RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 2-2021
DOI: 10.32091/RIID0036

Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità

Maria Romana Allegri

Il "pacchetto digitale" proposto dalla Commissione europea a dicembre 2020 segna l'affermazione dell'Unione come centro di potere sovrano sull'ambiente digitale, non solo rispetto alle grandi imprese multinazionali che gestiscono il flusso di informazioni in Internet, ma anche rispetto agli Stati nazionali, i quali vanno via via perdendo la possibilità di disciplinare in modo autonomo i fenomeni che avvengono online. Per realizzare tale obiettivo, la Commissione europea si è mossa principalmente lungo tre direttrici: 1) il *data sharing* per lo sviluppo di sistemi di intelligenza artificiale; 2) un maggiore controllo sui *gatekeeper* (cioè sulle piattaforme digitali in grado di condizionare l'accesso al mercato) onde evitare che essi possano abusare della loro posizione dominate; 3) una maggiore responsabilizzazione degli intermediari digitali per i contenuti prodotti e diffusi dagli utenti finali dei loro servizi, prestando particolare attenzione alle piattaforme di grandi dimensioni. Viene così scardinato il principio della neutralità del provider, sancito dalla direttiva europea sul commercio elettronico risalente al 2000. Attraverso la riaffermazione della propria "sovranità digitale" l'Unione europea sembra voler rivendicare la sua natura di spazio di libertà e di diritti, in grado di assicurare una governance antropocentrica e personalista dell'innovazione.

Commissione europea – Pacchetto digitale – Intermediari digitali

1. Introduzione: verso il 2030 con il *Digital Compass*

Il 9 marzo 2021 la Commissione europea ha presentato la comunicazione intitolata *2030 Digital Compass: the European way for the Digital Decade*[1], in cui ha delineato una prospettiva di trasformazione digitale dell'UE entro il 2030. La strategia delineata nella comunicazione si basa su quattro obiettivi-chiave da raggiungere nel prossimo decennio: 1) cittadini con adeguate competenze digitali e professionisti ICT altamente qualificati; 2) infrastrutture digitali sicure, efficienti e sostenibili; 3) trasformazione digitale delle imprese; 4) digitalizzazione dei servizi pubblici (e identità digitale universale per l'accesso a tutti i servizi pubblici). Il *Digital Compass* dovrebbe concretizzarsi in un programma di policy che il Parlamento europeo e il Consiglio dovrebbero adottare in codecisione, consistente in una serie di obiettivi concreti da raggiungere entro il 2030 e in un sistema di monitoraggio del loro progressivo raggiungimento, per il quale occorrerebbe sviluppare e implementare una serie di progetti *multi-countries*. I progressi ottenuti verrebbero via via registrati in un rapporto che la Commissione europea pubblicherebbe annualmente.

M.R. Allegri è professoressa associata di Diritto pubblico, dell'informazione e della comunicazione presso il Dipartimento di Comunicazione e ricerca sociale di Sapienza - Università di Roma. Questo saggio fa parte della Sezione monografica *La dimensione sociale dell'Unione europea nell'era della digitalizzazione* a cura di Maria Romana Allegri e Paola Marsocci.

La comunicazione sul *Digital Compass* rappresenta l'ultimo atto della "strategia digitale" che la Commissione presieduta da Ursula von der Leyen ha varato fin dal momento del suo insediamento. Infatti, fra le sei priorità che la Commissione europea si è data per il periodo 2019-24, la trasformazione digitale dell'Europa figura al secondo posto. Per realizzare tale obiettivo, la Commissione europea si è mossa – come si vedrà più avanti – principalmente lungo tre direttrici: 1) il *data sharing* per lo sviluppo di sistemi di intelligenza artificiale; 2) un maggiore controllo sui *gatekeeper* (cioè sulle piattaforme digitali in grado di condizionare l'accesso al mercato) onde evitare che essi possano abusare della loro posizione dominate; 3) una maggiore responsabilizzazione degli intermediari digitali per i contenuti prodotti e diffusi dagli utenti finali dei loro servizi.

Nella visione della Commissione europea, la "bussola digitale" che dovrà orientare il cammino dell'Unione europea verso il 2030 non potrà prescindere dal rispetto dei diritti fondamentali su cui l'UE si fonda, fra cui in particolare la libertà di espressione, la libertà di iniziativa economica, la tutela dei dati personali, il diritto all'oblio e la protezione dei diritti di proprietà intellettuale. A tal fine, la Commissione ha proposto al Parlamento e al Consiglio di approvare una dichiarazione interistituzionale, a complemento del "Pilastro europeo dei diritti sociali"[2], che contenga un insieme di principi finalizzati ad informare gli utenti e guidare i responsabili politici e gli operatori digitali. Questi principi riguardano: l'accesso universale ai servizi Internet; la realizzazione di un ambiente online sicuro e affidabile; la promozione dell'alfabetizzazione digitale e di competenze digitali universali tali da consentire alle persone di prendere parte attiva nella società e nel mondo; l'attenzione al rispetto dei processi decisionali democratici; l'accesso a sistemi e dispositivi digitali rispettosi dell'ambiente; lo sviluppo di servizi pubblici e amministrazioni digitali accessibili; la definizione di principi etici alla base del funzionamento degli algoritmi; la protezione e la responsabilizzazione dei bambini nello spazio online; l'accesso ai servizi sanitari digitali. Per definire con maggiore precisione il contenuto di questa "Dichiarazione di principi digitali", la Commissione europea ha aperto una consultazione pubblica che si concluderà a settembre 2021[3].

Nelle pagine che seguono verranno messi in luce alcuni fra gli aspetti più significativi e innovativi di questo percorso, le cui tappe principali sono costituite dalla *Strategia europea dei dati* (febbraio 2020)[4] e dalla conseguente proposta di regolamento sulla governance europea dei dati[5], cui si aggiungono la comunicazione della Commissione europea *Plasmare il futuro digitale dell'Europa*[6] e le successive proposte di regolamenti sui mercati equi e contendibili nel settore digitale[7] e sul mercato unico dei servizi digitali[8] (dicembre 2020). Non è un caso che il "pacchetto digitale" presentato dalla Commissione europea alla fine del 2020 includa proposte inerenti tanto al trattamento dei dati quanto alla responsabilità degli intermediari digitali. I due aspetti sono infatti intimamente connessi, posto che la progressiva trasformazione del ruolo dei provider nel corso dell'ultimo ventennio li ha resi protagonisti attivi, e non solo intermediari neutrali, sia sul fronte dell'organizzazione e gestione dei contenuti *user-generated* sia su quello del trattamento dei dati dei propri utenti, naturalmente a fini di profitto[9].

2. Il trattamento dei dati come opportunità di sviluppo del mercato interno

La *Strategia europea dei dati*[10] varata a febbraio 2020 rappresenta un deciso cambio di paradigma rispetto all'impostazione seguita negli anni precedenti, culminata nell'entrata in vigore, a maggio 2018, del regolamento generale sulla protezione dei dati personali n. 2016/679 (comunemente noto con la sigla GDPR)[11]. L'obiettivo di quel regolamento era infatti principalmente quello di proteggere i diritti e le libertà delle persone fisiche con riguardo al trattamento dei dati personali, predisponendo un quadro normativo uniforme per tutti gli Stati membri dell'Unione che permettesse la circolazione dei dati personali nel mercato interno, assistito però da un solido sistema di garanzie a tutela dei diritti individuali, incentrato sul duplice principio della trasparenza delle modalità e condizioni del trattamento e del necessario consenso informato degli interessati. Il concetto fondamentale su cui si incardinava l'impianto normativo del GDPR era quello del rischio intrinsecamente connesso ai trattamenti dei dati[12]. Per questo, il regolamento ha introdotto una serie di cautele, in base al principio di precauzione: per particolari categorie di dati personali considerati "sensibili" e per i soggetti particolarmente vulnerabili (ad esempio i minori) è stata predisposta una protezione rafforzata; per ridurre i rischi derivanti dal trattamento sono state incoraggiate misure precauzionali quali la pseudonimizzazione dei dati, la minimizzazione dei trattamenti e il principio di protezione dei dati fin dal momento della progettazione del trattamento e della definizione delle norme tecniche (*privacy by design e by default*); i titolari dei trattamenti di dati sono stati obbligati alla valutazione preventiva dei rischi derivanti da tali attività e all'applicazione di misure volte alla loro preven-

zione o attenuazione; è stata prevista una specifica procedura in caso di *data breach*, così come cautele nel caso di trasferimenti di dati verso paesi extra-UE.

Con la nuova *Strategia europea dei dati*, invece, l'accento si è spostato dal concetto di rischio al concetto di opportunità. Infatti, pur prendendo atto che «in una società in cui è in costante aumento la quantità di dati generati dai singoli cittadini, la metodologia di raccolta e utilizzo di tali dati deve porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europei», la Commissione europea non manca di sottolineare che «il volume crescente di dati industriali non personali e di dati pubblici in Europa, unito ai cambiamenti tecnologici riguardanti le modalità di conservazione ed elaborazione dei dati, costituirà una potenziale fonte di crescita e innovazione che è opportuno sfruttare». Quindi, è particolarmente importante cogliere l'opportunità offerta dai dati per il progresso sociale ed economico, affinché le imprese private e i decisori pubblici possano compiere scelte migliori, ma è altresì necessario mantenere la convinzione che l'essere umano sia e debba rimanere sempre l'elemento centrale del framework normativo.

