Center for European Studies

www.centereuropeanstudies.it

CES WORKING PAPERS 2025/04

ISSN (online): 2384-969X
ISSN (print): 2385-0310
ISBN 979-12-80042-30-9
https://www.centereuropeanstudies.it/cse/working-paper

Dipartimento di Studi Politici e Sociali
UNIVERSITÀ DEGLI STUDI DI SALERNO

CES WORKING PAPERS 2025/04

I Working Papers sono una Collana edita dall'Università degli Studi di Salerno
Tutti i testi pubblicati sono preventivamente sottoposti a due referees anonimi.

Center for European Studies (CES)

Direttore: Massimo Pendenza
Dipartimento di Studi Politici e Sociali
Università degli Studi di Salerno
Indirizzo: Via Giovanni Paolo II, 132
84084 Fisciano (Salerno), Italy
Tel: +39 (0)89 962282 Fax: +39 (0)89 963013
Email: direttore@centrostudieuropei.it

www.centereuropeanstudies.it

L’impatto della legislazione europea sulle piattaforme digitali tra costituzionalismo digitale e autonomia del sociale

Marco Deseriis

Abstract

L’articolo analizza la regolamentazione europea sulle piattaforme digitali, ricostruendone l'evoluzione da un approccio liberale orientato allo sviluppo del mercato unico a uno di tipo costituzionale volto a estendere i diritti fondamentali dei cittadini europei nella sfera digitale. Muovendo dallo schema teorico di Lawrence Lessig, il paper dimostra come la centralità infrastrutturale delle piattaforme abbia generato una concentrazione di potere che l’UE tenta di limitare tramite strumenti normativi come la Gdpr e il Digital Services Act. Tuttavia, questa legislazione, pur accrescendo la responsabilità delle piattaforme, indebolisce l’autonomia regolatrice degli utenti stessi.

Keywords: Sovranità digitale; Costituzionalismo digitale; Piattaforme

Profilo Autore

Marco Deseriis è professore associato presso la Classe di Scienze Politiche e Sociali della Scuola Normale Superiore, dove insegna sociologia dei processi culturali e comunicativi. È autore dei volumi *Piattaforme e partecipazione politica* (Mondadori 2024) e *Improper Names: Collective Pseudonyms from the Luddites to Anonymous* (University of Minnesota Press 2015). In passato ha ottenuto borse di ricerca post-dottorali come la Marie Curie Fellowship e la Andrew Mellon Foundation Fellowship, detenendo anche diversi incarichi in università come la New York University, la New School e Northeastern.

Email marco.deseriis@sns.it

L’impatto della legislazione europea sulle piattaforme digitali tra costituzionalismo digitale e autonomia del sociale

Marco Deseriis

Indice

1. Introduzione

In *Code and other laws of cyberspace*, un influente volume pubblicato sul finire degli anni Novanta, il costituzionalista americano Lawrence Lessig osserva che i navigatori del Web sono sottoposti a quattro tipologie di vincoli: il codice digitale, la legge, il mercato e le norme sociali. Lessig (1999) paragona il codice a una forma di architettura o di legge in grado di condizionare i comportamenti dei navigatori amplificandone o limitandone le libertà. Anche il diritto, l'economia di mercato e le norme sociali, osserva Lessig (*Ib.*), influenzano la navigazione nel cyberspazio. Ma lo fanno tramite la mediazione del codice digitale, il quale può essere configurato per rispondere ai requisiti provenienti dagli altri tre vincoli. Il codice può essere infatti programmato per far rispettare e applicare direttamente la legge, come nel caso di filtri software che riconoscono e bloccano automaticamente la diffusione di contenuti protetti da copyright. Analogamente, nel caso dell'economia di mercato, il codice viene impiegato per trasferire sul Web transazioni commerciali, come nel caso dell'e-commerce, o per creare nuove tipologie di mercato, come nel caso della raccolta e della compravendita di dati. Infine, il codice digitale può essere utilizzato per far rispettare norme sociali condivise, offrendo, ad esempio, ai gestori di una mailing list la possibilità di filtrare i messaggi, o la possibilità per gli amministratori dei social di raccogliere segnalazioni degli utenti su contenuti non graditi.

Sebbene il libro di Lessig sia stato pubblicato prima della nascita dei social media, esso fornisce ancora oggi un utile punto di partenza per cogliere la relazione tra architettura digitale, regolamentazione legislativa, economia di mercato e norme sociali. In questo articolo, adottiamo le categorie analitiche sviluppate dal giurista americano a partire però dalla constatazione di due cambiamenti fondamentali rispetto alla internet degli anni Novanta: la centralità delle piattaforme nell'attuale ecosistema digitale; e il ruolo di primo piano assunto dall'Unione europea nel regolamentare l'operato delle imprese che controllano oggi gran parte del codice, dell'infrastruttura e del traffico di internet. Il punto di partenza del paper è che se, come scrive Lessig (*Ib.*, p. 3), il *codice è legge* (*code is law*), allora la scelta dell'Unione europea di legiferare *sul* codice è una scelta sovrana. O, più precisamente, è una decisione politica che esprime la volontà delle istituzioni europee di *non* cedere sovranità alle grandi imprese di big tech. La legislazione europea punta infatti a proteggere diritti fondamentali dei cittadini europei quali il diritto alla privacy e protezione dei dati personali, all'informazione e alla libertà

d'espressione, alla sicurezza e alla salute fisica e mentale della persona, in particolare dei minori. Da un lato, l'ampiezza e la specificità dei regolamenti corrispondono all'evoluzione storica e materiale della sfera digitale. Come vedremo, è l'ampio ventaglio dei servizi di intermediazione digitale offerti oggi dalle piattaforme a rendere necessaria una legislazione articolata su molteplici livelli. Dall'altro, la legislazione dipende inevitabilmente da decisioni politiche soggettive.

Come argomentato da diversi studiosi di diritto costituzionale, i termini contrattuali (*Terms of service*) con cui le piattaforme definiscono unilateralmente il rapporto con i propri utenti, le porta di fatto a svolgere funzioni di governo che sono proprie dell'autorità pubblica (Suzor 2018; Celeste 2019; De Gregorio 2021). Tuttavia, poiché i ToS sono un contratto privato definito unilateralmente da un'azienda e non un patto tra governanti e governati, «in termini legali, ha poco senso parlare di 'diritti' in queste transazioni commerciali» (Suzor, 2018, p. 3). Eppure, nel corso degli anni, e in modo sempre più chiaro e definito a partire dagli anni Dieci, la legislazione europea ha progressivamente esteso i diritti fondamentali dei cittadini europei alla sfera digitale, limitando così l'autonomia delle piattaforme digitali. Questo processo ha preso corpo in primo luogo tramite una serie di decisioni *giuridiche* – in particolare, della Corte di giustizia europea – che hanno imposto alle piattaforme una crescente trasparenza e responsabilità (*accountability*) nella gestione dei dati e dei contenuti postati dagli utenti (De Gregorio 2022). In secondo luogo, diverse decisioni *politiche* hanno generato una serie di strumenti legislativi volti a ricondurre le attività degli intermediari digitali nel perimetro dello stato di diritto (*rule of law*). Come vedremo, due eventi storici dall'alto valore simbolico hanno contribuito ad accelerare tali decisioni: le rivelazioni di Edward Snowden sulla sorveglianza di massa tramite internet; e lo scandalo di Cambridge Analytica sull'uso non autorizzato dei dati personali degli utenti dei social per scopi di propaganda politica.

