazione russa una legge, concluso positivamente l'*iter* parlamentare, «deve essere inviata al Presidente Federale, il quale dispone di un potere di veto, potendo respingere la proposta entro 14 giorni dal suo ricevimento (art. 107.3 CFR). Si tratta di una decisione che può essere superata soltanto da una riapprovazione successiva del testo da parte di entrambe le Camere a maggioranza dei 2/3, nel qual caso il Presidente

Il terzo disegno di legge, che si poneva come fine la creazione di una rete *internet* nazionale autonoma, dopo le necessarie modifiche alla Legge federale n. 126 *Sulle comunicazioni*, è stato approvato nel mese di aprile 2019 prima dalla Duma e, pochi giorni dopo, dal Consiglio federale.

Tale Legge federale n. 90, denominata *Programma nazionale di economia digitale*, è entrata in vigore, dopo essere stato firmata il primo maggio 2019 dal Presidente Putin, il primo novembre dello stesso anno.

Il *Programma nazionale di economia digitale* ha gettato le basi dell'*Internet* russo, noto come *RuNet*, separato dalla struttura globale di *Internet*, che è entrato in funzione il 1° gennaio 2021, con l'obiettivo ufficiale di «prevenire eventuali conseguenze negative di una disconnessione totale dalla rete globale, ampiamente controllata dall'estero»[108].

Ufficialmente il progetto si pone il fine di proteggere la sicurezza nazionale[109] per evitare *cyber* attacchi e rendere la Federazione russa autosufficiente, ma in realtà esso si presta anche ad isolare i cittadini russi dall'*Internet* globale, permettendo alle autorità governative di sorvegliare e monitorare ed eventualmente bloccare all'interno del Paese i contenuti del traffico *online* sgraditi al potere politico.

In sostanza, *RuNet* può essere uno strumento di controllo totalitario, in quanto si tratta della creazione di un *Internet* sovrano, una *intranet* domestica, in cui tutte le informazioni e i dati vengono scambiati su *server* russi e altre apparecchiature tecnologiche di proprietà del Governo al fine di contrastare le minacce esterne e di tracciare, monitorare, filtrare il traffico *online* interno. Attraverso *RuNet*, il Governo ha, dunque, non solo la possibilità di poter isolare il Paese dalla rete *internet* globale, ma anche, attraverso il controllo preventivo da parte

è tenuto a promulgare la legge entro 7 giorni»: R. Tarchi, *Sistema delle fonti e poteri normativi dell'Esecutivo in una forma di Governo iper-presidenziale: il caso della Federazione Russa,* in Osservatorio sulle Fonti, n. 3/2018, pp. 11-12.

[108] Come ha dichiarato il Presidente della Federazione russa, Vladimir Putin, all'agenzia di stampa ufficiale russa TASS.

[109] In questo caso, come in moltissimi altri casi riguardanti anche Paesi democratici, l'uso dell'argomento della sicurezza viene utilizzato per affidare alle tecniche della sorveglianza «il compito di costruire dal basso il controllo capillare dei cittadini» e per ridurre libertà e diritti degli individui che «vengono lentamente erosi»: S. Rodotà, *op. cit*., pp. 381 e 326.

delle autorità, *in primis* il *Roskomnadzor*[110], di censurare qualsiasi critica interna nei confronti del Governo stesso, dei politici o del Paese in generale e di evitare la diffusione di notizie e giudizi critici provenienti *extra-intranet*, soffocando, di conseguenza, la libertà di informazione e di dibattito.

La legge in questione, inoltre, per semplificare l'azione di controllo e di censura delle autorità, impone a tutti gli operatori di rete di installare le *middle box*, che effettuano il filtro e la verifica dei contenuti che passano attraverso la rete. Questa pratica denominata *deep-packet inspection* consente al Governo russo di avere accesso e di controllare il traffico *internet* sia per scopi legittimi, ma anche per scopi di sorveglianza e censura.