In questo contesto si inserisce il *Libro bianco sull'intelligenza artificiale*[13] che, muovendo dalla strategia per l'IA già varata nel 2018[14], afferma che la crescita economica sostenibile attuale e futura e il benessere sociale dell'Europa si basano sempre di più sul valore creato dai dati e che, però, l'uso dell'IA può pregiudicare i valori su cui si fonda l'Unione e causare violazioni dei diritti fondamentali. Per questo, la Commissione europea intende impegnarsi per la realizzazione di un ecosistema di fiducia, migliorando il quadro normativo applicabile ai prodotti e ai servizi basati sull'IA, riducendo i rischi connessi alla loro utilizzazione e adottando una definizione di IA abbastanza flessibile da accogliere il progresso tecnologico, ma anche sufficientemente precisa da garantire la necessaria certezza del diritto.

Più recentemente la strategia digitale della Commissione europea si è arricchita[15] anche di una proposta di regolamento relativo alla governance europea dei dati (*Data Governance Act* o più sinteticamente DGA)[16], volto a introdurre uno specifico regime che regoli tutte le attività inerenti al *data sharing*, con specifico riferimento al riutilizzo dei dati in possesso delle pubbliche amministrazioni e alla libera condivisione dei dati fra soggetti pubblici e privati, grazie ai servizi offerti dai *data sharing provider*. Alla base di questa proposta vi è la convinzione che l'economia *data-driven* produrrà enormi benefici per i cittadini e che occorra quindi impegnarsi per la realizzazione di uno "spazio comune europeo di dati", in cui i dati possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione. A tal fine, occorre migliorare le condizioni per la condivisione dei dati nel mercato interno, creando un quadro armonizzato per gli scambi di dati attraverso lo strumento legislativo vincolante del regolamento, affrontando gli ostacoli al buon funzionamento di un'economia basata sui dati e predisponendo un quadro di governance a livello dell'Unione per l'accesso ai dati e il loro utilizzo, in particolare per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dal settore pubblico, la fornitura di servizi di condivisione dei dati da parte dei fornitori agli utenti commerciali e agli interessati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche. Il riutilizzo sicuro dei dati personali e dei dati commerciali riservati, a fini statistici, di ricerca e di innovazione, dovrebbe essere garantito dall'applicazione di tecniche – quali l'anonimizzazione, la pseudonimizzazione, la privacy differenziale, la generalizzazione o la soppressione e la casualizzazione – che consentono l'analisi dei dati nel rispetto della privacy individuale. Le imprese e gli interessati, infatti, dovranno poter confidare nel fatto che il riutilizzo di determinate categorie di dati protetti[17], detenuti dal settore pubblico, sarà effettuato in maniera tale da rispettare i loro diritti e interessi. Alcune disposizioni del DGA si riferiscono gli intermediari digitali che forniscono servizi di condivisione di dati: è necessario, infatti, che tali soggetti mantengano una posizione neutrale riguardo ai dati scambiati tra titolari e utenti dei dati, agendo solo in qualità di intermediari nelle transazioni e non utilizzando per altri fini i dati scambiati. È anche prevista l'istituzione di un Comitato europeo per l'innovazione in materia di dati, organo indipendente con funzioni, tra le altre, di garanzia di coerenza ed uniformità nell'applicazione del regolamento, di supporto e assistenza alla Commissione europea, di facilitazione della standardizzazione della governance europea dei dati, di promozione della cooperazione tra le autorità competenti.

Un aspetto particolarmente innovativo della proposta di regolamento sulla governance dei dati è l'introduzione del concetto di "altruismo dei dati", ovvero la possibilità di utilizzare i dati messi a disposizione su base volontaria dalle stesse persone cui i dati si riferiscono, oppure non personali messi a disposizione da persone giuridiche, per finalità di interesse generale, quali ad esempio l'assistenza sanitaria, la lotta ai cambiamenti climatici, la mobilità, l'elaborazione di statistiche ufficiali, l'erogazione di servizi pubblici, la ricerca scientifica e lo sviluppo tecnologico. Attraverso questo sistema, ci si aspetta di poter creare grandi banche di dati, la cui analisi

potrà favorire anche lo sviluppo di sistemi di intelligenza artificiale e di apprendimento automatizzato. È importante, però, che chi cede i propri dati per queste finalità cosiddette "altruistiche" – anche eventualmente sulla base di un consenso espresso in via generale, perché non sempre è possibile determinare con esattezza le finalità ultime del trattamento al momento della cessione del dato – debba avere fiducia nel fatto che i dati messi a disposizione servano effettivamente scopi di interesse generale e non vengano utilizzati per finalità di lucro. Si propone, quindi, la creazione di appositi enti non profit, stabiliti nell'Unione europea, cui le persone fisiche e giuridiche cui i dati si riferiscono potranno cedere i propri dati per le suindicate finalità; tali enti, iscrivendosi in un apposito registro tenuto dalla Commissione europea, otterranno la qualifica di "organizzazioni per l'altruismo dei dati", tenute alla trasparenza sulle finalità e modalità dei trattamenti e sottoposte alla vigilanza delle competenti autorità nazionali.

La cessione altruistica dei propri dati si fonda sull'assunto che i dati siano beni di rilevanza economica che appartengono alla persona cui si riferiscono e di cui il *data subject* può liberamente disporre nel rapporto contrattuale con il gestore della piattaforma, cedendoli a titolo di controprestazione per l'erogazione di un servizio. Tuttavia, ciò che rileva principalmente in questo caso non è tanto la concezione proprietaria del dato, quanto il controllo che il *data subject* deve poter mantenere sulla circolazione dei propri dati[18]. Infatti, al di là delle esigenze di tutela dei diritti della personalità e della libertà del consenso prestato al momento della cessione dei dati[19], è innegabile che lo sviluppo di un mercato digitale dei dati possa servire a tutelare anche esigenze collettive nel campo, ad esempio, della sanità, della sicurezza, della ricerca storica o scientifica, della protezione ambientale. Del resto, già da alcuni anni il quarto considerando del regolamento UE n. 2016/679 ci ricorda come il trattamento dei dati personali debba essere al servizio dell'uomo ed il diritto alla protezione delle informazioni di carattere personale vada considerato alla luce della sua funzione sociale, anziché come una prerogativa assoluta, e vada contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

3. Il controllo sui *gatekeeper* come affermazione di sovranità digitale

Il secondo aspetto su cui si è focalizzata l'attenzione della Commissione europea nella sua strategia digitale è quello di una nuova e più efficace regolamentazione del mercato interno dei servizi digitali, in modo da aumentare e armonizzare le responsabilità delle piattaforme online e dei prestatori di servizi di informazione, rafforzando allo stesso tempo la sorveglianza sui contenuti diffusi attraverso i servizi digitali di intermediazione. Quindi, nella comunicazione *Plasmare il futuro digitale dell'Europa*[20] la Commissione ha espresso l'esigenza che le tecnologie digitali contribuiscano al progresso dell'Europa migliorando la vita delle persone e la competitività delle imprese europee, ma che nello stesso tempo siano orientate al rispetto dei valori su cui l'UE si fonda. Per questo, la Commissione ritiene che occorra prevedere nuove regole finalizzate a contrastare comportamenti e contenuti illeciti online, a definire con maggior chiarezza le responsabilità di coloro che fungono da controllori dei flussi di informazioni e di dati, e ad accrescere la trasparenza sul modo in cui le informazioni vengono condivise e gestite su Internet.

In questo contesto si iscrivono le proposte facenti parte del cosiddetto "pacchetto digitale" che la Commissione europea ha presentato il 15 dicembre 2020: il *Digital Markets Act*[21] e il *Digital Services Act*[22]. Si tratta al momento di due proposte fra loro complementari, il cui iter di approvazione è ancora lungo e che, se e quando verranno approvate dal Parlamento europeo e dal Consiglio, potranno risultare anche significativamente modificate rispetto alla versione originaria. In ogni caso, la scelta dello strumento normativo del regolamento in luogo della direttiva (in base all'art. 114 TFUE, che prevede l'adozione di misure per garantire il funzionamento del mercato interno) è segno della volontà di pervenire all'uniformazione delle condizioni alle quali gli operatori digitali dovranno soggiacere per poter prestare i propri servizi nel mercato interno dell'UE, rendendo così più agevole la loro operatività transfrontaliera, ma anche il controllo sulle loro attività.