Nel complesso, la legislazione europea sul digitale può essere suddivisa in due macro-periodi. Nel primo periodo, che va dalla metà degli anni Novanta all'inizio degli anni Dieci, l'Unione adotta un approccio liberale, finalizzato allo sviluppo del mercato digitale europeo, concentrandosi da un lato sull'armonizzazione delle legislazioni degli stati membri e dall'altro sugli investimenti e il potenziamento delle infrastrutture digitali. Nel secondo periodo, che ha inizio negli anni Dieci, l'Unione adotta un approccio costituzionale, che estende i diritti fondamentali nella sfera digitale, aumentando gli oneri per i gestori dei servizi di intermediazione nella

gestione dei dati personali e nella moderazione dei contenuti. L'atto legislativo che segna il passaggio alla seconda fase è la Gdpr, il cui approccio si basa sulla valutazione e la mitigazione del rischio (*risk-based approach*). Tale approccio, fondato sulla responsabilizzazione del soggetto regolato, verrà poi esteso negli anni Venti al Digital Services Act e all'AI Act. Come vedremo, sono i gestori dei servizi di intermediazione digitale a dover identificare i rischi derivanti dalle loro stesse attività e a dover dimostrare di aver adottato le misure necessarie a minimizzarli. Se questa impostazione lascia alle piattaforme un certo margine di discrezionalità, il tentativo dell'Unione di incrementare il potere degli attori sociali nella moderazione dei contenuti rimane tuttavia incompleto. L'argomento conclusivo del paper è che nel contenzioso attualmente in corso tra l'Unione e big tech, a essere indebolita è proprio la capacità regolatrice delle norme sociali, ovvero la capacità degli utenti di internet di intervenire sui meccanismi e le norme alla base dello scambio comunicativo. Ciò non è dovuto tanto a un'assenza di volontà politica da parte degli utenti, quanto a una trasformazione delle condizioni sociotecniche che ne hanno progressivamente esautorato la capacità di incidere sull'ambiente in cui comunicano.

Nel paragrafo 2, il paper si concentra su questa trasformazione, dimostrando come l'ascesa delle piattaforme sia dovuta a diversi fattori, tra cui la capacità di porsi come intermediare tra diversi gruppi di utenti e di trarre vantaggio dal controllo delle infrastrutture per rafforzare la propria posizione dominante. Il paragrafo 3 ricostruisce la prima fase della regolamentazione europea, evidenziando una contraddizione implicita tra le normative volte a facilitare la formazione di un mercato unico del digitale e la volontà politica di proteggere i dati personali degli utenti. La sezione successiva, dedicata alla seconda fase della legislazione, è suddivisa in tre sottosezioni. Il paragrafo 3.1. discute il quadro normativo basato sulla valutazione del rischio della Gdpr e l'impatto di quest'ultima sulla capacità delle grandi corporation digitali di estrarre valore dai dati. Il paragrafo 3.2 analizza il Digital Services Act, una delle più ambiziose legislazioni al mondo in materia digitale, e in particolare la regolamentazione dei sistemi di moderazione e di raccomandazione algoritmica dei contenuti. Il paragrafo 3.3. mette in evidenza come questi ultimi non abbiano solo implicazioni sociali e politiche, ma anche economiche: la Platform-to-Business Regulation e il Digital Markets Act hanno infatti l'obiettivo di rendere il mercato digitale europeo effettivamente concorrenziale. Nella sezione conclusiva, il paper rivisita lo schema teorico di Lessig per osservare come una maggiore capacità di autoregolazione degli attori

sociali richiederebbe un'architettura digitale completamente diversa, basata su una maggiore autonomia delle forze sociali dal potere infrastrutturale delle piattaforme.

2. Il potere infrastrutturale e l'architettura digitale delle piattaforme

«Le piattaforme sono quello che fanno», scrive il teorico dei media Benjamin Bratton (2015, p. 40). «Esse aggregano elementi in insiemi temporanei di ordine superiore e, in linea di principio, aggiungono valore sia a quanto viene portato sulla piattaforma che alla piattaforma stessa». Sebbene i gestori della piattaforma e gli utenti beneficino entrambi, *in linea di principio*, del valore aggiunto generato, in pratica i primi ne estraggono un valore incomparabilmente più alto dei secondi. Ciò avviene in virtù della capacità delle piattaforme di porsi come intermediarie tra gli utenti, registrandone al contempo le transazioni. I dati raccolti vengono poi utilizzati dai gestori per un'ampia gamma di scopi, come «ottimizzare i processi produttivi, fornire informazioni sulle preferenze dei consumatori, controllare i lavoratori, gettare le basi di nuovi prodotti e servizi (le auto a guida autonoma, Siri) e venderli ai pubblicitari» (Srnicek 2017, pp. 40-41). Le piattaforme non si limitano infatti a ospitare diverse tipologie di servizi, ma sono definite in termini computazionali dalla loro *programmabilità*, ovvero dalla loro capacità di fornire accesso ad altre piattaforme, applicazioni e canali multimediali da cui raccolgono flussi aggiuntivi di dati.

Per descrivere la complessità e la scala planetaria di questa architettura multilivello, Bratton (2015) ha introdotto il concetto di *stack*, una megastruttura a più strati che va dai minerali utilizzati per produrre fisicamente le reti digitali ai servizi di *cloud*, dalle *smart cities* agli indirizzi e alle interfacce tramite cui gli utenti si connettono ai sistemi informatici. All'interno dello *stack* di Bratton le piattaforme occupano una funzione diagrammatica, in grado di illustrare il modo in cui i sei livelli di cui lo *stack* si compone -- la terra, il cloud, la città, l'indirizzo, l'interfaccia e l'utente -- sono sovrapposti e interconnessi. Come osserva Bratton, le piattaforme

> non cercano di determinare in modo rigido il rapporto tra causa ed effetto. Le piattaforme sono meccanismi generativi—motori che stabiliscono le condizioni di partecipazione

> secondo protocolli fissi (ad esempio, protocolli tecnici, discorsivi, formali). [...] Questo non significa che la neutralità formale di una piattaforma non sia strategica; una piattaforma darà una struttura ai propri livelli e ai propri *Utenti* in un modo e un'altra in un altro, dandosi così un suo ordinamento politico [*polity*]. È proprio per questo motivo che le piattaforme non sono solo modelli tecnici, ma anche modelli istituzionali (Ibid., p. 44).

Secondo la sociologa dei media José van Dijck (2021) la metafora dello stack presenta due limitazioni sostanziali. La prima è che le piattaforme non sono modelli chiaramente delineati. Poiché tendono a farsi infrastrutture e a gestire dati utilizzabili per diverse tipologie di business e in diversi settori, le piattaforme riconfigurano la distinzione tra pubblico e privato, tra ciò che governa e ciò che è governato. In secondo luogo, van Dijck osserva che «le piattaforme non sono tutte uguali e non sono sovrapposte [*stacked*] in modo casuale» (ibid, p. 2804). Per evidenziare la struttura gerarchica del web piattaformizzato, van Dijck ricorre alla metafora più tradizionale dell'albero, che suddivide in tre componenti: le radici, il tronco e i rami. Le radici rappresentano l'infrastruttura di base su cui è costruita internet, dal protocollo Tcp/Ip ai cavi sottomarini per il trasporto dati, dai dati center ai punti di interscambio tra reti appartenenti a sistemi diversi. Il tronco rappresenta servizi di intermediazione come i motori di ricerca, i sistemi di pagamento digitale, gli app store e i social media. E i rami rappresentano applicazioni e piattaforme settoriali, che dipendono a loro volta da servizi di piattaforma generalisti. La centralità del tronco fa sì che big tech controlli snodi essenziali per il passaggio delle informazioni: «Se hai bisogno di raggiungere un numero considerevole di utenti, devi passare per Facebook; per vendere prodotti a una clientela di massa, dipendi dalla rete di venditori di Amazon; per scaricare applicazioni, gli app store di Apple e Google sono colli di bottiglia inevitabili; e per reperire informazioni, devi passare per il territorio dei motori di ricerca di Google o Microsoft» (van Dijck, Ibid., p. 2809). Inoltre, le piattaforme sono interdipendenti. Ad esempio, i sistemi di cloud Amazon Web Services e Azure di Microsoft affittano server sia ad altre piattaforme generaliste come Apple che a piattaforme di settore come Airbnb ed Uber. A loro volta, social come Facebook e X dipendono dagli app store di Google ed Apple. E via dicendo.