Il Governo russo con *RuNet*, una volta che il progetto sarà completato, avrà la possibilità di controllare ed eventualmente censurare, in particolare, le attività sul *Web* dei dissidenti. Il rafforzamento del controllo governativo sul *Web* è, infatti, un obiettivo certamente non secondario della legge su *Internet* sovrano, che si pone il fine di soffocare «*the right of people in Russia to free speech and freedom information online*» come è stato affermato, al momento della promulgazione della Legge in questione, dalla Organizzazione indipendente per la difesa dei diritti umani *Human Rights Watch*[111].

### *5.3. Le conseguenze della guerra: dall'isolamento dalla Rete globale a quello politico internazionale*

Soffermiamoci, ora, sulle sanzioni contro la Federazione russa che sono state determinate dall'invasione dell'Ucraina.

La *ratio* sottesa all'esame delle sanzioni imposte a livello internazionale alla Federazione russa, che di seguito verranno prese in considerazione, è quella di riflettere su quale possibile futuro potrà avere in particolare il pluralismo politico in questo Paese a causa dell'isolamento in cui verrà a trovarsi dal punto di vista delle relazioni internazionali

[110] Il Roskomnadzor, Servizio federale per la supervisione delle comunicazioni, delle tecnologie dell'informazione e dei *mass media*, è l'ente del Governo russo che si occupa di regolare le telecomunicazioni e di controllare *Internet* «gestendone tutti i contenuti con la motivazione ufficiale di proteggere RuNet da attacchi informatici»: M. Cochi, *op. cit.*, p. 2.

[111] *Russia: New Law Expands Government Control Online. Wider Internet Surveillance*, in *Human Rights Watch*, 31 ottobre 2019.

con i Paesi democratici occidentali e da quello determinato dall'adozione della *RuNet*.

Il Comitato dei Ministri del Consiglio d'Europa, reputando l'invasione dell'Ucraina «una grave violazione del diritto internazionale», il 25 febbraio 2022, ha deciso, ai sensi dell'articolo 8 dello Statuto[112], di sospendere, con effetto immediato, la Federazione russa dai suoi diritti di rappresentanza nel Comitato dei Ministri e nell'Assemblea Parlamentare[113].

Con questa decisione[114] di natura temporanea e presa con l'intenzione di non chiudere la possibilità di instaurare trattative, come sarebbe avvenuto in caso di espulsione, la Federazione russa rimaneva membro del Consiglio d'Europa e parte della Convenzione europea dei diritti dell'uomo.

Sui rapporti fra la CEDU e la Federazione russa è necessario, almeno in brevissima sintesi, fare un'importante precisazione: la Federazione è entrata a far parte della CEDU nel 1998 e, pertanto, le sentenze della Corte di Strasburgo dovrebbero essere vincolanti per il Paese, ma spesso la Federazione russa le ha viste come un'ingerenza nella sua sovranità giuridica e il Parlamento russo ha emanato la Legge federale n. 7-FZ 2015, che ha conferito alla Corte costituzionale russa il compito di pronunciarsi su tale questione con l'onere di dare la priorità alla

[112] Tale articolo prevede che «ogni Membro del Consiglio d'Europa che contravvenga alle disposizioni dell'articolo 3, può essere sospeso dal diritto di rappresentanza e invitato dal Comitato dei Ministri a recedere nelle condizioni di cui all'articolo 7». In particolare, l'art. 3 stabilisce che «ogni Membro del Consiglio d'Europa riconosce il principio della preminenza del Diritto e il principio secondo il quale ogni persona soggetta alla sua giurisdizione deve godere dei diritti dell'uomo e delle libertà fondamentali. Esso si obbliga a collaborare sinceramente e operosamente al perseguimento dello scopo definito nel capo I».

[113] «*The decision of the Council of Europe of 25 February to suspend the Russian Federation's right to representation was taken because its invasion of Ukraine goes against everything we stand for and is a violation of our statute and of the European Convention on Human Rights*». È il caso di ricordare che i rapporti fra la Federazione russa e il Consiglio d'Europa, dopo la sua adesione avvenuta il 28 febbraio 1996, sono sempre stati difficoltosi a causa di conflitti che, lungo l'arco di molti anni, hanno visto la Federazione russa ingerirsi a più riprese negli affari interni di alcuni Stati confinanti.