Il *Digital Markets Act* (o più sinteticamente DMA) costituisce in qualche modo l'inevitabile completamento di un percorso già iniziato con il regolamento (UE) 2019/1150, volto a promuovere maggiore equità e trasparenza nelle condizioni contrattuali praticate dalle piattaforme digitali (compresi i motori di ricerca) nei confronti degli utenti commerciali, cioè di quei soggetti imprenditoriali che si servono di servizi digitali di intermediazione per promuovere l'offerta al pubblico dei propri prodotti, affinché la crescente dipendenza delle imprese dagli intermediari digitali non si traduca indirettamente in condizioni più svantaggiose per gli utenti finali, cioè i consumatori[23]. Già nel regolamento del 2019, infatti, si esprimeva l'esigenza di assoggettare a una qualche forma di regolamentazione l'assoluta discrezionalità con cui gli intermediari digitali interagivano con gli

utenti commerciali, limitando la loro libertà di impresa e producendo distorsioni nel sistema di libera concorrenza del mercato interno. A integrazione del suddetto quadro normativo, la proposta in esame muove dalla constatazione che le grandi piattaforme digitali, svolgendo un ruolo di intermediazione per la maggior parte delle transazioni tra utenti finali e utenti commerciali, controllano l'accesso ai mercati digitali in cui operano e, grazie alla loro posizione di predominio sul mercato e alla possibilità di tracciare e profilare in modo completo gli utenti finali, possono attuare pratiche sleali nei confronti degli utenti o di altri operatori digitali. Proprio per reagire alla scarsa contendibilità dei mercati digitali e alle pratiche concorrenziali sleali in tale settore, la proposta di regolamento individua alcuni servizi digitali "di base", che sono controllati da un numero limitato di grandi piattaforme digitali – fra cui i servizi di intermediazione, i *social network*, i motori di ricerca, i servizi per la condivisione di video, i servizi di messaggistica, i sistemi operativi, i servizi *cloud*, i sistemi di pubblicità – e stabilisce una serie di indicatori e parametri piuttosto precisi in base ai quali il prestatore di tali servizi può essere considerato un *gatekeeper*, cioè un controllore dell'accesso al mercato. I *gatekeeper*, proprio in ragione della loro influenza sul mercato, dovranno astenersi dal mettere in pratica tutti quei comportamenti – nei confronti di utenti commerciali, di inserzionisti pubblicitari, di editori e di fornitori di servizi ausiliari – che possono essere considerati sleali rispetto al principio di libera concorrenza o che comunque limitano l'apertura e la contendibilità dei mercati digitali. Alla Commissione europea spetterebbe il compito di monitorare l'osservanza degli obblighi gravanti sui *gatekeeper*, di disporne a talune condizioni la sospensione temporanea, di aggiornarli periodicamente anche in base all'esito di apposite verifiche di mercato, di adottare decisioni nei casi di inosservanza, che possono comportare per il *gatekeeper* anche l'applicazione di una sanzione pecuniaria eventualmente assistita da penalità di mora. In tal modo, il ruolo della Commissione europea nel controllo della concorrenzialità nel settore dei servizi digitali di base diverrebbe estremamente rilevante.

Tralasciando in questa sede l'analisi dettagliata delle norme contenute nella proposta di regolamento[24], sembra opportuno considerare il *Digital Markets Act* – così come anche il suo "gemello diverso", il *Digital Services Act* – come elemento sintomatico di un conflitto sull'esercizio della sovranità nello spazio di Internet fra grandi piattaforme digitali, Stati nazionali e Unione europea[25].

La sovranità, intesa come potestà suprema di determinare le regole vigenti in un determinato territorio anche attraverso l'esercizio di poteri coercitivi e, allo stesso tempo, come rivendicazione di piena indipendenza e autonomia rispetto a centri di potere esterni, nasce come un attributo proprio dello Stato, intrinsecamente legato alla sua dimensione territoriale. Tuttavia, la natura a-territoriale di Internet rende inefficace l'esercizio del potere statale, privando l'ordinamento giuridico nazionale del suo tradizionale ambito di applicazione, quello cioè di un territorio delimitato da confini. Nello spazio sconfinato di Internet, la sovranità statale risulta indebolita e lo Stato perde il suo potere coercitivo e di controllo rispetto ai comportamenti degli altri soggetti che operano nel medesimo spazio, risultando sempre più incapace di controllare i grandi attori globali. Si affermano allora nuovi centri di potere privati, fra cui quelli delle grandi piattaforme digitali che, nella prassi, non solo si sottraggono alla potestà statale, ma per certi versi si pongono sullo stesso piano dello Stato stesso in termini di esercizio della sovranità. Esse hanno infatti progressivamente acquisito *de facto* il potere, difficilmente limitabile, di dettare le regole applicabili nell'ambiente di Internet, tanto da determinare la governance del sistema e in qualche modo anche la sua stessa architettura[26]. Non è quindi errato affermare che oggi la sovranità si sta trasformando in una questione essenzialmente tecnica, dal momento che il ricorso all'architettura (intesa come infrastruttura progettuale tecnologica) al fine di regolare le condotte dei destinatari delle norme implica la disarticolazione dei principi stessi su cui si fondano gli ordinamenti giuridici costituzionali contemporanei, in particolare quello della formazione della norma giuridica attraverso procedimenti democratici[27].

Ma c'è di più. Il principio della sovranità popolare, sui cui si fonda lo Stato costituzionale democratico-pluralista, è sottoposto alle tensioni derivanti dalle trasformazioni delle tecnologie algoritmiche, che permettono alle piattaforme digitali di influenzare le scelte (anche politiche) dei propri utenti e di coartarne in qualche modo la volontà. Infine, stiamo assistendo a un passaggio ulteriore, quello cioè che vede le piattaforme digitali non più solo rivendicare la propria autonomia e indipendenza dal potere statale in nome di sovrastanti logiche di mercato, ma pretendere addirittura di porsi a presidio del sistema di valori alla base degli ordinamenti liberal-democratici[28], nel momento in cui esse si arrogano il potere di determinare unilateralmente, in base a regole autoprodotte, quali tipi di comportamenti, informazioni e contenuti possono essere espressi attraverso i servizi da esse offerti e quali invece debbano essere inibiti o censurati.

Ciò è avvenuto perché i governi nazionali, non potendo intervenire direttamente sui mezzi di comunicazione per via del divieto di censura previsto a livello costituzionale, ricercano più o meno indirettamente la cooperazione degli intermediari digitali affinché siano questi ultimi a praticare forme di censura preventiva (privatizzata) attraverso il filtraggio dei contenuti o altre metodologie di controllo consentite oggi dall'evoluzione tecnologica[29]. Ne è derivata, nel tempo, una sostanziale discrezionalità, elasticità e spesso arbitrarietà nell'applicazione delle policy di *content moderation* da parte dei gestori delle piattaforme digitali, favorite dal fatto che gli intermediari digitali, che sono in grado di condizionare la diffusione di contenuti di terzi, potrebbero tendere verso un atteggiamento di cautela precauzionale, onde evitare conseguenze per loro sfavorevoli. Infatti, la cosiddetta "privatizzazione sostanziale della censura"[30], in assenza di controlli pubblici e di garanzie che essa avvenga nel rispetto del bilanciamento dei diritti e degli interessi sottostanti, può comportare il rischio di rimozione integrale dei contenuti contestati, con grave pregiudizio per la democrazia ed il discorso pubblico.

In questo contesto si inserisce l'Unione europea, che con il *Digital Markets Act* ha compiuto una decisa scelta di campo: quella cioè di affermarsi come centro di potere sovrano nel mercato interno dei servizi digitali, dettando regole cogenti che riducono gli spazi di autonomia dei *gatekeeper* di Internet, imponendosi non solo sulle pretese autoregolative delle piattaforme digitali, ma anche sulla potestà legislativa degli Stati nazionali. La proposta di regolamento, infatti, non lascia agli Stati membri alcun margine di manovra – anzi dichiara esplicitamente la volontà di impedire agli Stati membri di applicare normative nazionali specifiche al fine di evitare la frammentazione del mercato interno (considerando n. 9) –, vieta alle autorità nazionali di adottare qualsiasi decisione in contrasto con quelle assunte dalla Commissione europea ai sensi del regolamento (art. 1, par. 7) ed esclude le autorità nazionali persino da qualsiasi forma di controllo sull'applicazione del regolamento stesso, demandando tale compito integralmente alla Commissione europea.

Un simile atteggiamento si riscontra anche nella proposta di *Digital Services Act*, di cui si parlerà nel paragrafo successivo, ma solo relativamente alle piattaforme di dimensioni molto grandi. Queste ultime, infatti, per via della loro dimensione multinazionale sfuggono inevitabilmente al controllo e alla giurisdizione dei singoli Stati membri; per questo motivo, a differenza delle piattaforme digitali di "dimensioni normali" – che sono sottoposte alla vigilanza dei Coordinatori dei servizi digitali degli Stati membri (art. 41) e che possono subire sanzioni stabilite da autorità nazionali (art. 42) – quelle molto grandi, secondo la proposta di DSA, sono soggette a un sistema di vigilanza rafforzata ed eventuale sanzione di cui è responsabile unicamente la Commissione europea (artt. 50-66).

Così, attraverso la riaffermazione della propria "sovranità digitale" – intesa in questo caso come potestà di regolamentazione e controllo delle *tech companies* – l'Unione europea sembra voler rivendicare un sistema di tutele che la connota come spazio di libertà e di diritti, capace di assicurare un governo antropocentrico e personalista dell'innovazione[31]. Le minacce derivanti dall'impiego di sofisticate tecnologie informatiche richiedono l'intervento dei poteri pubblici al fine di assicurare un'effettiva e concreta tutela dei diritti fondamentali delle persone; di qui la rivendicazione da parte di un organismo sopranazionale come l'UE del potere di disciplinare l'innovazione digitale e difendere tali diritti. Di fronte, dunque, al sempre più pervasivo utilizzo della tecnologia nella vita privata e pubblica, l'Unione europea intende riaffermare la propria sovranità digitale all'interno dei propri confini territoriali e con riguardo ai propri cittadini, nei confronti non solo dei grandi players digitali ma anche dei suoi Stati membri.