Questo sistema di relazioni è intrinsecamente oligopolistico, il che spiega perché mentre le aziende di big tech sono nominalmente in competizione, esse difendono spesso i propri interessi in modo comune, chiedendo meno regolamentazione e utilizzando il proprio *potere infrastrutturale* per prevenire l'emergere di competitor.

Ad esempio, Amazon ha saputo sfruttare la propria posizione dominante nel settore del *cloud* e del commercio elettronico sia per acquisire le start-up che utilizzano maggiormente i server Aws che per promuovere prodotti e servizi di sua proprietà a spese degli utenti business del suo *marketplace*. Per questo motivo, Lina Khan suggerisce di aggiornare la legislazione antitrust con misure profilattiche che impediscano a «un'impresa dominante l'ingresso in un mercato che essa già serve come piattaforma, e quindi la competizione diretta con imprese che dipendono dalla [piattaforma] stessa» (2016, p. 793). Come vedremo nella prossima sezione, la legislazione europea ha recepito almeno in parte i suggerimenti di Khan (divenuta tra il 2021 e il 2025 chair della Federal Trade Commission) regolamentando due elementi centrali nel *core business* delle piattaforme: la gestione dei dati personali degli utenti; e gli algoritmi per la raccomandazione dei contenuti.

Tuttavia, il controllo che le piattaforme esercitano sulle infrastrutture non è solo una *causa* del loro potere ma anche un *effetto* della loro popolarità. Come osserva Srnicek (2017), le piattaforme devono il loro successo alla capacità di sfruttare gli effetti di rete (*network effects*), ovvero di sfruttare il valore aggiunto creato dagli utenti stessi. Ad esempio, il sistema dei *like* introdotto da Facebook crea utilità per gli utenti fornendo loro indicazioni sull'apprezzamento sociale dei contenuti. L'architettura dei *social network* di prima generazione, nati nella prima metà degli anni Duemila, costruisce tale apprezzamento a partire dalle reti sociali e gli interessi preesistenti degli utenti. Come è noto, la gestione algoritmica delle relazioni sociali volta a gratificare l'utente e a favorire il cementarsi di una miriade di identità di gruppo, ha finito per produrre una sfera pubblica socialmente frammentata e politicamente polarizzata, in cui gli utenti hanno maggiori probabilità di essere esposti alla disinformazione, alla propaganda e alle fake news (Pariser 2011; Sunstein 2017; Benkler, Farris & Roberts 2018; Vosoughi, Roi & Aral 2018; Cosentino 2020). Come vedremo nei paragrafi 3.1 e 3.2, la regolamentazione europea è intervenuta anche su questo aspetto, introducendo alcuni obblighi per le piattaforme in materia di moderazione e raccomandazione algoritmica dei contenuti volti a ridurre i rischi derivanti da questo tipo di architettura digitale.

3. La prima fase della regolamentazione europea: unificazione del mercato e protezione dei dati personali

La legislazione europea sul digitale è considerata tra le più avanzate e stringenti al mondo. Da un lato, essa è parte integrante del cosiddetto *effetto Bruxelles*, ovvero della capacità dell'Unione di influenzare indirettamente i mercati globali stabilendo standard rigorosi in diversi campi, dalla protezione ambientale alla sicurezza del cibo, dalla legislazione antitrust alla protezione della privacy (Bradford 2020). Dall'altro lato, essa è frutto di una condizione di relativa debolezza economica, dovuta per lo più alle limitate dimensioni delle imprese europee. Uno degli obiettivi dichiarati di legislazioni come il Digital Markets Act e il Digital Services Act è infatti quello di favorire la competitività delle imprese europee limitando al contempo lo strapotere economico di big tech.[1]

È importante tuttavia sottolineare come questo tipo di orientamento abbia iniziato a esplicitarsi soltanto a partire dagli anni Dieci. Nelle due decadi precedenti, l'Unione punta sull'integrazione del mercato digitale europeo, concentrandosi da un lato sull'armonizzazione delle legislazioni degli stati membri e dall'altro sullo sviluppo di una normativa atta a facilitare il commercio elettronico all'interno del mercato unico. Queste due direttrici sono evidenti nei due provvedimenti di maggior rilievo della prima fase: la Data Protection Directive (1995/46/EC) e la e-Commerce Directive (2000/31/EC). La prima, che verrà sostituita nel 2016 dalla General Data Protection Regulation, prevede una serie di oneri per i gestori di servizi digitali. Tra questi, vi sono l'obbligo di informare gli utenti sulla raccolta dei dati personali, di ottenerne il consenso, di esplicitare lo scopo della raccolta dei dati e di circoscriverne il trattamento in rapporto agli scopi dichiarati (*legitimate purpose*). Il secondo provvedimento, la e-Commerce Directive, getta le basi per la creazione del mercato digitale europeo, stabilendo il principio che i fornitori di servizi digitali debbano seguire le leggi dello stato membro di provenienza e non di quello in cui offrono servizi. La direttiva esenta inoltre gli intermediari digitali dalla responsabilità diretta per la trasmissione (*mere conduit*), la copia (*caching*) e l'archiviazione

[1] Con l'espressione big tech, ci riferiamo qui alle sette aziende con la maggior capitalizzazione di Borsa al mondo: Alphabet, Amazon, Apple, Meta, Microsoft, Nvidia e Tesla.

(*hosting*) di dati contenenti informazioni illegali, a patto che gli intermediari intervengano prontamente per rimuoverli una volta che ne sono venuti a conoscenza.[2]

In questo senso, la prima fase della regolamentazione europea sul digitale cerca di bilanciare due principi potenzialmente in contraddizione tra loro: il diritto alla privacy dei cittadini europei; e il diritto delle imprese digitali di fornire servizi che comportano la raccolta e il trattamento di dati personali. Sebbene la e-Commerce Directive esenti le imprese dalla responsabilità oggettiva per i dati prodotti e trasmessi dagli utenti, va tuttavia osservato che già negli anni Novanta, nel suo insieme, la normativa europea prevede oneri maggiori per le imprese rispetto a quelli previsti da normative americane equivalenti, come il Communications Decency Act del 1996 e il Digital Millennium Copyright Act del 1998. Per questo motivo, nel 2000, Unione europea e Stati Uniti stipulavano un accordo quadro, il *Safe Harbor agreement*, che consentiva il trasferimento dei dati personali degli utenti europei oltreoceano, a patto però che le imprese americane rispettassero le condizioni della normativa europea. Nell'ottobre 2015, tuttavia, la Corte di giustizia europea invalidava l'accordo, dichiarandolo incompatibile con la normativa europea sulla protezione dei dati personali.[3]

3.1. La seconda fase della regolamentazione europea: la Gdpr

Un fattore determinante nella decisione dell'Alta corte erano state le rivelazioni di Edward Snowden sulla sorveglianza elettronica globale della Nsa statunitense e degli altri membri delle Five Eyes. Queste aprono a tutti gli effetti la seconda fase della regolamentazione europea sul digitale, la quale si caratterizza per un aumento degli obblighi dei gestori in materia di protezione dei dati personali. Diversi autori osservano infatti che le rivelazioni del *whistleblower* americano finirono per cambiare i rapporti di forza all'interno istituzioni europee, rendendo vana la pressione lobbistica di big tech per annacquare il testo base della Gdpr (Rossi 2016; Kalyanpur e Newman 2019; Laurer e Seidl 2021).

