NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

Governing the ungoverned. Recenti proposte europee e internazionali per regolare il digitale*

di Flavia Zorzi Giustiniani **

In tema di diritto nel cyberspazio il quadrimestre qui in rassegna si segnala anzitutto per due proposte legislative, presentate dalla Commissione europea il 15 dicembre scorso, per dare attuazione alla Strategia Digitale Europea1: **il Digital Services Act**2 e il **Digital Single Market Act**3. Mediante tali iniziative la Commissione si propone di stabilire un apparato normativo unico in tutta la UE che renda il digitale uno spazio più aperto e sicuro nel rispetto dei valori e dei principi fondamentali dell'Unione4. In particolare le due proposte mirano, da un lato, ad aumentare l'innovazione e la competività europea e, dall'altro, a rendere la Rete più equa e aperta e porre un argine allo strapotere di quei pochi colossi privati che la dominano (le c.d. *Big Tech*); tutto ciò mediante una protezione effettiva dei diritti degli utenti nonché delle imprese e piattaforme digitali di piccole e medie dimensioni. Così facendo si colma una vistosa lacuna del sistema giuridico europeo, il cui quadro normativo in tema di servizi e mercati digitali è tuttora dettato da un atto, la direttiva 2000/31/CE sul commercio elettronico5, oramai del tutto inadeguato, malgrado i numerosi

* Contributo sottoposto a *peer review*.

** Ricercatrice di Diritto internazionale presso l'Università Telematica Internazionale UNINETTUNO.

[1] Il 21 novembre 2018 la Commissione Europea ha adottato la c.d. "Digital Strategy", allo scopo di promuovere una visione che possa traghettare l'Europa verso la creazione di una società attenta al digitale e ai diritti degli utenti (cfr. C(2018) 7118 final, https://ec.europa.eu/info/publications/EC-Digital-Strategy_en). Un'anticipazione delle due proposte legislative si trova poi nella Comunicazione della Commissione del 19 febbraio 2020 "Plasmare il futuro digitale dell'Europa" (COM(2020) 67 final). In tale Comunicazione la Commissione espone il suo approccio per rendere l'UE leader della trasformazione digitale facendo riferimento a tre pilastri: "Tecnologia al servizio delle persone", "Un'economia digitale equa e competitiva" e "Una società aperta, democratica e sostenibile".

[2] Cfr. COM(2020) 825 final, 15 dicembre 2020.

[3] Cfr. COM(2020) 842 final, 15 dicembre 2020.

[4] Come dichiarato dalla vicepresidente esecutiva della Commissione europea Margrethe Vestager (cfr. Eunews, Vestager: "Identità digitale europea e Digital services act proteggeranno la democrazia dell'UE", 30 ottobre 2020, https://www.eunews.it/2020/10/30/vestageridentita-digitale-europea-digital-services-act-proteggeranno-democrazia/136917).

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

ISSN 2279-7238

interventi chiarificatori della Corte di Giustizia in sede interpretativa6, a regolare un settore che si è sviluppato e modificato in modo dirompente nell'ultimo ventennio.

Non si tratta invero del primo tentativo in Europa di regolamentare il digitale e responsabilizzare le grandi piattaforme digitali, i cosidetti *gatekeepers* del Web. Già da diversi anni la Commissione chiede ai giganti della Rete di conformarsi ad un codice di condotta e pubblicare resoconti periodici sulla loro azione di moderazione di contenuti illegali e di incitazione all'odio7. Inoltre diversi Stati hanno fatto ricorso a disposizioni normative aventi efficacia vincolante per costringere le *Big Tech* a rimuovere immantinente i suddetti contenuti8. Nondimeno, l'inadeguatezza di tali soluzioni ed il rischio di una crescente frammentazione giuridica hanno indotto la Commissione ad elaborare ex novo un apparato di norme per dotare infine l'Unione di un quadro giuridico unico. Il nuovo pacchetto di riforme, da tempo atteso, si è poi rivelato tanto più necessario nell'attuale crisi pandemica, che ha amplificato a dismisura il ruolo di Internet e dei suoi *gatekeepers* in tutto il mondo.

Vediamo ora le due proposte nel dettaglio.