La medesima tendenza, del resto, era stata avviata fin dal 2016 con l'approvazione del regolamento generale sulla protezione dei dati personali (GDPR), cui si è già accennato in precedenza: la portata innovativa di quel regolamento, in vigore da maggio 2018, consiste appunto nel fatto che per la prima volta l'elemento che ne determina l'applicabilità è collegato al luogo in cui è situato l'interessato, imponendo così alle imprese multinazionali del web di adeguarsi alla normativa europea – e non a quella del paese in cui hanno la sede – ogniqualvolta trattano dati di cittadini dell'Unione o offrono servizi fruibili nel territorio dell'Unione. Dunque, anche mediante il GDPR l'Unione europea ha inteso perseguire l'obiettivo di uniformare la regolamentazione dei flussi di informazioni attraversano l'Europa, sottraendo il mondo digitale al dominio dei colossi stranieri, soprattutto nord-americani, ma anche alla variabilità delle legislazioni nazionali. In questo modo, l'UE ha tentato di rispondere in modo efficace alla necessità di stabilire confini anche nell'ambiente liquido di Internet, delimitando lo spazio di esercizio dei propri poteri sovrani e offrendo ai suoi cittadini una maggiore tutela in termini di sicurezza informatica[32].

4. Verso il superamento della presunzione di neutralità del provider e del "dogma" dell'inapplicabilità di obblighi di sorveglianza

Sempre nel solco della tendenza espressa dall'Unione europea verso il recupero di sovranità del settore della digitalizzazione a scapito degli Stati membri – sia pure in modo meno marcato rispetto alla proposta di DMA– si inserisce la proposta di *Digital Services Act* (o più sinteticamente DSA), presentata anch'essa il 15 dicembre 2020[33]. Quest'ultima muove dalla constatazione che, a distanza di un ventennio dall'entrata in vigore della direttiva europea sul commercio elettronico[34] che regola attualmente il mercato dei servizi digitali, tale settore ha subito una profonda e rapida evoluzione e trasformazione, tanto da rendere le norme vigenti inadeguate a plasmare la realtà attuale, caratterizzata da un'enorme varietà e quantità di servizi, prodotti e fornitori. La trasposizione della direttiva *e-commerce* nelle diverse legislazioni nazionali ha prodotto una certa difformità nelle soluzioni normative adottate nei singoli Stati membri dell'UE, difformità cui appunto l'introduzione di un nuovo regolamento intenderebbe ovviare. Le divergenze riguardano non solo la qualificazione delle diverse categorie di intermediari digitali e le condizioni alle quali sia possibile attribuire loro una qualche responsabilità per i contenuti da essi veicolati, ma anche la qualificazione dei contenuti illeciti online e le possibili misure per contrastarne la diffusione.

Nel presentare la proposta di DSA, la Commissione europea ha tenuto conto delle tre risoluzioni adottate dal Parlamento europeo nella seduta del 20 ottobre 2020[35], che contengono un deciso appello a mantenere i principi essenziali della vigente direttiva sul commercio elettronico – cioè in particolare il principio dell'irresponsabilità del provider per i contenuti *user-generated* e il divieto di obblighi di sorveglianza e filtraggio preventivi – e a tutelare i diritti fondamentali nell'ambiente online e l'anonimato online, ove ciò sia tecnicamente possibile. Le risoluzioni chiedono però anche ai prestatori dei servizi digitali una maggiore trasparenza, obblighi più stringenti in materia di informazione e un quadro più chiaro e uniforme delle loro responsabilità, fra cui anche l'introduzione di obblighi effettivi per contrastare i contenuti illegali online. Il Parlamento europeo, infine, spinge per la messa a punto di un sistema di vigilanza pubblica a livello nazionale e di Unione europea e per il rafforzamento della cooperazione tra le autorità competenti delle varie giurisdizioni nell'applicazione delle norme, soprattutto per quanto riguarda le questioni transfrontaliere. Insomma, lo scopo ultimo della nuova legislazione sui servizi digitali dovrebbe essere quello di promuovere un ambiente digitale competitivo, rafforzando la fiducia dei consumatori nell'economia digitale, ma rispettando allo stesso tempo i diritti fondamentali degli utenti. Per questo occorrono norme armonizzate sulla lotta ai contenuti illegali online, sulle esenzioni dalla responsabilità per i prestatori di servizi e sulla moderazione dei contenuti, nonché sugli obblighi di comunicazione e trasparenza e sulle procedure di *notice-and-take-down*, al fine di assicurare il rispetto dei diritti fondamentali e garantire un ricorso giurisdizionale indipendente.

Tutto ciò considerato, la proposta di regolamento sui servizi digitali propone alcune modifiche e integrazioni del quadro normativo vigente, dettato dalla ormai datata direttiva sul commercio elettronico 2000/31/CE e interpretato secondo la relativa giurisprudenza della Corte europea di Giustizia, in ordine a molteplici aspetti.

In primo luogo, la proposta circoscrive il suo campo di applicazione ai "servizi intermediati" – cioè qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario, secondo la definizione fornita dalla direttiva UE 2015/1535[36] – di semplice trasporto (*mere conduit*)[37], memorizzazione temporanea (*caching*)[38] e permanente (*hosting*)[39], con l'esplicita esclusione dei servizi di media audiovisivi, che ricadono invece nella particolare disciplina dettata dalla direttiva 2010/13/UE[40], così come modificata dalla direttiva (UE) 1808/2018. Le nuove norme si applicherebbero ai prestatori di servizi intermediari indipendentemente dal loro luogo di stabilimento o di residenza, nella misura in cui prestano servizi nell'Unione, come dimostrato da un collegamento sostanziale con l'Unione[41].

In secondo luogo, la proposta mantiene l'attuale regime di irresponsabilità dell'intermediario digitale per i contenuti *user-generated*, a condizione che il provider non dia origine alla trasmissione, non ne selezioni il destinatario e non selezioni né modifichi le informazioni trasmesse[42]. In sintesi, con la proposta in esame la posizione di neutralità del provider non sarebbe più implicitamente presunta in via generale, ma qualificata di volta in volta in base a precisi requisiti, che diventano più stringenti via via che aumenta la complessità del servizio offerto[43]. Ai prestatori di servizi di memorizzazione temporanea (*caching*), infatti, viene anche richiesto, al fine di mantenere l'esenzione dalla responsabilità, di conformarsi alle condizioni di accesso alle informazioni e alle norme sull'aggiornamento delle informazioni comunemente adottate dalle imprese del settore, nonché di astenersi dall'interferire con l'uso lecito della tecnologia uti-

lizzata per ottenere dati sull'impiego delle informazioni e soprattutto di agire prontamente per rimuovere le informazioni memorizzate o disabilitare l'accesso alle stesse non acquisita l'effettiva conoscenza del fatto che le informazioni all'origine della trasmissione siano state rimosse dalla rete o che l'accesso alle informazioni sia stato disabilitato (art. 4). Ai prestatori di servizi di *hosting*, infine, vengono richiesti ulteriori requisiti come precondizione per l'esenzione da responsabilità (art. 5): non essere effettivamente a conoscenza delle attività o dei contenuti illeciti e, per quanto attiene a domande risarcitorie, non essere consapevole di fatti o circostanze che rendono manifesta l'illiceità dell'attività o dei contenuti; inoltre, agire immediatamente per rimuovere i contenuti illeciti o per disabilitare l'accesso agli stessi, non appena acquisita la conoscenza di tali attività o contenuti illeciti o la consapevolezza di tali fatti o circostanze.

Quest'ultima precisazione è particolarmente significativa, perché fuga ogni dubbio sul fatto che il fornitore di servizi di *hosting* abbia l'obbligo di attivarsi con prontezza per contrastare la diffusione di contenuti illeciti, indipendentemente dalla modalità tramite le quali abbia acquisito conoscenza o consapevolezza della loro illiceità. Da questo punto di vista, la proposta di regolamento supera decisamente l'impostazione ambigua della direttiva 2000/31/CE attualmente vigente (art. 14) che, da un lato, chiede all'*hosting provider* di attivarsi prontamente per rimuovere i contenuti illeciti non appena acquisita la conoscenza o consapevolezza della loro illiceità ma, dall'altro, permette ai singoli Stati membri di definire autonomamente le condizioni alle quali detta conoscenza o consapevolezza possa ritenersi effettivamente acquista, generando così divergenze interpretative e applicative a livello comunitario e nazionale, che rendono dirimente il contributo interpretativo della giurisprudenza[44]. Secondo il framework normativo ad oggi vigente, infatti, poiché il presupposto per il riconoscimento dell'irresponsabilità dell'*hosting provider* è proprio il suo atteggiamento neutrale rispetto ai contenuti veicolati, un "eccesso di zelo" nella disabilitazione o rimozione di contenuti a seguito di richieste da parte degli utenti, soprattutto se non suffragate da un ordine di un'autorità amministrativa o giudiziaria, porterebbe alla paradossale conclusione di far venire meno la presunzione di neutralità del provider e, conseguentemente, la sua irresponsabilità. Al contrario, la proposta di regolamento imporrebbe al provider di adottare un comportamento proattivo di contrasto ai contenuti illeciti proprio per poter continuare a godere del regime di *safe harbour*.