[2] https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng.
[3] https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

Al di là di questo elemento contingente, la Gdpr segna un passaggio di fase a una nuova tipologia di regolamentazione basata sul principio di responsabilizzazione (*accountability*) del soggetto regolato. Come osservato, tale principio, enunciato nell'articolo 5, paragrafo 2, viene attuato tramite il ricorso a un modello normativo basato sulla valutazione del rischio.[4] In pratica, il titolare del trattamento (*data controller*) e il responsabile del trattamento (*data processor*) dei dati devono valutare il livello di rischio che le proprie attività comportano per la protezione della privacy e dei dati personali degli utenti, sviluppando la strategia migliore per minimizzare i rischi identificati.[5] Qualora il titolare e il responsabile del trattamento non effettuino un'adeguata valutazione dei rischi e non adottino le misure tecniche e organizzative volte a minimizzarli questi saranno ritenuti responsabili e passibili di sanzioni.[6]

Adottando un approccio basato sulla protezione dei dati *by design and by default*, la Gdpr sostituisce e rafforza la Direttiva 1995/46 sotto diversi punti di vista. In primo luogo, trattandosi di una regolamentazione, la Gdpr ha il valore immediato di legge in tutti gli stati membri dell'Unione. In secondo luogo, essa estende gli obblighi sul trattamento dei dati personali a tutti i fornitori di servizi digitali, compresi quelli basati al di fuori dell'Unione. Terzo, la Gdpr comprende nella definizione di dato personale un ampio spettro di informazioni, includendo numeri IP, cookies, dati biometrici, genetici e di locazione geografica degli utenti. Quarto, il consenso informato viene rafforzato, costringendo i gestori a offrire agli utenti una chiara opzione di rifiutare il trattamento dei propri dati. Quinto, anche gli obblighi di trasparenza aumentano, visto che i gestori sono obbligati a fornire agli utenti una copia dei loro dati ogni qual volta questi ne facciano richiesta. Sesto, nel caso di incidenti comportanti la violazione dei dati personali, i gestori devono notificare l'avvenuta violazione (*data breach*) entro 72 ore all'autorità pubblica di riferimento. Settimo, la violazione delle norme contenute nella Gdpr comporta multe elevate, fino al 4% del fatturato totale di un'azienda.[7]

Nel complesso, quindi, la Gdpr limita la possibilità di estrarre valore dal bene più importante delle grandi corporation digitali, i dati degli utenti. Offrendo a questi ultimi la possibilità di negare il consenso per il trattamento, e costringendo i gestori

[4] https://gdpr-info.eu/art-5-gdpr.
[5] https://gdpr-info.eu/art-25-gdpr.
[6] https://gdpr-info.eu/art-82-gdpr.
[7] Nel maggio 2023, il gruppo Meta veniva multato 1,2 miliardi di euro per aver effettuato massicci trasferimenti di dati degli utenti europei di Facebook su server statunitensi, senza aver garantito un adeguato livello di protezione dei dati personali.

a limitare l'uso dei dati agli scopi dichiarati, la Gdpr riduce, almeno potenzialmente, il valore economico dei dati, impedendone la rivendita a soggetti terzi o il riutilizzo per scopi che esulano dall'ambito del servizio offerto. Tuttavia, la Gdpr non regolamenta direttamente il secondo *asset* delle piattaforme evidenziato da Khan (2016): gli algoritmi di raccomandazione dei contenuti (*recommender system*). Come vedremo nei paragrafi 3.2 e 3.3, gli algoritmi sono uno degli oggetti centrali della regolamentazione del secondo periodo, sia per le loro implicazioni sociali e politiche che per la loro rilevanza economica.

3.2. Il Digital Services Act

Come osservato, la seconda fase della normativa europea si caratterizza non solo per un'intensificazione degli oneri per i gestori di servizi digitali ma anche per un'estensione delle norme ad ambiti precedentemente deregolamentati. In particolare, il Digital Services Act (d'ora in poi, Dsa), approvato nel 2022 ed entrato in vigore nel 2023, prevede un ambiente digitale in cui i diritti fondamentali dei cittadini europei siano protetti e il più possibile al riparo da una serie di rischi, come la diffusione di informazioni illegali o dannose (*harmful*) per la dignità umana, per i processi democratici, per la salute fisica e mentale, per la sicurezza dei minori e per la parità di trattamento di diversi gruppi sociali.[8] Accanto a questo tipo di regolamentazione della vita sociale e politica, una seconda direttrice, di natura più strettamente economica, punta a creare un mercato digitale effettivamente concorrenziale, aggiornando la e-Commerce Directive tramite legislazioni come il DSA, la Platform-to-business Regulation e il Digital Markets Act.

Se le rivelazioni di Snowden hanno avuto l'effetto indiretto di rafforzare la normativa europea sulla privacy, vi sono pochi dubbi sul fatto che lo scandalo di Cambridge Analytica, scoppiato nel 2018 in seguito alle rivelazioni di un ex-dipendente della società, abbia avuto l'effetto di accelerare l'approvazione di una normativa pensata specificamente per le piattaforme digitali.[9] Lo scandalo rivelò

[8] Anche l'AI Act, approvato nel 2024, utilizza un impianto normativo basato sulla valutazione del rischio prevedendo livelli crescenti di regolamentazione in proporzione a quattro tipologie di rischio: minimo, limitato, alto e inaccettabile.

[9] Ciò è evidente da una serie di eventi verificatisi nello stesso 2018. Nel mese di aprile, Facebook informava la Commissione che i dati di 2,7 milioni di utenti europei erano stati utilizzati in modo non consensuale da Cambridge Analytica. Nel mese di maggio, l'audizione di Mark Zuckerberg al Parlamento

l'uso non autorizzato dei dati di 87 milioni di utenti Facebook per la creazione di spot elettorali personalizzati sulla base dei profili psicologici di ciascun utente, spingendo la Commissione a elaborare una legislazione volta a prevenire il ripetersi di simili incidenti. In particolare, il Dsa punta a proteggere diritti fondamentali dei cittadini europei, come il diritto a essere informati e alla libertà d'espressione, stabilendo maggiori responsabilità per i servizi di intermediazione digitale in relazione alla diffusione di contenuti illegali e dannosi per gli utenti. Se la e-Commerce Directive esentava gli intermediari digitali dalla responsabilità diretta per la trasmissione, la copia e l'archiviazione dei dati, il Dsa riconosce che le piattaforme digitali, in particolare quelle con più di 45 milioni di utenti (denominate Very Large Online Platforms, o Vlop, e Very large Online Search Engines, o Vlose), hanno delle responsabilità particolari nella gestione dei dati e dei contenuti dovute alle proprie dimensioni.