La proposta di regolamento **Digital Markets Act** (DMA) concerne gli aspetti commerciali e di concorrenza del settore digitale. L'obiettivo precipuo del DMA è quello di evitare comportamenti sleali e condotte manipolatorie da parte delle grandi piattaforme digitali così da consentire a tutti – singoli utilizzatori finali come piccole realtà imprenditoriali – di poter beneficiare appieno dell'economia digitale "in a contestable and fair environment"9. A tal fine il DMA impone una serie di obblighi in capo a quelle piattaforme che possano definirsi vere e proprie guardiane (*gatekeepers*) della Rete sulla base dei seguenti requisiti: a) avere un impatto significativo sul mercato interno; b) gestire un servizio di piattaforma essenziale che collega un gran numero di imprese ad una grande base di utenti; e c) avere (o essere in procinto di avere) una posizione radicata e durevole nel mercato10. I suddetti requisiti si presumono soddisfatti in presenza di taluni elementi qualitativi e quantitativi (come ad esempio fatturare almeno 6,5 miliardi di euro nella UE per il criterio sub lett. a)). I "controllori dell'accesso" così identificati dovranno adoperarsi per rimuovere le barriere all'ingresso sul mercato digitale di altri operatori e nello specifico adempiere ad una serie di obblighi di facere (ad es. permettere a terzi di interagire con i loro servizi in determinate situazioni) e non facere (ad es. non limitare la facoltà degli utenti di

[6] Particolarmente significative sono al riguardo le sentenze rese nei casi Scarlet Extended SA v. SABAM (sent. III sez. C-70/10 relativa all'art.15.1 della Direttiva e all'assenza di obblighi di controllo sui fornitori di servizi online) e Delfi AS v. Estonia (sent. 64668/09 relativa a un conflitto tra la libertà di espressione ex art. 10 Cedu e l'art. 14 della direttiva 2000/31, concernente le responsabilità degli *hosting providers*).

[7] Si veda in particolare il Codice di condotta del 2016 per contrastare l'illecito incitamento all'odio online (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct) nonché la comunicazione e la raccomandazione del 2018 della Commissione destinate a piattaforme online e Stati membri sulla lotta ai contenuti illeciti online (https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online).

[8] Cfr. ad esempio la legge tedesca contro le fake news e l'odio in rete (Netzwerkdurchsetzungsgesetz, NetzDG), in vigore dal 1° ottobre 2017.

[9] COM(2020) 842 final, p. 3.

[10] Cfr. art. 3.1 del DMA.

ISSN 2279-7238

disinstallare software o applicazioni pre-installate)11. Il mancato rispetto di questi obblighi comporterà sanzioni ingenti, corrispondenti ad un massimo del 10% del fatturato mondiale del *gatekeeper* interessato e, nel caso di violazioni sistematiche, financo la dismissione di determinate attività in assenza di alternative egualmente efficaci12. Alla Commissione europea, in quanto responsabile dell'*enforcement*, è poi assegnato il potere di svolgere indagini di mercato al fine di aggiornare detti obblighi alla luce di nuove pratiche anticoncorrenziali eventualmente rilevate13.

Il **Digitale Services Act** (DSA) ha invece come obiettivo precipuo quello di regolamentare i servizi digitali14 e più specificamente di stabilire le responsabilità dei fornitori di servizi di intermediazione online. Il quadro normativo vigente, incentrato come già accennato sulla direttiva E-Commerce, non viene interamente stravolto. Non a caso la proposta di regolamento non mette in discussione i cardini del regime di responsabilità come stabilito dalla direttiva e che è stato oggetto nel tempo di diversi interventi chiarificatori della Corte di giustizia. Il nuovo testo ripropone infatti la tripartizione tra servizi di *mere conduit*, *caching* e *hosting*, come pure il riferimento al *general monitoring ban*. Inoltre, ponendosi come framework generale, il DSA non pregiudica l'applicabilità dei diversi strumenti di *lex specialis* in vigore, quali ad esempio la Direttiva 2010/13/CE, come modificata dalla Direttiva (UE) 2018/1808, sulla piattaforma di video sharing per quanto riguarda i contenuti audiovisivi e le comunicazioni commerciali audiovisive15.

Le specifiche modifiche al quadro vigente mirano dunque a garantire essenzialmente un maggior grado di trasparenza e responsabilità stabilendo un regime differenziato per gli intermediari digitali.