L'art. 7 della proposta di regolamento è molto chiaro sul fatto che ai prestatori di servizi intermediari non sono imposti obblighi generali di sorveglianza sulle informazioni trasmesse o memorizzate, né di accertamento attivo di fatti o circostanze che indichino la presenza di attività illegali[45]. Il ché non significa, però, che essi debbano temere di perdere l'esenzione di responsabilità qualora svolgano indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso ad essi (art. 6). Dunque, il superamento della posizione di neutralità, anche per iniziativa spontanea del provider stesso, è esplicitamente incoraggiato. Del resto, la proposta di DSA sembra allinearsi all'opinione, oggi generalmente condivisa, secondo cui il ricorso a filtri di ricerca automatizzati, soprattutto per le piattaforme di grandi dimensioni, sia in concreto l'unico strumento praticabile per garantire, da una parte, una tutela effettiva della vita privata e dei diritti della personalità degli utenti e, dall'altra parte, per non imporre oneri economici straordinari a carico del gestore del servizio, a patto di assicurare un adeguato livello di trasparenza dei parametri di funzionamento degli algoritmi di filtraggio.

Per facilitare l'acquisizione di conoscenza dei contenuti illeciti da parte degli *hosting provider*[46], l'art. 14 della proposta di regolamento introdurrebbe, sulla falsariga del modello rappresentato dal DMCA statunitense[47], l'obbligo per questa particolare categoria di intermediari digitali di approntare procedure di *notice-and-take-down* di facile accesso e uso per gli utenti, che consentano a questi ultimi di segnalare la presenza di contenuti illeciti nella piattaforma[48]. In questo modo, si ovvierebbe all'attuale incertezza, derivante dal fatto che né la direttiva 2000/31/CE né la normativa nazionale di recepimento precisano le modalità attraverso le quali il provider possa acquisire effettiva conoscenza dell'illecito[49]. Le notifiche però dovranno essere formulate con un certo grado di precisione: dovranno ad esempio esplicitare le ragioni per le quali si ritiene che taluni contenuti siano illegali, indicare gli indirizzi URL esatti[50] e, se necessario, ulteriori informazioni che consentano di identificare tali contenuti. Se formulate in questo modo, le notifiche permetteranno al provider di acquisire una conoscenza effettiva dell'illecito (art. 14 par. 3) e di attivarsi con *due diligence* per vagliare le notifiche e adottare le conseguenti decisioni[51]. L'attivazione del provider in conseguenza della notifica, gli permetterebbe di continuare a beneficiare del regime di esenzione dalla responsabilità, che invece perderebbe in caso di inerzia. Dopo aver vagliato la notifica il provider, se convinto dell'illiceità dei contenuti segnalati, potrà rimuovere tali informazioni o inibire l'accesso ad esse. È importante, però, che tale decisione sia

debitamente e dettagliatamente motivata, in modo da permettere al destinatario del servizio interessato di esercitare in modo effettivo i possibili mezzi di ricorso, scegliendo fra i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria (art. 15).

Naturalmente, l'azione di contrasto ai contenuti illeciti da parte degli *hosting provider* non verrà avviata solo a seguito di notifica da parte degli utenti, ma anche in conseguenza di un ordine proveniente da un'autorità amministrativa o giudiziaria degli Stati membri, emanato in base alla normativa nazionale (art. 8). Appena ricevuto tale ordine, i prestatori dei servizi saranno tenuti ad informare l'autorità nazionale che lo ha emesso delle misure adottate per ottemperarvi. L'ordine, però, dovrà essere formulato in modo chiaro e specifico e dovrà, fra l'altro, contenere la motivazione su cui si fonda l'illegalità dei contenuti contestati e soprattutto gli URL esatti[52] in cui tali contenuti sono localizzati, nonché eventuali informazioni supplementari che ne consentano l'identificazione.

Una questione che la proposta di regolamento non pare aver definito è quella dell'esatta nozione di "contenuto illecito". Tuttavia, il considerando n. 12 ne dà un'interpretazione assai ampia: «tale concetto dovrebbe in particolare intendersi riferito alle informazioni, indipendentemente dalla loro forma, che ai sensi del diritto applicabile sono di per sé illegali, quali l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che riguardano attività illegali, quali la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il *cyberstalking*, la vendita di prodotti non conformi o contraffatti, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore o le attività che comportano violazioni della normativa sulla tutela dei consumatori. A tale riguardo è irrilevante che l'illegalità delle informazioni o delle attività sia sancita dal diritto dell'Unione o dal diritto nazionale conforme al diritto dell'Unione e quale sia la natura esatta o l'oggetto preciso della legge in questione». Conseguentemente, l'art. 2 lett. g della proposta di regolamento qualifica come contenuto illegale «qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni».

Ciò significa che l'*hosting provider*, nella valutazione che dovrà compiere circa l'opportunità di rendere inaccessibili taluni contenuti, dovrà tener conto di un corpus normativo assai vasto di livello tanto europeo quanto nazionale, cosa che può rivelarsi piuttosto complicata, se si considera, da un lato, la natura transfrontaliera dell'attività di gran parte degli intermediari digitali e, dall'altro, la variabilità con cui le legislazioni nazionali tipizzano le varie categorie di illeciti. Il provider, dunque, dovrebbe conoscere la normativa in vigore nei diversi Stati membri in cui opera e adottare policy più o meno restrittive a seconda del contesto nazionale di riferimento. È evidente come questo possa complicare non poco l'attività degli intermediari digitali, oltre al fatto che una disparità di trattamento per il medesimo contenuto, giustificata in base alla diversità della legislazione nazionale applicabile, potrebbe determinare l'insorgere di controversie fra operatori digitali, da un lato, e utenti o autorità nazionali, dall'altro. Proprio per tentare di ovviare a questi problemi, quindi, si registra una iniziale tendenza da parte dell'ordinamento giuridico dell'Unione a raggiungere un certo livello di armonizzazione normativa almeno in relazione ad alcuni tipi di contenuti illeciti che circolano online, attraverso una legislazione settoriale che impone ai provider di adottare misure di contrasto alla loro diffusione[53]. In tutti questi casi il diritto dell'UE grava i provider di maggiori obblighi di controllo rispetto alla disciplina generale e restringe l'area della loro irresponsabilità, accrescendo invece il livello di diligenza professionale che gli intermediari digitali devono dimostrare di aver seguito.

Mentre l'allestimento di efficaci procedure di *notice-and-take-down* è previsto dalla proposta di regolamento come onere in capo ai soli *hosting provider*, alcuni obblighi di comunicazione e trasparenza sono previsti per tutti i tipi di prestatori di servizi intermediari (artt. 10-12). Tutti, infatti, dovranno istituire un punto di contatto unico che consenta la comunicazione diretta, per via elettronica, con le autorità nazionali ed europee; inoltre, qualora essi prestino i propri servizi nell'Unione pur non essendo stabiliti al suo interno, dovranno designare un proprio rappresentante legale in uno Stato membro dell'Unione, che potrà essere ritenuto responsabile del mancato rispetto degli obblighi derivanti dal regolamento. Per quanto riguarda il rapporto con gli utenti, i prestatori di servizi intermediari dovranno esplicitare nelle condizioni d'uso del servizio, in modo chiaro, non ambiguo e facilmente accessibile, le modalità di trattamento delle informazioni fornite dai destinatari del servizio, con particolare riferimento alle tecniche di *content moderation*, compresi il processo decisionale algoritmico e la verifica umana[54]. Infine, almeno una volta l'anno i prestatori di servizi intermediari dovranno pubblicare relazioni

chiare, facilmente comprensibili e dettagliate sulle attività di moderazione dei contenuti svolte durante il periodo di riferimento.

5. Una questione di dimensioni: la categoria delle piattaforme digitali

Un aspetto interessante della proposta di regolamento in esame riguarda il fatto che gli obblighi gravanti sui diversi tipi di intermediari digitali sono graduati in base sia alle loro dimensioni sia alla complessità dei servizi da essi offerti. In particolare, la sezione 3 della proposta di regolamento DSA (artt. 16-24) si riferisce unicamente alla categoria delle "piattaforme digitali"[55], ad esclusione di quelle che possono essere considerate piccole imprese o microimprese[56]. Le piattaforme digitali avranno l'obbligo ulteriore di dover allestire efficaci meccanismi interni di gestione dei reclami, in modo che gli utenti possano facilmente e gratuitamente presentare per via elettronica reclami contro le decisioni di rimozione o disabilitazione di informazioni, di sospensione o disabilitazione del servizio, di sospensione o cessazione dell'account; tali reclami dovranno essere gestiti in modo tempestivo, diligente e obiettivo e le conseguenti decisioni dovranno essere comunicate ai destinatari senza ritardo. Inoltre, in ogni Stato membro dell'Unione dovranno essere istituiti appositi organismi di risoluzione extragiudiziale delle controversie fra intermediari digitali e utenti dei loro servizi, cui questi ultimi dovranno poter ricorrere se insoddisfatti dell'esito del reclamo o in alternativa al reclamo stesso.

In presenza di contenuti illeciti chiunque potrà presentare segnalazioni alle piattaforme digitali, ma queste ultime faranno in modo di prestare attenzione prioritaria alle notifiche provenienti da soggetti qualificati come "segnalatori attendibili", cioè enti accreditati dagli Stati membri che rappresentano interessi collettivi e sono indipendenti dagli intermediari digitali. Nel caso di utenti che con frequenza diffondono contenuti manifestamente illegali, le piattaforme digitali potranno reagire sospendendo nei loro confronti i propri servizi (art. 20 par. 1). Inoltre, qualora la piattaforma abbia motivo di sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato grave che comporta una minaccia per la vita o la sicurezza delle persone, essa dovrà informarne senza indugio le competenti autorità nazionali o l'Europol, fornendo tutte le informazioni in suo possesso (art. 21).