Come nel caso della e-Commerce Directive, le piattaforme non hanno l'obbligo di monitorare proattivamente i contenuti postati dagli utenti e possono evitare conseguenze legali se li rimuovono non appena ne vengono a conoscenza. Tuttavia, seguendo l'impianto *risk-based* della Gdpr, il Dsa prevede che Vlop e Vlose debbano condurre una valutazione dei rischi sistemici che i propri sistemi di raccolta e analisi dei dati, nonché di raccomandazione e moderazione dei contenuti, pongono in quattro aree: a) la disseminazione di contenuti illegali; b) l'esercizio dei diritti fondamentali dei cittadini europei; c) il discorso civico e i processi elettorali; e d) la violenza di genere, la protezione della salute pubblica e dei minori, e del benessere psicofisico della persona.[10] Vlop e Vlose sono inoltre tenute a offrire un sistema standardizzato per la segnalazione e la rimozione dei contenuti (*notice and action*) e a esplicitare le modalità con cui avviene la moderazione degli stessi.[11] Questo obbligo di trasparenza si applica anche all'*hosting* di utenti business e alla raccolta pubblicitaria: Vlop e Vlose devono mantenere un database contenente informazioni verificate degli utenti business

Europeo offriva più un'opportunità ai deputati di perorare la necessità di regolamentare le piattaforme digitali che non al Ceo di Meta di dimostrare la capacità di darsi delle regole proprie. Tra i vari interventi, a spiccare fu Guy Verhofstadt, ex premier belga e presidente del gruppo liberale Alde. Paragonando Zuckerberg a un genio che ha perso il controllo della propria invenzione, finendo per creare un "mostro digitale" potenzialmente in grado di distruggere la democrazia, Verhofstadt avvertì il fondatore di Facebook che in assenza di una sua cooperazione effettiva, le autorità europee non avrebbero esitato a sottoporre Meta e le altre piattaforme digitali a una regolamentazione molto più stringente di quella esistente. A giugno, il Consiglio d'Europa chiedeva alla Commissione europea di stilare un piano d'azione coordinato per combattere la disinformazione in vista delle elezioni europee del 2019.

[10] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html.

[11] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_15.html.

(art. 30);[12] e un database delle inserzioni pubblicitarie (art. 39), rendendole accessibili a scopo di ispezione.[13] Queste due norme servono a scoraggiare la vendita di prodotti illegali, le truffe digitali e le pubblicità fraudolente, compresi gli spot elettorali manipolatori o basati sulla disinformazione. Inoltre, le piattaforme sono tenute a dare priorità alle segnalazioni provenienti da segnalatori attendibili (*trusted flaggers*), vale a dire organizzazioni della società civile ed enti pubblici certificati, specializzati nell'identificazione di contenuti illegali o comunque dannosi per i diritti degli utenti europei.[14] Infine, gli articoli 27 e 38 del Dsa stabiliscono che gli utenti debbano poter conoscere i parametri dei sistemi di raccomandazione algoritmica e debbano poter optare per sistemi non basati sulla raccolta dei dati personali e la profilazione.[15]

Nel complesso, quindi, il Dsa aumenta significativamente le responsabilità delle piattaforme, introducendo penalità elevate, fino al 6% del fatturato totale, per coloro che violano le norme in materia di trasparenza, moderazione dei contenuti e protezione degli utenti. Inoltre, il Dsa è una delle prime legislazioni a regolamentare i sistemi di ranking e raccomandazione dei contenuti, prevedendo che questi debbano essere aperti all'ispezione di soggetti indipendenti[16] e di ricercatori certificati in grado di analizzarli.[17] Per facilitare il compito di questi ultimi, nel 2023, il Dsa ha istituito l'*European Center for Algorithmic Transparency* (Ecat), con sede a Siviglia.[18] La missione dell'Ecat è condurre test sui sistemi algoritmici di Vlop e Vlose, in particolare dei sistemi di raccomandazione dei contenuti, valutarne l'impatto sociale nel breve, medio e lungo periodo, e identificare misure di mitigazione dei rischi sistemici sollevati dagli stessi (Panigutti et al. 2025).

[12] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_30.html.
[13] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_39.html.
[14] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_22.html.
[15] https://Dsa-observatory.eu/2024/11/22/the-regulation-of-recommender-systems-under-the-Dsa-a-transition-from-default-to-multiple-and-dynamic-controls/.
[16] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_37.html.
[17] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_40.html.
[18] https://algorithmic-transparency.ec.europa.eu.

3.3. La Platform-to-business regulation e il Digital Markets Act

L'apertura dei sistemi di raccomandazione dei contenuti all'ispezione di enti e ricercatori indipendenti è finalizzata non solo a verificare l'impatto degli algoritmi sulla società e la politica ma anche sull'economia europea. I *recommender systems* compaiono infatti anche in normative come la Platform-to-business Regulation (P2b), entrata in vigore nel 2019, e il Digital Markets Act (Dma), entrato in vigore nel 2023, il cui obiettivo primario è creare un mercato digitale equo e libero da abusi di posizione dominante.

Sebbene la P2b sia tra le legislazioni europee meno conosciute, essa sancisce il diritto degli utenti business delle piattaforme e dei motori di ricerca a un trattamento imparziale e trasparente. L'articolo 5 della P2b stabilisce che gli intermediari digitali debbano esplicitare nelle condizioni contrattuali i parametri utilizzati per determinare il ranking dei prodotti e dei servizi offerti dagli utenti business, nonché il peso attribuito a ciascun parametro.[19] Inoltre, l'articolo 7 stabilisce che gli intermediari digitali debbano rivelare l'esistenza di trattamenti differenziati per alcuni prodotti o servizi e le ragioni economiche, commerciali o legali che ne sono alla base.[20] Questa norma è completata e rafforzata dall'articolo 6 del Dma, il quale stabilisce che le piattaforme non possono riservare un trattamento preferenziale ai propri prodotti e servizi né utilizzare i dati prodotti dagli utenti business per competere con loro.[21]

Il Dma interviene inoltre sul potere infrastrutturale delle piattaforme introducendo la categoria di *gatekeeper* per designare sei grandi gruppi--Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft--i quali controllano a loro volta 23 servizi di piattaforma (*core platform services*) operanti in diversi settori.[22] Ad esempio, mentre Alphabet possiede servizi di piattaforma come Google Search, YouTube, Android, Maps e Chrome, Meta controlla servizi come Facebook, Instagram, Whatsapp, Messenger e Meta Ads. Da questa distinzione discendono una serie di norme finalizzate a prevenire pratiche anticoncorrenziali. L'articolo 7 obbliga inoltre i *gatekeeper* a rendere i propri servizi di piattaforma interoperabili con servizi

[19] https://eur-lex.europa.eu/eli/reg/2019/1150/oj/eng.
[20] Ibid.
[21] https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_6.html.
[22] https://digital-markets-act.ec.europa.eu/gatekeepers_en.

concorrenziali.[23] Al momento, infatti, gli utenti di Whatsapp non possono scambiare messaggi con utenti Telegram, mentre gli utenti di Apple iOS non possono comunicare direttamente con quelli di Google Android usando le applicazioni di messaggistica preinstallate nei rispettivi telefoni.[24] La normativa punta ad abbattere queste barriere costringendo i *gatekeeper* a fornire le interfacce necessarie all'interoperabilità tra servizi concorrenziali, limitando così la loro capacità di rinchiudere i propri utenti in ecosistemi digitali separati. Questo obbligo è complementare alla proibizione, esplicitata nell'articolo 5 del Dma, di incrociare dati personali generati da servizi di piattaforma appartenenti a un unico *gatekeeper* (ad esempio, Facebook e Whatsapp) o di iscrivere automaticamente gli utenti a più servizi controllati dallo stesso *gatekeeper*.[25] Lo stesso articolo prevede inoltre che i *gatekeeper* debbano lasciare i propri utenti business liberi di promuovere offerte dei propri prodotti e servizi su piattaforme esterne all'ecosistema del *gatekeeper* (una norma nota come *anti-steering*).