[114] Nel comunicato diramato il 25 febbraio si legge: «La decisione di oggi significa che la Russia rimane membro del Consiglio d'Europa e parte delle sue convenzioni, compresa la Convenzione europea dei diritti dell'uomo. La sospensione non è una misura definitiva ma temporanea, lasciando aperti i canali di comunicazione».

tutela degli interessi della Federazione nelle controversie dinanzi alla Corte EDU.

La Corte costituzionale russa l'anno successivo ha riaffermato, con la sentenza n. 12-P/2016, il principio che «la Federazione russa non è obbligata a dare esecuzione a quelle sentenze della Corte EDU che constatano la violazione della CEDU da parte di norme della legislazione russa giudicate conformi alla Costituzione», perché, in sostanza, la Legge federale prima citata «autorizza le autorità a ignorare le decisioni degli organismi internazionali a cui la Russia ha aderito se queste "violano i principi e le norme fondamentali della Costituzione russa"»[115].

In seguito, nel 2019, il Presidente Putin ha proposto una modifica, poi approvata nel 2020, della Costituzione russa, per sancire la superiorità delle pronunce della Corte costituzionale russa sulle sentenze rese da tutti i tribunali internazionali, comprese quelle della Corte europea dei diritti dell'uomo.

Chiarito questo rilevante aspetto, riprendiamo il filo del discorso.

L'azione militare contro l'Ucraina ha provocato anche l'intervento della Corte Europea dei Diritti dell'Uomo, che ha adottato il 28 febbraio, ai sensi dell'art. 39 CEDU, su richiesta del Governo ucraino, che aveva presentato un ricorso in cui accusava la Federazione russa di violare la Convenzione per aver invaso uno Stato indipendente e di commettere numerose violazioni dei diritti umani, un provvedimento cautelare nei confronti della Federazione russa.

Con tale provvedimento la Corte EDU invitava la Federazione russa «*to refrain from military attacks against civilians and civilian objects, including residential premises, emergency vehicles and other specially protected civilian objects such as schools and hospitals, and to ensure immediately the safety of the medical establishments, personnel and emergency vehicles within the territory under attack or siege by Russian troops*» e chiedeva contestualmente al Governo russo di informare con tempestività la Corte sulle misure adottate per assicurare il rispetto della Convenzione.

Contrariamente alle aspettative, però, il Ministro degli Esteri russo, Serghei Lavrov, il 10 marzo, ha dichiarato che la Federazione russa

[115] Sul punto, per il periodo fino al 2016, v. A. Di Gregorio, *Russia. Il confronto tra la Corte costituzionale e la Corte europea per i diritti dell'uomo tra chiusure e segnali di distensione*, in Federalismi.it, n. 2/2016, pp. 1-21.

riteneva che il corso degli eventi fosse ormai "irreversibile" e che non intendeva più far parte del Consiglio d'Europa[116], dal momento che l'EU e i Paesi della Nato erano ostili nei suoi confronti e abusavano della loro maggioranza assoluta nel Comitato dei Ministri del Consiglio d'Europa per far prevalere le loro tesi e che tale comportamento stava portando alla «distruzione del Consiglio d'Europa e dello spazio giuridico e umanitario in Europa».

Tale decisione ha comportato anche il recesso dalla CEDU ai sensi dell'art. 58, par. 3[117], e, in conformità con la risoluzione del 22 marzo 2022[118], la Corte europea dei diritti dell'uomo ha accolto i ricorsi presentati contro la Federazione russa fino allo scorso 16 settembre, giorno in cui il recesso è diventato effettivo.

Dal momento che sono pendenti presso la Corte EDU più di diciassettemila ricorsi nei confronti della Federazione russa; dopo la sua uscita dalla Convenzione e l'estromissione del giudice russo dalla Corte, è sorta una grave problematica in quanto la Corte può decidere solamente i ricorsi che possono essere giudicati dal Giudice unico, che li può dichiarare inammissibili, e dal Comitato di tre giudici, che può decidere esclusivamente sui casi ripetitivi con consolidata giurisprudenza[119].