Sono anzitutto previsti obblighi di *due diligence*, che vengono calibrati in funzione della natura dei servizi offerti nonché delle dimensioni degli intermediari e del loro impatto sul mercato16. Con l'obiettivo di garantire una maggiore trasparenza e di conseguenza una maggiore protezione dei consumatori si stabilisce inoltre l'obbligo, indistintamente per tutti gli intermediari, di riportare all'interno delle *terms and conditions* ogni restrizione o limitazione che i *providers* impongono in relazione all'uso dei loro servizi17. I soli fornitori di servizi di *hosting* – ovvero di conservazione di informazioni fornite dagli utilizzatori – sono invece tenuti a porre in atto, secondo una procedura standardizzata, dei meccanismi di *notice and take down* per la rimozione di contenuti illegali o lesivi di diritti a seguito di una semplice e rapida notificazione da parte dei singoli utenti interessati18. In caso di rimozione ovvero disabilitazione del contenuto, il fornitore dovrà poi fornire uno *statement of reasons* all'utente

11 Cfr. artt. 5-6 del DMA.
12 Cfr. artt. 26 e 16 del DMA.
13 Cfr. art. 10.1 del DMA.
14 Per servizi digitali si intendono tra l'altro i servizi degli intermediari online, come quelli relativi all'accesso ad internet, i servizi cloud, le piattaforme online, gli intermediari di contenuti, di merci o i servizi messi a disposizione da terzi.
15 Cfr. art. 1.5 del DSA per un'elencazione esaustiva di tale normativa di settore.
16 Cfr. il Capitolo III del DSA.
17 Cfr. art. 12 del DSA.
18 Cfr. art. 14.1 del DSA.

ISSN 2279-7238

che aveva inserito il contenuto in oggetto19. Assoluta priorità dovrà essere assegnata dai providers a quei segnalatori - i c.d. "trusted flaggers" - che possedendo delle particolari qualifiche e competenze enunciate dal DSA sono identificati come tali dal Digital Services Coordinator nazionale20. Infine, mentre le micro e piccole imprese ai sensi dell'allegato alla raccomandazione 2003/361/CE sono esenti dagli obblighi ulteriori posti dal DSA sulle piattaforme online21, un regime di responsabilità aggravata è invece previsto per quelle piattaforme ("very large online platforms") che raggiungono almeno 45 milioni di utenti nell'Unione (ovvero che rappresentano il 10% della popolazione europea). Queste dovranno, tra l'altro, con cadenza almeno annuale effettuare una valutazione dei rischi sistemici determinati dal o relativi al funzionamento e all'utilizzo dei propri servizi, adottare misure ragionevoli ed efficaci al fine di mitigare detti rischi e sottoporsi a proprie spese a controlli esterni e indipendenti22.

La proposta prevede infine l'istituzione di un apposito meccanismo di sorveglianza e di *enforcement* incentrato su due nuove figure, il Compliance officer e il Digital Services Coordinator. Il primo dovrà essere nominato esclusivamente dalle "very large online platforms" ed essere dotato delle qualifiche professionali e abilità previste dal DSA. Potrà essere anche una figura interna, a patto che svolga le sue mansioni in modo indipendente23. Il Digital Services Coordinator, invece, è una nuova autorità nazionale indipendente incaricata di vigilare sul rispetto del Regolamento in modo imparziale, trasparente e tempestivo. Sarà responsabile per tutte le questioni relative all'applicazione e al rispetto del DSA24.

Un altro sviluppo importante, stavolta sul piano giurisprudenziale, si deve alla Corte di Giustizia europea, che nella sentenza resa dalla sua Grande Sezione il 15 settembre scorso si è pronunciata per la prima volta sul **principio della *net neutrality*** (neutralità della Rete o Internet aperta)25. La pronuncia, resa in via pregiudiziale, trae origine da due controversie che vedevano opposti la società ungherese Telenor, fornitrice di accesso a Internet, e il Presidente dell'Autorità nazionale ungherese dei media e delle comunicazioni, che aveva ingiunto alla prima di porre termine ad alcuni servizi proposti ai suoi clienti tramite due pacchetti di accesso preferenziale (c.d. *zero-rating*, a "tariffa zero"). Lo *zero-rating* è una pratica commerciale del mercato della telefonia mobile che consiste nel fornire al consumatore un accesso gratuito ma al contempo limitato e condizionato ad Internet. Più precisamente, mediante tali pacchetti i fornitori di connettività privilegiano determinate applicazioni e i relativi servizi proponendoli a costo zero e assoggettano al contempo l'uso delle altre applicazioni e degli altri servizi a misure di blocco o di rallentamento. Com'é evidente una siffatta pratica commerciale, limitando i servizi che sono fruibili gratuitamente dai