In breve, nel loro insieme, le norme del Dma puntano a ridurre la capacità dei grandi gruppi digitali di integrare verticalmente i propri servizi, costringendoli ad aprirsi orizzontalmente all'interscambio con servizi concorrenziali. Esse cercano inoltre di impedire ai giganti del digitale di sfruttare la propria posizione dominante per dare priorità, tramite gli algoritmi di raccomandazione, ai propri prodotti o per impedire l'utilizzo da parte degli utenti business di piattaforme concorrenziali con il proprio ecosistema.

4. Conclusioni

In questo paper, abbiamo visto come nelle ultime tre decadi la normativa europea sul digitale si sia sviluppata lungo due direttrici: una direttrice economica e una direttrice sociale e politica. Mentre in una prima fase il legislatore puntava ad armonizzare le normative statali e a creare le condizioni per la nascita di un mercato digitale europeo unificato, a partire dagli anni Dieci l'Unione ha incrementato gli oneri per i gestori dei servizi di intermediazione digitale. In questo modo,

[23] https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_7.html.
[24] https://www.medialaws.eu/digital-markets-act-and-the-interoperability-requirement-is-data-protection-in-danger.
[25] https://www.eu-digital-markets-act.com/Digital_Markets_Act_Article_5.html.

l'approccio basato sulla valutazione del rischio (*risk-based approach*) adottato da legislazioni come la Gdpr, il Dsa e, più recentemente, l'AI Act ha fatto sì che le esenzioni *safe harbor* degli anni Novanta siano state progressivamente integrate con misure che richiedono alle piattaforme una maggiore responsabilità nella gestione dei dati e dei contenuti postati dagli utenti. In questo senso, legislazioni come la Gdpr, il Dsa e il Dsa segnano un passaggio di fase dal *safe harbor* degli anni Novanta al *responsible harbor* attuale, in cui i *gatekeeper* vedono aumentare obblighi di trasparenza e due diligence in diverse aree, come la verifica dell'identità degli utenti business, la trasparenza dei sistemi di raccomandazione e degli algoritmi di *ranking* di contenuti, i criteri di moderazione, l'interoperabilità, e la possibilità per gli utenti di inviare segnalazioni ed effettuare ricorsi.

Tuttavia, responsabilità, trasparenza, e *due diligence* richiedono investimenti in risorse umane e tecnologiche. L'attuale contesto politico sembra però essere caratterizzato dal tentativo dei gestori delle piattaforme, o quantomeno di alcune di esse, di *deresponsabilizzarsi* e sottrarsi il più possibile dagli obblighi previsti dalle normative europee. Ad esempio, l'acquisizione di Twitter da parte dei Elon Musk nel 2022 e il conseguente licenziamento dell'80% della sua forza lavoro ha portato il magnate sudafricano ad affidare la moderazione di X a sistemi basati su filtri automatici e agli utenti stessi del social. Analogamente, nel gennaio 2025, Mark Zuckerberg annunciava che il gruppo Meta avrebbe ridotto drasticamente il numero dei moderatori di Facebook, Instagram e Threads per adottare un modello simile a quello delle Community Notes di X. Questo prevede che utenti autorizzati segnalino post che ritengono falsi o inaccurati, allegandovi una nota di contesto contenente informazioni aggiuntive.[26] La nota viene pubblicata da un algoritmo nel momento in cui riceve una valutazione sufficientemente alta da utenti di diverso orientamento politico, garantendone, presumibilmente, l'imparzialità.[27] In questo senso, si può dire che i proprietari dei social stiano tentando di elevare le *norme sociali* -- una delle quattro categorie del modello di Lessig (1999) discusso all'inizio di questo paper -- a principio regolatore dei contenuti, accusando al contempo l'Unione

[26] Justin Hendrix, "Transcript: Mark Zuckerberg Announces Major Changes to Meta's Content Moderation Policies and Operations", *Tech Policy Press*, January 7, 2025. https://www.techpolicy.press/transcript-mark-zuckerberg-announces-major-changes-to-metas-content-moderation-policies-and-operations.

[27] E' stato tuttavia osservato che questo sistema genera un numero estremamente limitato di note pubblicabili, riducendo significativamente l'impatto del *fact-checking* basato sull'input degli utenti. Vedi Eric Fan, Rachael, Dottle e Kurt Wagner, "Twitter's Fact-Checking System Has a Major Blind Spot: Anything Divisive". *Bloomberg*, December 19, 2022. Archiviato dall'originale su https://web.archive.org/web/20221230133333/https://www.bloomberg.com/graphics/2022-twitter-birdwatch-community-notes-misinformation-politics.

europea di voler censurare la libertà di parola. Dal canto suo, la Commessione europea ha respinto le accuse di censura, sottolineando come le piattaforme siano libere di adottare i sistemi di moderazione e di *fact-checking* che ritengono opportuni, sottolineando però al contempo che essi debbano essere efficaci nel combattere la disinformazione.[28] La Commissione, inoltre, facendo leva sui poteri d'indagine che il Dsa le assegna, ha aperto indagini su X, TikTok, Facebook e Pornhub, accusandole di non proteggere gli utenti da diversi rischi, come la disinformazione e l'interferenza nei processi elettorali, la diffusione di discorsi d'odio e la mancata protezione dei minori. Analogamente, la Commissione si è servita dei poteri investigativi conferitile dal Dma per aprire indagini su *gatekeeper* come Alphabet, Apple e Meta, accusandoli di pratiche di mercato anti-competitive.[29]

Anche se gli esiti di queste indagini non sono ancora noti, la disputa legale tra l'Unione europea e big tech ha evidenti risvolti politici, come evidenziato dalle recenti dichiarazioni del presidente degli Stati Uniti sui paesi che adottano o intendono adottare regolamentazioni stringenti in materia digitale.[30] Tale disputa pone in primo piano il tema della sovranità digitale, che si configura in questo caso come un conflitto tra due tipologie di codice: il codice della legge e il codice digitale. Da un lato, come osserva Giovanni De Gregorio (2022), l'imponente apparato di regolamentazione europeo basato sulla valutazione del rischio cerca di bilanciare la necessità di creare un mercato digitale competitivo e aperto all'innovazione con la protezione dei diritti fondamentali dei cittadini europei. In questo senso, osserva De Gregorio (Ibid.), il *risk-based approach* adottato dal'Unione finisce per estendere il bilanciamento di interessi e valori, una funzione che è intrinsecamente costituzionale, alla sfera digitale. Dall'altro, il tentativo di responsabilizzare i grandi proprietari del codice digitale nella gestione del rischio finisce per delegare loro il compito di valutare rischi e misure di mitigazione necessarie. Certamente, nella sua evoluzione storica dalla Gdpr al Dsa all'AI Act la

[28] Philip Blenkinsop, "We do not censor media, EU says in response to Meta," *Reuters*, January 8, 2025. https://www.reuters.com/technology/we-do-not-censor-social-media-eu-says-response-meta-2025-01-08.