Ulteriori obblighi gravanti sulle piattaforme digitali riguarderebbero, secondo la proposta di regolamento, i rapporti con gli operatori commerciali: la piattaforma digitale che consente a questi ultimi di utilizzare i servizi da essa offerti per pubblicizzare o offrire prodotti o servizi a consumatori situati nell'Unione dovrà previamente acquisire una serie di informazioni dettagliate su di essi, che potranno essere messe a disposizione degli utenti e delle competenti autorità nazionali ed europee (art. 22).

Infine, le piattaforme digitali saranno tenute alla trasparenza del numero medio dei destinatari dei loro servizi, del numero di controversie risolte per via extragiudiziale e del loro esito, del numero di decisioni di sospensione del servizio adottate come reazione ad abusi, dell'uso di strumenti automatizzati di *content moderation*, della pubblicità online (natura del messaggio pubblicitario, identità del committente, parametri utilizzati per determinare i destinatari)[57].

Fra le piattaforme digitali la proposta di regolamento considera distintamente la particolare categoria delle "piattaforme digitali di dimensioni molto grandi", quelle cioè che raggiungono un numero di destinatari superiore a 45 milioni o comunque al 10% della popolazione dell'Unione. Solo a queste si applicano le disposizioni supplementari contenuti agli artt. 25-33. Tale trattamento differenziato si giustificherebbe in ragione dei rischi sistemici posti da tali piattaforme, proprio per via delle loro grandi dimensioni, in termini di impatto sul mercato interno, influenza sull'opinione pubblica e sui processi democratici ed elettorali, diffusione di contenuti illeciti, pregiudizio per i diritti fondamentali, protezione dei minori (considerando nn. 54-57). Per prevenire ed attenuare i rischi sistemici, alle piattaforme di grandi dimensioni è richiesta una diligenza maggiore rispetto agli altri intermediari digitali (considerando n. 58). Esse infatti, utilizzando sistemi di raccomandazione basati sulla profilazione degli utenti, possono presentare loro le informazioni in un determinato ordine di priorità o secondo sistemi di classificazione precostituiti, di cui è necessario che i destinatari dei servizi comprendano i parametri di funzionamento (considerando n. 62). Occorrerebbe, inoltre, che le grandi piattaforme garantissero la trasparenza dei messaggi pubblicitari predisponendo all'uopo appositi registri accessibili al pubblico, in modo da facilitare la vigilanza sui rischi emergenti derivanti dalla distribuzione della pubblicità online, ad esempio in relazione alla pubblicità illegale o alle tecniche di manipolazione e alla disinformazione, che possono avere ripercussioni negative sulla salute e sulla sicurezza pubblica, sul dibattito civico, sulla partecipazione politica e sull'uguaglianza dei cittadini (considerando n. 63). Infine, in particolari situazioni di crisi (ad esempio terremoti, uragani, pandemie, minacce terroristiche, guerre) bisogna tenere conto

dell'importante ruolo svolto dalle piattaforme online di dimensioni molto grandi nella diffusione delle informazioni e potenzialmente anche della disinformazione: per questo è opportuno che tali piattaforme predispongano specifici protocolli di crisi da utilizzare in simili circostanze (considerando n. 71).

Muovendo da tali premesse, la proposta di regolamento chiede alle piattaforme molto grandi di analizzare e valutare annualmente eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi nell'Unione – con particolare riferimento alla possibile diffusione dei contenuti illeciti, ad eventuali effetti negativi per l'esercizio dei diritti fondamentali e alla possibilità di manipolazioni intenzionali di tali servizi anche mediante strumenti automatizzati (*bot*, *troll*, ecc.) – e di adottare una serie di misure volte all'attenuazione di tali rischi. I principali parametri utilizzati dalle grandi piattaforme nei sistemi di raccomandazione dovranno essere chiaramente esplicitati nelle condizioni generali del servizio e agli utenti dovrà essere consentito facilmente di selezionare e modificare le opzioni prescelte per ciascun sistema di raccomandazione. Una serie di informazioni riguardanti la pubblicità online (fra cui anche i parametri utilizzati per l'individuazione dei destinatari dei messaggi pubblicitari) dovranno essere raccolte in un registro pubblico e ivi conservate e mantenute accessibili per un anno. Le grandi piattaforme dovranno, inoltre, sottoporsi annualmente a proprie spese ad audit effettuati da organismi indipendenti, nominare un "responsabile della conformità" incaricato di monitorare la conformità alle disposizioni del nuovo regolamento, consentire alle competenti autorità nazionali[58] e alla Commissione europea l'accesso ai dati necessari per monitorare e valutare la conformità al regolamento, adempiere ad obblighi di comunicazione trasparente di una serie di relazioni sulla valutazione dei rischi, sulle misure adottate in tal senso, sugli esiti delle procedure di audit, ecc. Secondo gli artt. 50 e ss., le piattaforme digitali di dimensioni molto grandi saranno soggette a una complessa procedura di vigilanza rafforzata in più fasi sulla conformità alle disposizioni del nuovo regolamento, che coinvolgerà il Coordinatore dei servizi digitali del luogo di stabilimento[59], il Comitato europeo per servizi digitali[60] e soprattutto la Commissione europea; la procedura potrebbe concludersi con sanzioni pecuniarie assistite da penalità di mora.

Come si è già evidenziato, proprio le dimensioni molto grandi di talune piattaforme digitali, operanti ovviamente su scala multinazionale, sono alla base della scelta di affidare interamente alla Commissione europea la responsabilità del sistema di vigilanza rafforzata che la proposta di DSA prevede agli artt. 50-66 e che potrebbe concludersi anche con l'applicazione di sanzioni. Così come nel "gemello" DMA, anche in questo caso il ruolo della Commissione europea è assolutamente centrale e sovrasta completamente quello delle autorità nazionali, dimostrando la volontà della Commissione europea di rafforzare la propria "sovranità digitale". Invece, per le piattaforme digitali più piccole viene mantenuta una dimensione nazionale della vigilanza, affidata ai Coordinatori nazionali dei servizi digitali: esse rimangono infatti assoggettate al controllo e alla giurisdizione delle competenti autorità degli Stati membri, che mantengono il potere sanzionatorio su di esse (artt. 41-42). Quindi, le dimensioni delle piattaforme – qualificate non in base a parametri territoriali (il numero di Stati membri interessati da tali servizi) bensì personali (il numero di persone che ne fruiscono) – determinano la maggiore o minore rilevanza del ruolo delle autorità nazionali rispetto alla Commissione europea. In altre parole, l'elemento personalistico collegato alle piattaforme digitali determina il *quantum* di sovranità che gli Stati membri possono ancora esercitare direttamente in tale ambito, rispetto al *quantum* che viene invece esercitato a livello sovranazionale.

6. Conclusioni

Alla base del "pacchetto digitale" proposto dalla Commissione europea alla fine del 2020 vi è la decisa tendenza verso l'affermazione dell'Unione come centro di potere sovrano sull'ambiente digitale, non solo rispetto alle grandi imprese multinazionali che gestiscono il flusso di informazioni in Internet, ma anche rispetto agli Stati nazionali, i quali vanno via via perdendo la possibilità di disciplinare in modo autonomo i fenomeni che avvengono online. La natura a-territoriale di Internet rende inefficace l'esercizio del potere statale e ciò ha nel tempo favorito l'affermazione di nuovi centri di potere privati, fra cui le grandi piattaforme digitali, che dettano le regole applicabili all'ambiente di Internet, ne sorvegliano il rispetto e addirittura pretendono di determinare il sistema valoriale applicabile ai servizi da esse offerti, attraverso una sostanziale discrezionalità, elasticità e spesso arbitrarietà nell'applicazione delle policy di *content moderation*. Per reagire a questa tendenza, la ricetta proposta dalla Commissione europea prevede un notevole ridimensionamento della potestà normativa degli Stati membri sugli operatori del mercato digitale, nonché la loro esclusione da qualsiasi forma di controllo sul rispetto delle regole da parte delle web company, demandando tale compito integralmente alla Commissione europea.

L'affermazione di sovranità presuppone la definizione dei confini entro i quali tale sovranità può essere esercitata. Ed ecco, allora, che nello spazio fluido di Internet, refrattario all'imposizione di barriere territoriali, si va affermando il principio per cui l'estensione e il limite dell'effettività del diritto dell'Unione sulla "vita digitale" coincide non tanto con il suo territorio (normativa applicabile alle imprese stabilite nell'Unione o che prestano i propri servizi nell'Unione) quanto con i suoi cittadini (normativa applicabile ai servizi digitali prestati o fruiti da cittadini dell'Unione). La prevalenza dell'elemento personalistico rispetto a quello geografico nell'esercizio della sovranità digitale da parte dell'Unione europea è un aspetto che occorre assolutamente evidenziare per poter inquadrare correttamente le proposte normative in esame.