[19] Cfr. art. 15 del DSA.
[20] Cfr. art. 19 del DSA.
[21] Cfr. art. 16 del DSA.
[22] Cfr. art. 26 del DSA.
[23] Cfr. art. 32 del DSA.
[24] Cfr. art. 38.1 del DSA. Al Digital Services Coordinatot é dedicata la Sezione 1 della Parte IV del DSA (artt. 38-46).
[25] Cfr. CGE, cause riunite C-807/18 e 39/19, Telenor Magyarország Zrt. contro Nemzeti Média- és Hírközlési Hatóság Elnöke.

ISSN 2279-7238

consumatori, è suscettibile di influenzare le scelte e le abitudini degli stessi26.

Adita da Telenor, la Corte ungherese aveva quindi interrogato la CGE circa la compatibilità di tali pacchetti con l'art. 3 del regolamento (UE) 2015/2120, del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica27 e con il regolamento (UE) 531/2012 del 13 giugno 2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

Va premesso al riguardo che, sebbene le pratiche di *zero-rating* non siano menzionate espressamente dal Regolamento, il Berec - l'agenzia europea che fornisce assistenza professionale e amministrativa all'Organismo dei regolatori europei delle comunicazioni elettroniche - nel 2016 aveva adottato delle linee guida che includevano siffatte pratiche nell'ambito di applicazione del medesimo28.

Nella sua pronuncia la Corte ha ritenuto anzitutto le offerte di Telenor in contrasto con l'art. 3, c. 1 e 2 del Regolamento in quanto limitano l'esercizio dei diritti degli utenti finali dallo stesso sanciti. Secondo la CGE, infatti, l'art. 3.2 prevede che gli accordi conclusi tra i fornitori di servizi di accesso ad Internet e gli utenti finali nonché le pratiche commerciali adottate dai primi non devono limitare l'esercizio dei diritti di cui all'art. 3.1, incluso il diritto di utilizzare contenuti, applicazioni e servizi tramite un servizio di accesso al web. Ne discende che la compatibilità di siffatti accordi con l'art. 3.2 di tale regolamento deve essere valutata caso per caso, alla luce dei parametri menzionati al considerando 7 del Regolamento29. È interessante notare, al riguardo, come la CGE abbia evidenziato che la nozione di "utenti finali" non coincide con quella di consumatori bensì include pure le persone fisiche o giuridiche che si servono dell'accesso a Internet per fornire contenuti, applicazioni e servizi30. I pacchetti che includono una tariffa zero sono idonei a limitare l'esercizio dei diritti degli utenti finali su una parte significativa del mercato e danneggiano pertanto non solo quanti utilizzano servizi di connettività per accedere a contenuti, applicazioni e servizi, ma anche i professionisti che, attraverso la rete, offrono tali contenuti e servizi31.

Con riguardo all'interpretazione del terzo paragrafo dell'art. 3 la Corte ha poi affermato

[26] E' notoria, al riguardo, l'offerta "Facebook Zero" con la quale alcuni operatori telefonici proponevano l'accesso gratuito ad una versione ridotta (di solo testo) del social media. Tale offerta, rivolta ai consumatori di numerosi Paesi africani, è stata considerata una forma di colonialismo digitale (cfr. O. Solon,"It's digital colonialism": how Facebook's free internet service has failed its users, «The guardian», 27 luglio 2017, https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets).

[27] In particolare con il disposto dell'art. 3, c. 1 e 2, che garantisce un certo numero di diritti agli utenti finali di servizi di accesso a Internet e che vieta ai fornitori di detti servizi di adottare accordi o pratiche commerciali che limitino l'esercizio di tali diritti, nonché dell'art. 3, c. 3, che sancisce un obbligo generale di trattamento equo e non discriminatorio del traffico.

[28] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, 30 agosto 2016.

[29] Cfr. par. 43 della sentenza.

[30] Cfr. par. 36-39 della sentenza.