[29] Directorate-General for Competition, Directorate-General for Communications Networks, Content and Technology, "Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act", March 25, 2024. https://digital-markets-act.ec.europa.eu/commission-opens-non-compliance-investigations-against-alphabet-apple-and-meta-under-digital-markets-2024-03-25_en.

[30] Francesca Niola, "I Digital Act europei che sfidano Trump: Non cediamo sui diritti," *Agenda Digitale*, 5 settembre 2025. https://www.agendadigitale.eu/mercati-digitali/i-digital-act-europei-che-sfidano-trump-non-cediamo-su-diritti.

legislazione europea lascia sempre meno spazio alla discrezionalità, arrivando a definire preventivamente le categorie di rischio e gli oneri derivati (Dunn e De Gregorio 2022).

Tuttavia, è anche vero che le piattaforme dispongono di un ampio ventaglio di strumenti per gestire dati e contenuti come meglio credono. Il caso appena citato della moderazione dei contenuti è, in questo senso, emblematico. In un'ottica di razionalizzazione dei costi, i proprietari dei social ricorrono infatti sempre più alla moderazione automatica per le violazioni di alto livello (soprattutto contenuti pornografici, con finalità terroristiche, protetti da copyright o istiganti all'odio), mentre affidano sempre più agli utenti il compito di determinare la liceità e il valore di post controversi ma non manifestamente illegali. Va osservato che gli utenti non controllano in alcun modo i criteri di moderazione e i sistemi di raccomandazione dei contenuti, i quali sono integrati nell'architettura dei social a livello di progettazione e non possono essere in alcun modo modificati. Insomma, anche quando i social sembrano voler dare più potere agli utenti, lo fanno adottando una grammatica comunicativa che è innanzitutto funzionale a un modello di business basato sulla sorveglianza dei loro comportamenti, l'estrazione e la vendita dei dati.[31] Da questo punto di vista, la scelta dell'Unione di introdurre, tramite il Dsa, categorie privilegiate di segnalatori attendibili (*trusted flaggers*) per monitorare i contenuti dei social sembra essere quantomeno incompiuta o incompleta. I segnalatori sono infatti per lo più organizzazioni che rappresentano interessi industriali settoriali – soprattutto nel settore della protezione dei diritti di proprietà intellettuale – e non rappresentano in alcun modo l'articolazione della società civile in tutta la sua complessità.[32]

In conclusione, per tornare allo schema di Lessig con cui abbiamo introdotto questo *working paper*, il conflitto in corso tra l'Unione e big tech può essere rappresentato come un'arena discorsiva in cui si confrontano tre tipologie di forze: la *legge* statale, l'*architettura* del codice digitale e gli interessi dei fornitori di servizi di intermediazione nel *mercato* digitale. A essere sottorappresentato è invece il ruolo delle *norme* sociali, ovvero la capacità degli utenti di determinare

[31] Ad esempio, il like introdotto da Facebook è un simbolo altamente funzionale alla raccolta pubblicitaria perché consente di quantificare rapidamente l'apprezzamento sociale di un brand o di un prodotto. Per contro, come osserva Tufecki (2017), l'introduzione del simbolo del *dislike*, o del pollice verso, avrebbe potuto creare più di un imbarazzo a marchi non graditi dai consumatori o finiti nel mirino di campagne di boicottaggio.

[32] L'elenco dei segnalatori attendibili del DSA è disponibile a https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-Dsa.

autonomamente le regole di base dello scambio comunicativo. Per poter essere esercitata pienamente, tale capacità richiederebbe tuttavia l'implementazione di un'architettura digitale fondata su un'economia politica e un modello di business non estrattivisti. Sebbene questo modello sia presente in alcuni esperimenti di piattaforme cooperative e social alternativi, come Mastodon ad esempio (Sorci 2025), questi non sono complessivamente in grado di sfidare l'egemonia di big tech (Deseriis 2024). Tuttavia, la legislazione europea, abbinata a investimenti pubblici volti a facilitare la creazione di infrastrutture e piattaforme digitali di pubblica utilità, può creare le condizioni affinché ciò sia possibile. In questo senso, di fronte al «nuovo colonialismo di big tech» (Mejias e Couldry 2024), la regolamentazione europea della sfera digitale è una condizione necessaria per l'esercizio della sovranità digitale. Al tempo stesso, cittadine e cittadini europei potranno esercitare pienamente i propri diritti costituzionali solo quando avranno essi stessi un ruolo attivo nel determinare le condizioni socio-tecniche e le norme comunicative alla base della comunicazione digitale.

Riferimenti bibliografici

Benkler Y., Farris, S., Roberts, H. (2018), *Network propaganda. Manipulation, disinformation and radicalization in American politics*, Oxford University Press, Oxford.

Bratton B. (2016), *The stack: on software and sovereignty*, MIT Press, Cambridge (Mass.).

Celeste E. (2019), *Digital constitutionalism: a new systematic theorisation*, in «International Review of Law, Computers & Technology», vol. 33, n. 1, pp. 76–99. DOI: 10.1080/13600869.2019.1562604.

Cosentino, G. (2020), *Social media and the post-truth world order: the global dynamics of disinformation*, Palgrave, New York.

De Gregorio G. (2022), *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*. Cambridge University Press, Cambridge.

De Gregorio, G., Dunn, P. (2022), *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in «Common Market Law Review», vol. 59, n. 2, pp. 473–500 DOI: 10.54648/cola2022032.

Deseriis M. (2024), *Piattaforme e partecipazione politica*, Mondadori Università, Milano.

Kalyanpur, N., Newman, A.L. (2019), *The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation,* in «Journal of Common Market Studies», vol. 57, n. 3, pp. 448–67. DOI: 10.1111/jcms.12810.

Khan, L.M. (2016), *Amazon's antitrust paradox*, in «Yale Law Journal», vol. 126, pp. 710–805.

Laurer, M., Seidl, T. (2021), *Regulating the European data-driven economy: a case study on the General Data Protection Regulation*, in «Policy & Internet», vol. 13, n. 2, pp. 257–77. DOI: 10.1002/poi3.246.

Lessig L. (1999), *Code and other laws of cyberspace*, Basic Books, New York.

Mejias, U., Couldry N. (2024), *Data grab: the new colonialism of big tech and how to fight back*, University of Chicago Press, Chicago (IL).

Pariser E. (2011), *The filter bubble: what the internet is hiding from you*, Penguin, New York.

Rossi, A. (2016)*, Internet privacy in the European Union and the United States*. Tesi di dottorato, European University Institute, Firenze.

Sorci, G., (2025) *Server ribelli: R-esistenza digitale e hacktismo nel Fediverso in Italia*. Meltemi, Roma.

Srnicek N. (2017), *Platform Capitalism*, Polity, Cambridge.

Sunstein C. R. (2017), *Republic: divided democracy in the age of social media*, Princeton University Press, Princeton (NJ).

Suzor N. (2018), *Digital constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms*, in «Social Media + Society», vol. 4, n. 3. DOI: 10.1177/2056305118787812.

Tufecki, Z. (2017), *Twitter and tear gas: the power and fragility of networked protest*, Yale University Press, New Haven (CT).

Van Dijck, J. (2020), *Seeing the forest for the trees: visualizing platformization and its governance*, in «New Media & Society», vol. 23, n. 9, pp. 2801–2819. DOI: 10.1177/1461444820940293.