---

[116] Il recesso di uno Stato membro del Consiglio d'Europa è previsto dall'articolo 7 dello Statuto del Consiglio d'Europa: «Ogni Membro può recedere dal Consiglio d'Europa, notificando la sua risoluzione al Segretario Generale. La notificazione avrà effetto alla fine dell'anno finanziario in corso, qualora sia stata fatta nei primi nove mesi dello stesso, e alla fine dell'anno finanziario seguente, qualora sia stata fatta negli ultimi tre mesi».

[117] Il recesso dalla CEDU è previsto dall'articolo 58 della Convenzione: 1. Un'Alta Parte contraente può denunciare la presente Convenzione solo dopo un periodo di cinque anni a partire dalla data di entrata in vigore della Convenzione nei suoi confronti e dando un preavviso di sei mesi mediante notifica indirizzata al Segretario generale del Consiglio d'Europa, che ne informa le altre Parti contraenti. 2. Tale denuncia non può avere l'effetto di svincolare l'Alta Parte contraente interessata dagli obblighi contenuti nella presente Convenzione per quanto riguarda qualunque fatto suscettibile di costituire una violazione di tali obblighi, da essa posto in essere anteriormente alla data in cui la denuncia è divenuta efficace. 3. Alla stessa condizione, cesserebbe d'esser parte alla presente Convenzione qualunque Parte contraente che non fosse più membro del Consiglio d'Europa.

[118] *Echr.coe.int*.

[119] La Corte di Strasburgo è suddivisa in sezioni, all'interno delle sezioni si costituiscono quattro formazioni giudicanti: Giudice unico, Comitato dei tre Giudici, Camera e Grande Camera.

In tutti i restanti casi, di pertinenza della Camera e, eventualmente, della Grande Camera, poiché la presenza del giudice nazionale è indispensabile, ai sensi dell'art. 26 della Convenzione, non potrà essere presa alcuna decisione, per il principio di parità delle armi che prevede che ogni parte legale, in questo caso la Federazione russa in qualità di convenuto, partecipi al contraddittorio, lasciando così i cittadini russi privi della tutela, fornita dalla CEDU, dei loro diritti fondamentali nei confronti di un Paese privo di una normativa adeguata al fine di evitare la violazione degli stessi[120] perché poco propenso a riconoscerli e, tantomeno, a garantirli.

In questo modo, verrà meno quel ruolo centrale che, in questi anni, hanno avuto il Consiglio d'Europa e il sistema di tutela giurisdizionale rappresentato dalla Corte europea dei diritti dell'uomo, che hanno vigilato sulla condotta delle Autorità russe, spesso pronte ad intervenire con misure repressive nei confronti degli oppositori politici al fine di scoraggiare, limitare e soffocare la loro attività[121] e di «sopprimere quel pluralismo politico che fa parte di una "democrazia politica effettiva" governata dallo "Stato di diritto", concetti ai quali fa riferimento il preambolo della Convenzione»[122].

---

[120] Sul punto, v. Corte EDU, *Navalny c. Russia*, ricorsi nn. 29580/12, 36847/12, 11252/13, 12317/13 e 43746/14, sentenza della Grande Camera del 15 novembre 2018, §§ 118; 148-151; 183; 185-186.

[121] Un esempio significativo della repressione attuata dalle autorità russe nei confronti dei dissidenti politici è quello che riguarda Alexej Navalny, uno dei principali oppositori politici del Presidente Vladimir Putin e *leader* della campagna anti-corruzione. A causa della sua attività politica, questo dissidente è stato più volte arrestato e ha subito, dopo l'espletamento di numerosi processi "pilotati" dal potere politico e senza la garanzia di un equo processo, diverse condanne per aver organizzato e/o partecipato a manifestazioni politiche non autorizzate, per diffamazione, per estremismo e per corruzione. Navalny ha più volte fatto ricorso alla Corte EDU lamentando la violazione da parte delle Autorità russe di alcuni suoi diritti fondamentali attinenti: alla libertà e alla sicurezza (art. 5 § 1 CEDU), ad essere sottoposto ad un equo processo (art. 6 CEDU), alla libertà di riunione e associazione (art. 11 CEDU), alla possibilità di impegnarsi politicamente in virtù del pluralismo politico (art. 18 CEDU). La Corte EDU non solo ha ammesso i ricorsi, ma, dopo aver riconosciuto la loro fondatezza, ha condannato la Federazione russa, v., *ex multis*, le seguenti sentenze: Corte EDU, *Case of Navalny and Ofitserov v. Russia. Applications nos. 46632/13 and 28671/14*, sentenza 23 febbraio 2016; Corte EDU, *Navalny c. Russia*, ricorsi nn. 29580/12, 36847/12, 11252/13, 12317/13 e 43746/14, sentenza del 2 febbraio 2018; Corte EDU, *Navalny c. Russia*, ricorsi nn. 29580/12, 36847/12, 11252/13, 12317/13 e 43746/14, sentenza della Grande Camera del 15 novembre 2018.