In relazione alla governance europea dei dati, l'UE ha decisamente spostato la propria attenzione dalla intrinseca rischiosità dei trattamenti dei dati personali, per i quali il GDPR ha previsto una serie di cautele, alla grande opportunità che il *data sharing* rappresenta per lo sviluppo del mercato interno. A tal fine, è necessario che gli intermediari digitali che forniscono servizi di condivisione di dati mantengano una posizione neutrale rispetto ai dati scambiati, agendo solo in qualità di intermediari nelle transazioni e non utilizzando i dati per altri fini. Ciò è particolarmente importante nel caso del trattamento dei dati cosiddetto "altruistico", cioè effettuato per finalità di pubblico interesse da parte di intermediari digitali non profit appositamente costituiti.

Occorre altresì sottolineare l'evoluzione del ruolo dei provider, che nel corso dell'ultimo ventennio si sono progressivamente trasformati in protagonisti attivi sia sul fronte dell'organizzazione e gestione dei contenuti *user-generated* sia su quello del trattamento dei dati dei propri utenti, scardinando l'assioma della loro neutralità postulato dalla direttiva europea sul commercio elettronico risalente al 2000.

La questione della neutralità riguarda anche i cosiddetti *gatekeeper*, cioè le piattaforme digitali che controllano l'accesso ai servizi digitali "di base". Ad essi si chiede non solo di astenersi dal mettere in atto pratiche anticoncorrenziali a scapito di altri operatori del mercato o degli stessi utenti, ma anche di garantire la trasparenza dei messaggi pubblicitari (natura del messaggio pubblicitario, identità del committente, parametri utilizzati per determinare i destinatari) e dei criteri utilizzati dai sistemi di *content moderation* e di raccomandazione basati sulla profilazione degli utenti, nonché di analizzare e valutare annualmente eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi nell'Unione e di sottoporsi a una complessa procedura di vigilanza rafforzata. A tutti gli *hosting provider* poi, anche a quelli di minori dimensioni, viene richiesto di approntare specifiche procedure di *notice-and-take-down* per la segnalazione dei contenuti illeciti e di attivarsi prontamente per valutare le segnalazioni ricevute, rimuovere i contenuti contestati o disabilitare l'accesso ad essi. Tali obblighi, la cui quantità e complessità varia in base alle maggiori o minori dimensioni dell'intermediario digitale di riferimento, segnano di fatto il radicale superamento del principio della neutralità del provider rispetto ai contenuti prodotti e diffusi dagli utenti: il sistema di notifica consente al provider di acquisire l'effettiva conoscenza dell'illecito e, in conseguenza della notifica, il provider è tenuto ad attivarsi per poter continuare a beneficiare del regime di esenzione dalla responsabilità, che invece perderebbe in caso di inerzia. Addirittura, i provider sono esplicitamente incoraggiati a svolgere indagini di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali: dunque, si fa strada il principio secondo cui il *content filtering* automatizzato, soprattutto per le piattaforme di grandi dimensioni, sia in concreto l'unico strumento praticabile per contrastare la loro diffusione.

Tutto ciò considerato, le proposte contenute nel "pacchetto digitale" possono essere considerate come elementi sintomatici di un conflitto sull'esercizio della sovranità nello spazio di Internet fra le grandi piattaforme digitali, gli Stati nazionali e l'Unione europea. Il sociologo Zygmunt Bauman ha definito i processi di globalizzazione come «la grande guerra di indipendenza dallo spazio», ossia «una guerra durante la quale i centri decisionali, insieme alle motivazioni stesse che determinano le decisioni, gli uni e le altre ormai liberi da legami territoriali, hanno preso a distaccarsi, in forma continua e inesorabile, dai vincoli imposti dai processi di localizzazione»[61]. Si può allora affermare che l'Unione europea sta prendendo parte a questa guerra sforzandosi di riaffermare il proprio controllo sui flussi di informazione che corrono attraverso Internet, riconfigurando il concetto di confine e individuando un *ambitus* geografico preciso in cui poter esercitare la propria sovranità.

Note

[1]Doc. COM(2021) 118 del 9 marzo 2021.

[2]Il Pilastro europeo dei diritti sociali è un insieme di 20 principi e diritti fondamentali in ambito sociale, adottati dal Parlamento europeo, dal Consiglio e dalla Commissione europea il 17 novembre 2017 a Göteborg, in Svezia.

[3]Cfr. Commissione europea, *Dichiarazione di principi digitali - la "via europea" per la società digitale*.

[4]Doc. COM(2020) 66 del 19 febbraio 2020.

[5]Doc. COM(2020) 767 del 25 novembre 2020.

[6]Doc. COM(2020) 67 del 19 febbraio 2020.

[7]Doc. COM(2020) 842 del 15 dicembre 2020.

[8]Doc. COM(2020) 825 del 15 dicembre 2020.

[9]G. De Gregorio, *The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?*, EUI Working Paper RSCAS n. 36, 2019, 21 p.

[10]Doc. COM(2020) 66 cit.

[11]Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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). Tale regolamento è comunemente noto come GDPR (*General Data Protection Regulation*).

[12]S. Calzolaio, *Protezione dei dati personali*, in "Digesto delle discipline pubblicistiche. Aggiornamento", Utet, 2017, spec. pp. 627-629; F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), "Intelligenza Artificiale, protezione dei dati personali e regolazione", Giappichelli, 2018, spec. pp. 41, 46-51 e 166-167.

[13]Doc. COM(2020) 65 del 19 febbraio 2020.

[14]Doc. COM(2018) 237 del 25 aprile 2018 intitolata *L'intelligenza artificiale per l'Europa*.

[15]A completamento del regolamento generale sulla protezione dei dati personali già in vigore da maggio 2018 (regolamento UE n. 2016/679), del regolamento 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea e della direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[16]Doc. COM(2020) 767 cit.

[17]Si pensi ai dati protetti da diritti di proprietà intellettuale o ai dati sensibili di natura non personale, quali ad esempio i segreti commerciali.

[18]F. Pizzetti, *op. cit.*, spec. pp. 16-23 e 37; G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in "Politica del diritto", 2019, n. 2, pp. 199-236.

[19]F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in "Contratto e impresa", 2019, n. 1, pp. 34-58; I. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in "Osservatorio del diritto civile e commerciale", 2018, n. 1, pp. 67-106; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in "Rivista trimestrale di diritto e procedura civile", 2018, n. 2, pp. 411-440; S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in "MediaLaws", 2019, n. 3, pp. 131-147.

[20]Doc. COM(2020) 67 cit.

[21]*Proposta di regolamento relativo ai mercati equi e contendibili nel settore digitale*, doc. COM(2020) 842 cit.

[22]Doc. COM(2020) 825 cit.

[23]Interessanti considerazioni sul regolamento (UE) 2019/1150 in F. Foltran, *Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri negoziali*, in "MediaLaws", 2019, n. 3, pp. 162-176. Si veda anche M.C. Caurasano, *Le piattaforme online e la tutela degli utenti digitali al tempo della pandemia*, in "Persona e mercato", 2020, n. 4, pp. 466-476.

[24]Per una accurata analisi dei contenuti della proposta di regolamento DMA si rimanda al *dossier n. 52*, 18 maggio 2021, realizzato dalla Camera dei deputati, Ufficio rapporti con l'Unione europea. Si veda ancora lo studio pubblicato a gennaio 2021 dal Centre on Regulation in Europe, intitolato *The European proposal for a Digital Markets Act: a first assessment* e, sempre a cura del Centre on Regulation in Europe (maggio 2021), lo studio intitolato *Making the Digital Markets Act more resilient and effective*; si veda, infine, A. de Streel, P. Larouche, *The European Digital Markets Act proposal: How to improve a regulatory revolution*, in "Concurrences", 2021, n. 2, p. 46-63.

[25]Aa.Vv., *Costituzionalismo e globalizzazione*, Atti del xvii convegno annuale AIC, Jovene, 2014, 217 p.; G. Azzariti, *Il costituzionalismo moderno può sopravvivere?*, Laterza, 2013, spec. pp. 1-56; F. Balaguer Callejón, *Social network, società tecnologiche e democrazia*, in "Nomos", 2019, n. 3, pp. 1-19; A. Gatti, *Istituzioni e anarchia nella rete. I paradigmi tradizionali della sovranità alla prova di Internet*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 3, pp. 711-742; T. Groppi, *Alle frontiere dello stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in "Consulta Online", 2020, n. 3, pp. 675-683; E. Maestri, *Lex informatica e soft law. Le architetture normative del cyberspazio*, in "Ars interpretandi", 2017, n. 1, pp. 15-28; O. Pollicino, *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "Federalismi.it", 2019, n. 19, pp. 1-15; A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in questa Rivista, 2020, n. 1, pp. 5-34; Id., *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in "MediaLaws", 2020, n. 3, pp. 178-195.

[26]È certamente merito di L. Lessig (*Code 2.0.*, Basic Books, 2006) aver sollevato l'attenzione dei giuristi sul fatto che il design (l'architettura) condizioni il comportamento e le scelte individuali tanto nel mondo reale quanto in quello digitale (*code is law*). Sulla funzione architetturale del codice si veda anche R. Kitchin, M. Dodge, *Code/Space: software and everyday life*, Cambridge, MIT Press, 2011, 304 p. In Italia G. Sartor (*Il diritto della rete globale*, in "Ciberspazio e diritto", 2003, n. 1, pp. 67-94) ha da tempo evidenziato come il cyberspazio sia soggetto a un graduale processo di colonizzazione da parte dei propri attori, che ne plasmano l'architettura. In particolare, sul crescente ruolo delle imprese multinazionali di promotrici di un "diritto senza Stato" derivante dalla *corporate governance* si veda G. Teubner, *Codes of conduct delle imprese multinazionali: effettività e legittimità*, Editoriale Scientifica, 2009, 44 p. Più recentemente ed estesamente, Id., *Ibridi e attanti. Attori collettivi ed enti non umani nella società e nel diritto*, Mimesis, 2015, 223 p.