Vosoughi, S., Roi, D., Aral, S. (2018), *The spread of true and false news online*, in «Science», vol. 359, n. 6380, pp. 1146-1151. DOI: 10.1126/science.aap9559.

Center for European Studies (CES)

Working Papers

2014

14 | 01

Fabio Serricchio, *Cittadinanza europea e avversione alla moneta unica al tempo della crisi economica. Il caso italiano in prospettiva comparata.*

2015

15 | 01

Dario Verderame, *L'Europa in festival. Indagine sulle potenzialità e i limiti della partecipazione in ambito europeo attraverso uno studio di caso.*

15 | 02

Beatrice Benocci, *Tedeschi, europeisti nonostante tutto.*

15 | 03

Luana Maria Arena, *La regolamentazione del lobbying in Europa.*

2016

16 | 01

Vittorio Cotesta, *Max Weber e l'identità europea.*

16 | 02

Donatella Pacelli, *Two Paths of Analysing Totalitarianism in Europe. The Crises of Mankind in Kurt Wolff and Gugliemo Ferrero.*

16 | 03

Roberta Iannone, *Quale anima per quale Europa. Il pensiero nascosto di Werner Sombart.*

16 | 04

Andrea Salvini e Federica Ruggiero, *I NEET, l'Europa e il caso italiano.*

2017

17 | 01

Carlo Mongardini, *Carlo Curcio e l'idea di Europa.*

17 | 02

Massimo Pendenza, *L'Europa dei tradimenti. Il cosmopolitismo normativo europeo sotto attacco.*

17 | 03

Marco Di Gregorio, *La "creatività europea" e le sue retoriche.*

17 | 04

Irina Sikorskaya, *Intercultural education policies across Europe as responses to cultural diversity (2006-2016).*

2018

18 | 01

Larissa Titarenko, *Belarus and the European Union. From confrontation to the dialogue.*

18 | 02

Laura Leonardi, *La crisi dell'Europa. La "distruzione creativa" e le nuove solidarietà sociali.*

18 | 03

Giovanni Santambrogio, *Leaving the Euro. A feasible option for Italy?*

18 | 04

David Inglis, *Cosmopolitismi in tensione. L'Unione europea dal cosmopolitismo al neo-liberismo.*

Center for European Studies (CES)

Working Papers

2019

19 | 01 **Irina Sikorskaya,** *Reformation of higher education in the EaP countries: cultural dimensions under the shadow.*

19 | 02 **Vahe Khumaryan,** *Against European Hegemony Discourse. Vladimir Putin and Other Voics in the Post-2012 Russia.*

19 | 03 **Francesca Romana Lenzi,** *La sfida dell'identità per l'Europa.*

19 | 04 **Giuseppe Allegri,** *Per una European Social Union. Dal pilastro europeo dei diritti sociali a un Welfare multilivello?*

2020

20 | 01 **Ayse Aysu Sinik,** *Migration Policies of the European Union and Turkey with special consideration of the 2016 Readmission Agreement.*

20 | 02 **David Inglis,** *Durkheim, l'"Europa' e la Brexit.*

20 | 03 **Giovanni Moro,** *Locating European Citizenship.*

20 | 04 **Pietro Pasculli,** *Il 'percorso speciale' della Nuova Turchia: dalla corsa agli standard europei alle nuove ambizioni internazionali.*

2021

21 | 01 **Dario Verderame, Beatrice Benocci**, *Giovani e Europa: dinamiche nella maturazione di memorie autocritiche nei "nativi europei".*

21 | 02 **Andrea Girometti,** *Bourdieu e l'Europa: un rapporto a due dimensioni.*

21 | 03 **Irina Sikorska,** *Increasing imperative of the intercultural education in European policies, initiatives and actions.*

21 | 04 **Angela Mendola,** *Omogenitorialità sociale e pluralismo dei modelli familiari in Europa.*

2022

22 | 01 **Edoardo Toniolatti,** *I Verdi tedeschi fra Germania ed Europa: evoluzione e nuove sfide.*

22 | 02 **Ubaldo Villani-Lubelli,** *La guerra in Ucraina (2022), l'Unione Europea e il ruolo della NATO: un'analisi storico-politica.*

22 | 03 **Carlo Burelli, Niccolò Donati,** *Il valore della solidarietà per un'Unione Europea funzionale.*

22 | 04 **Pietro Pasculli,** *La leadership dell'Unione Europea nella politica climatica internazionale*

Center for European Studies (CES)

Working Papers

2023

23 | 01 **Matteo Gerli,** *Un progetto "in divenire". La politica europea della ricerca e dell'innovazione tra integrazione e differenziazione.*

23 | 02 **Massimo Pendenza,** *Un momento hamiltoniano? La risposta solidaristica dell'Unione europea alla crisi pandemica.*

23 | 03 **Vanessa Lamattina,** *Il sistema formativo europeo tra competizione e modello hayekiano di conoscenza.*

2024

24 | 01 **Beatrice Benocci,** *L'idea di un'Europa geopolitica. Una prima riflessione sui concetti di limes, impero e democrazia nella nuova percezione globale.*

24 | 02 **Edoardo Toniolatti,** *La Germania e le elezioni europee del 2024. Il caso AfD: prospettive e sviluppi*

24 | 03 **Guido Montani,** *Rivoluzione e federalismo. Riflessioni su violenza, guerra e pacificazione*

2025

25 | 01 **Luigi Cannella,** *L'Europa in bilico: osare o attendere?*

25 | 02 **Laura Bentivoglio,** *L'Europa "stampata". L'avvio del processo di integrazione europea attraverso gli articoli della Gazzetta del Mezzogiorno 1950-1957*

25 | 03 **Andrea Apollonio,** *EU Memory Politics: Shifting towards securitisation?*

25 | 04 **Marco Deseriis,** *L'impatto della legislazione europea sulle piattaforme digitali tra costituzionalismo digitale e autonomia del sociale*

Il Center for European Studies (CES), fondato nel 2012, promuove e valorizza la ricerca sulla società, la storia, la politica, le istituzioni e la cultura europea, mettendo assieme le conoscenze dei ricercatori di diverse aree disciplinari del Dipartimento di Studi Politici e Sociali (DiSPS) dell'Università degli Studi di Salerno. Compito del Centro è la promozione della discussione pubblica sul tema dell'Europa mediante l'organizzazione di seminari e convegni nazionali ed internazionali, la cura di pubblicazione di studi e ricerche, la presentazione di libri, la promozione di gruppi di studio e di ricerca anche mediante il reperimento di fonti di finanziamento presso enti privati, pubblici e di privato sociale.
Esso offre un supporto di ricerca scientifica e di pertinenti servizi alle attività didattiche di lauree triennali, magistrali e a master dedicati al tema dell'Europa e si propone di sviluppare e favorire contatti con enti, fondazione e Centri di altre università nazionali ed internazionali interessati alle questioni oggetto di ricerca da parte del Centro, anche attraverso lo scambio di ricercatori tra di essi.

Center for European Studies

www.centereuropeanstudies.it

CSE WORKING PAPERS 2025/04

Direttore: Massimo Pendenza
Dipartimento di Studi Politici e Sociali
Università degli Studi di Salerno
Via Giovanni Paolo II, 132
84084 Fisciano (Sa), Italy

Tel: +39 (0)89 962282
Fax: +39 (0)89 963013
Mail: direttore@centrostudieuropei.it

www.centereuropeanstudies.it