[122] Corte EDU, *Navalny c. Russia*, ricorsi nn. 29580/12, 36847/12, 11252/13, 12317/13 e 43746/14, cit., § 175.

## 6. Conclusione

Dopo aver affrontato i temi della libertà di informazione e del *free speech* nei Paesi democratici e nei Paesi autoritari, che, come abbiamo visto, presentano problematiche diverse ma ugualmente importanti, è possibile, a questo punto, trarre qualche conclusione.

Per quanto riguarda i Paesi liberal-democratici, dove ci si pone il problema di una regolamentazione delle piattaforme e dei *social* alla ricerca di assetti in grado di rendere effettiva la libertà di informazione e di espressione degli utenti di *Internet*[123], è possibile precisare alcuni esiti complessivi dell'analisi svolta in riferimento ad essi.

Un esito di grande importanza attiene al riconoscimento della necessità di non affidare alle piattaforme e ai *social media*, come *Facebook* e *Twitter*, che sono imprese private, estranee al circuito politico-rappresentativo e orientate alla ricerca del profitto, il potere di monitorare l'informazione e di ponderare discrezionalmente interessi dal momento che tali attività possono destrutturare e depotenziare «lo stesso sistema di *checks and balance* sotteso al principio democratico»[124], con possibili importanti ricadute negative sulla libertà d'espressione e sul pluralismo informativo.

Per questo, specialmente nell'Unione europea, si è progressivamente imposta la volontà di regolamentare le piattaforme alla luce di una strategia non volta ad indebolire la loro funzione nella società, dal momento che ormai non si può più prescindere da esse, ma a rendere più "equilibrato" il loro modello e a rafforzarlo in senso democratico, cercando di dar vita ad un sistema che vede regolatori pubblici e regolatori privati coesistere, attraverso il *public* e il *private enforcement*, nello stesso spazio regolatorio.

A tal fine, l'Unione europea si ripromette, cercando di disciplinare con il *DSA* il potere che di fatto le piattaforme detengono nell'odierna era digitale, di rendere effettiva la tutela dei diritti fondamentali della persona.

Dal momento che gli obiettivi che l'Unione europea si è imposta

[123] Sul punto è importante ricordare che il 28 aprile 2022 gli Stati Uniti, l'UE e numerosi altri Paesi, (alcuni dei quali, però, non particolarmente rispettosi dei principi democratici, ad esempio l'Ungheria e la Colombia) hanno firmato un "codice" di condotta, denominato *Declaration for the Future of the Internet*, teso a fissare principi generali e regole per l'uso di un *Internet* affidabile, sicuro e globale.

[124] P. Stanzione, *op. cit*., p. 14.

non sono certamente facili da raggiungere, sorge, fin da ora, la necessità di verificare nei prossimi mesi quale sarà l'effettiva implementazione del DSA e la difficile attuazione della co-regolazione che ne deriverà.

Passando ai Paesi autoritari si deve osservare che la "regolamentazione" delle piattaforme e dei *social* non è operata dai Governi in vista di un contenimento del potere delle grandi piattaforme a tutela del pluralismo dell'informazione e della libertà di pensiero, ma per sottoporle al potere politico, a fini di propaganda e di manipolazione dei cittadini per ottenerne il consenso.

Tale orientamento vede, sempre più, una acutizzazione della repressione della libertà di pensiero che è "giustificata" dai regimi autoritari, a seconda dei casi, come abbiamo visto, da esigenze legate alla guerra e/o dal timore di rivolte sociali antigovernative.