[31] Cfr. par. 45-46 della sentenza.

ISSN 2279-7238

che le misure di gestione del traffico, seppure permesse dalla disposizione, devono comunque rispettare taluni requisiti. Questi ultimi attengono alla qualità tecnica del servizio e non possono invece basarsi su considerazioni di ordine commerciale32. In particolare, secondo la Corte "deve ritenersi fondata su tali «considerazioni di ordine commerciale» qualsiasi misura di un fornitore di servizi di accesso a Internet nei confronti di qualsiasi utente finale […] che porti, senza basarsi su tali requisiti, a non trattare in modo equo e senza discriminazioni i contenuti, le applicazioni o i servizi offerti dai diversi fornitori di contenuti, di applicazioni o di servizi"33. Le misure di rallentamento e blocco del traffico dei pacchetti *zero-rating* esaminati sono pertanto vietate in quanto contrarie al principio della *net neutrality* ex art. 3.3, e ciò indipendentemente dal loro impatto sull'esercizio dei diritti degli utenti finali34.

Un ulteriore sviluppo degno di nota, infine, è costituito dall'**Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means35**. Tale dichiarazione è il risultato di un seminario virtuale tenutosi il 20 ottobre scorso all'Università di Oxford e copatrocinato dall'Oxford Institute for Ethics, Law and Armed Conflict della Blavatnik School of Government, Microsoft e il governo giapponese. Al seminario hanno preso parte una settantina di esperti tra i quali avvocati internazionalisti, diplomatici, rappresentanti dell'industria e informatici. Ad oggi lo Statement è stato sottoscritto da più di 170 giuristi di diritto internazionale36. Si tratta della terza di una serie di dichiarazioni, adottate durante la pandemia del Covid-19, che enunciano una breve lista di norme e principi di diritto internazionale la cui applicabilità alle *cyber operations* può dirsi indiscussa37. L'intento di questo "Oxford Process", tuttora in corso, è quello di offrire un punto di riferimento chiaro ed essenziale agli Stati e agli altri *stakeholders* interessati sul contenuto della normativa internazionale applicabile a fattispecie di pressante attualità38. Un siffatto esercizio é lungi dall'essere ozioso perché, se la generale applicabilità del diritto internazionale nel cyberspazio pare oramai pacificamente accettata dagli Stati, ad essere ancora dibattuto é "the extent to which existing international rules or principles apply to this new area of state activity"39. Il terzo Statement disciplina in particolare una serie di

32 Cfr. par. 48 della sentenza.

33 *Ibid.*

34 Cfr. par. 50 della sentenza.

35 Cfr. https://www.elac.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through.

36 Un elenco aggiornato é disponibile al link sovraindicato.

37 Cfr. Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health-Care Sector, 21 maggio 2020 (disponibile al link https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea); e The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, 7 agosto 2020 (disponibile al link https://www.elac.ox.ac.uk/article/the-second-oxford-statement).

38 "As with the prior two Oxford Statements, the goal of the present Statement is not to cover all applicable principles of international law, but rather, to articulate a short list of consensus protections that apply under existing international law to foreign cyberoperations with adverse consequences on electoral processes […]" (https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means/).

39 Cfr. D. Akande, A. Coco, T. de Souza Dias, Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond, 5 gennaio 2021, https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

ISSN 2279-7238

obblighi negativi e positivi per gli Stati così suddivisi: Duty to Refrain; Duty Not to Render Assistance; Due Diligence; Obligation to Protect Against Foreign Electoral Interference. Richiamando da un lato testi normativi fondamentali, quali la Carta ONU e il Patto internazionale sui diritti civili e politici, e dall'altro recenti strumenti settoriali quali gli UN Guiding Principles on Business and Human Rights40 e la Joint Declaration on Freedom of Expression and Elections in the Digital Age41, lo Statement afferma tra l'altro che gli Stati devono astenersi dall'effettuare operazioni cibernetiche che hanno conseguenze negative per i processi elettorali in altri Stati e dal fornire assistenza a tali operazioni, come pure proteggere e garantire l'integrità dei propri processi elettorali dalle interferenze di altri Stati.

[40] UN Office of the High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework'(2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[41] Declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, and the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, 30 aprile 2020, https://www.ohchr.org/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf.

ISSN 2279-7238