In questi Paesi, pertanto, non si scorge al momento la possibilità di qualche passo avanti a favore della democratizzazione della vita politica e del pluralismo.

A ben vedere, anzi, se consideriamo lo stato attuale delle cose, che vede una tendenza verso un crescente autoritarismo globale, almeno per il prossimo futuro, ci si deve attendere una regressione in senso autoritario, anche se, essendo la situazione interna dei Paesi illiberali "in movimento", non si possono escludere *a priori* inversioni di tendenza.

In generale, a chiusura dell'articolo, è di fondamentale importanza ribadire anche per i Paesi liberal-democratici «l'importanza essenziale del pluralismo, dell'apertura al confronto e alla discussione per la salute della nostra democrazia»[125], perché, quando si entra, come nel caso del conflitto russo-ucraino, in una logica di rifiuto del confronto e di opposizione totale fra due gruppi antagonisti, si determina l'impossibilità di comporre lo scontro, mentre dovrebbe essere «il tempo dei "costruttori di pace"»[126].

Soltanto se ci si metterà su questa strada sarà possibile vivere in futuro in un mondo come quello desiderato da uno dei due Nobel per la Pace 2021: «*Now, please, with me, close your eyes. And imagine the world as it should be. A world of peace, trust and empathy, bringing out the best that we can be*»[127].

---

[125] A. Nicita, *op. cit*., p. 27.

[126] G. Azzariti, *La Costituzione rimossa*, in Costituzionalismo.it, n. 1/2022, parte I, p. II.

[127] M. Ressa, *Nobel Peace Prize lecture*, Oslo, 10 Dicembre 2021.

* * *


## Abstract

### Ita

Lo scritto affronta il problema della libertà di parola e di informazione nell'età digitale, mettendo a confronto i Paesi liberal-democratici e i Paesi illiberali. Nella prima parte del contributo si mostra come nei Paesi democratici le piattaforme e i *social media*, attraverso gli algoritmi, confezionano messaggi *ad hoc* sui vari destinatari e li racchiudono in *echo chamber*. Ciò determina una crescente polarizzazione fra gli utenti che spesso li spinge a ricorrere all'*hate speech* e limita fortemente il *free marketplace of ideas*. Preso atto delle appena menzionate problematiche, il legislatore europeo si è impegnato a regolamentare il potere dei giganti del *Web* dando vita al *Digital Service Act*. Nella seconda parte è affrontato il problema dell'uso strumentale della rete da parte dei regimi autoritari, con particolare riferimento alla Federazione russa. La Legge federale n. 90 del 2019, denominata *Programma nazionale di economia digitale*, ha gettato le basi dell'*Internet* russo (*RuNet*) separato dalla struttura globale di *Internet*. Attraverso *RuNet* la Federazione russa non soltanto potrà proteggere la sicurezza nazionale per evitare *cyber* attacchi (obiettivo ufficiale), ma avrà anche la possibilità di sorvegliare i cittadini russi, obiettivo non certamente secondario della legge sull'*Internet* sovrano russo.

### En

This essay deals with the problem of freedom of speech and information in the digital age by comparing liberal-democratic countries and illiberal countries. The first part of the paper shows how platforms and social media in democratic countries create *ad hoc* messages on the various receivers and enclose them in echo chambers through algorithms. This leads to a growing polarization among users that often pushes them to recourse to hate speech and severely limits the free marketplace of ideas. Bearing this in mind, the European legislator has committed itself to regulating the power of Tech Giants by drafting the *Digital Service Act*. In the second section the issue of the instrumental use of the network by authoritarian regimes is addressed, with particular reference to the Russian Federation. Federal Law No. 90 of 2019, referred to as the *National Program of Digital Economy*, laid the foundations of the Russian Internet (*RuNet*) as opposed to the global structure of Internet. Through *RuNet* the Russian Federation will not only be able to protect national security and avoid cyber-attacks (official target), but will also have the opportunity to monitor Russian citizens, which certainly does not represent a secondary objective of the Russian sovereign Internet law.

# *Costituzionalismo.it*

*Email: info@costituzionalismo.it*
*Registrazione presso il Tribunale di Roma*
*ISSN: 2036-6744 | Costituzionalismo.it (Roma)*