[27]Fra coloro che confutano l'idea che le regole di derivazione tecnico-scientifica possano davvero costituire un fattore di disgregazione per l'ordinamento democratico fondato sulla rappresentanza politica E. Castorina, *Scienza, tecnica e diritto costituzionale*, in "Rivista AIC", 2015, n. 4, pp. 1-49.

[28]L. Belli, L. Zingales, *Platform value(s): A multidimensional framework for online responsibility*, in "Computer Law & Security Review", vol. 36, 2020, p. 1-8; G. Teubner, *Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution*, in "The Italian Law Journal", 2017, n. 1, p. 193-205.

[29]J.M. Balkin, *Old School/New School Speech Regulation*, in "Harward Law Review", vol. 127, 2014, n. 8, p. 2296-2342. Id., *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in "UC Davis Law Review", vol. 51, 2018, n. 3, p. 1149-1210. Si veda anche M. Bettoni, *Profili giuridici della privatizzazione della censura*, in "Ciberspazio e diritto", 2011, n. 4, pp. 363-384.

[30]M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in questa Rivista, 2019, n. 1, pp. 35-51. Si veda inoltre T. Gillespie, *Custodians of the Internet. Platforms, content*

moderation and the hidden decisions that shape social media, Yale University Press, 2018, 277 p.

[31]Sulla necessità di sviluppare un "costituzionalismo digitale multilivello" mediante l'individuazione di nuovi centri di potere complementari rispetto a quelli statuali, in modo da indirizzare le *tech companies* verso il rispetto dei principi e valori costituzionali, si veda N. Suzor, *A constitutional moment: How we might reimagine platform governance*, in "Computer Law &Technology Review", vol. 36, 2020, p. 1-4.

[32]Si veda in proposito C. Sartoretti, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in "Federalismi.it", 2019, n. 13, pp. 1-31.

[33]Doc. COM(2020) 825 cit. Si veda in proposito il dossier n. 51 (12 maggio 2021) predisposto dalla Camera dei deputati, Ufficio rapporti con l'Unione europea. Rispetto alla proposta di DMA, nel DSA gli Stati membri mantengono un certo ruolo nella vigilanza sugli intermediari digitali, almeno con riferimento alle piattaforme di dimensioni "normali", nonché la responsabilità principale del controllo sull'applicazione della normativa.

[34]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 (direttiva sul commercio elettronico).

[35]P9_TA(2020)0272, P9_TA(2020)0273 e P9_TA(2020)0274.

[36]Direttiva 2015/1535/UE del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[37]Ad esempio, i servizi di connessione a Internet.

[38]Per esempio, i servizi di posta elettronica, di messaggistica istantanea o di *home banking*.

[39]Tutti i servizi che prevedono la memorizzazione permanente di informazioni, fra cui *ex multis* i social network o i servizi di *cloud storage*.

[40]Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi).

[41]Il collegamento sostanziale sussisterebbe non solo nel caso in cui il prestatore del servizio è stabilito nell'Unione, ma potrebbe anche desumersi sulla base dell'esistenza di un numero considerevole di utenti in uno o più Stati membri o dell'orientamento delle attività verso uno o più Stati membri.

[42]Sulla (ir)responsabilità del provider per i contenuti diffusi dagli utenti attraverso le piattaforme digitali mi sia consentito il rinvio a M.R. Allegri, *Ubi social Ibi ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2019, spec. pp. 53-74, nonché alla bibliografia ivi citata. Si vedano inoltre, fra gli scritti più recenti su questo argomento: L. Albertini, *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in "MediaLaws, Law and Media Working Paper Series", 2019, n. 4, pp. 1-182; R. Cosio, *La responsabilità del prestatore di servizi di hosting*, in "Jus civile", 2020, n. 4, pp. 887-905; G. D'Alfonso, *Verso una maggiore responsabilizzazione dell'*hosting provider *tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive* de jure condendo, in "Federalismi.it", 2020, n. 2, pp. 108-147; M.L. Montagnani, *Internet, contenuti illeciti e responsabilità degli intermediari*, Egea, 2018, 266 p.; C. Novelli, *Il social giudizioso. La giurisprudenza italiana sulla responsabilità civile degli Internet Service Providers*, in questa Rivista, 2019, n. 1, pp. 97-106; R. Panetta, *Il ruolo dell'Internet Service Provider e i profili di responsabilità civile*, in "Responsabilità civile e previdenza", 2019, n. 3, pp. 1017-1035; E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider – passivi e attivi – tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in "Rivista di diritto industriale", 2017, n. 1, pp. 75-122.

[43]Per la verità, il percorso verso il riconoscimento anche normativo dell'ineludibile funzione "attiva" (cioè di organizzazione e gestione dei contenuti) delle piattaforme digitali, intimamente connessa alla loro stessa natura, è iniziato già da qualche anno. Ad esempio, la direttiva 2018/1808/UE del 14 novembre 2018, che ha modificato la precedente direttiva 2010/13/UE sui servizi di media audiovisivi, contiene una definizione di "servizio di piattaforma per la condivisione di video" (art. 1, par. 1, lett. a bis) secondo la quale, pur non avendo responsabilità editoriale, il gestore della piattaforma determina l'organizzazione del servizio «anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento». Analogamente, la direttiva 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale, del 17 aprile 2019, stabilisce all'art. 2 par. 6 che il «prestatore di servizi di condivisione di contenuti online» ha lo scopo di «di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro». È evidente, quindi, che a un intermediario di questo tipo non può essere attribuita una posizione di neutralità rispetto ai contenuti veicolati dalla piattaforma. Del resto, l'art. 17 della medesima direttiva addirittura impone al fornitore di tali servizi di attivarsi presso i titolari dei diritti di proprietà intellettuale al fine di ottenere da essi l'autorizzazione a diffondere le opere protette dal diritto d'autore e prescrive che, onde sfuggire alla responsabilità derivante dalla divulgazione non autorizzata di opere protette, il provider debba dimostrare di aver compiuto il massimo sforzo per ottenere l'autorizzazione, di aver adottato elevati standard di diligenza professionale e di aver agito tempestivamente, in seguito a segnalazione dei titolari dei diritti, per disabilitare l'accesso ai contenuti contestati. Si assiste quindi, in relazione alla protezione del diritto d'autore, a un completo capovolgimento della posizione del provider rispetto alla direttiva sul commercio elettronico 2000/31/CE: se nella direttiva *e-commerce* la posizione di neutralità del provider era presunta ai fini dell'esenzione dalla responsabilità, in quella sul diritto d'autore invece, per il medesimo fine, è necessario che il provider dimostri di aver tenuto un comportamento proattivo.

[44]In particolare, gli artt. 16 e 17 del d. lgs. 70/2003, con cui la direttiva *e-commerce* è stata recepita nell'ordinamento giuridico italiano, non paiono pienamente conformi alla direttiva, lasciando infatti intendere che la conoscenza dell'illecito da parte del provider possa considerarsi acquisita solo in conseguenza di una comunicazione proveniente dalle competenti autorità giudiziarie e amministrative e non *aliunde*, e che il provider debba attivarsi per la rimozione o disabilitazione dei contenuti illeciti sono su richiesta delle suddette autorità e non anche spontaneamente. Tuttavia, secondo un consolidato orientamento giurisprudenziale (ad esempio, CGUE, *L'Oreal c. eBay*, 12 luglio 2011, causa C-324/09; CGUE, *GS Media BV c. Sanoma ed altri*, 8 settembre 2016, causa C-160/15) la responsabilità civile dell'*hosting provider* sussiste invece in tutti i casi in cui egli abbia avuto effettiva conoscenza dell'illiceità di talune attività o taluni contenuti, a prescindere dalla natura e dalle caratteristiche, anche formali, della comunicazione ricevuta, che potrebbe provenire anche dallo stesso utente danneggiato; inoltre, la limitazione di responsabilità non può essere applicata al provider che, sulla base dei crite-

ri di diligenza e ragionevolezza, abbia omesso di attivarsi per impedire la prosecuzione dell'illecito. Anche a livello nazionale, pur omettendo di esaminare in questa sede la cospicua giurisprudenza di merito (per la quale si rimanda alla bibliografia citata nella nota 42), va ricordata almeno la sentenza della Corte di Cassazione, sez. I civ., n. 7708 del 19 marzo 2019 (*RTI c. Yahoo!*). In tale occasione la Corte ha affermato che la nozione di hosting provider attivo – quello cioè che «svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito» e che pertanto non si sottrae all'applicazione delle comuni regole sulla responsabilità civile – «può ormai ritenersi dunque un approdo acquisito in ambito comunitario». Così, in linea con quanto già affermato da tempo da CGUE (12 luglio 2011, causa C-324/09), la Cassazione ha ribadito che la valutazione del giudice sulla conoscenza da parte del provider dell'esistenza di un'attività o di un'informazione illecita va condotta alla stregua della diligenza professionale esigibile dall'operatore economico.

[45]In particolare, in *Scarlet extended c. Sabam*, 24 novembre 2011, causa C-70/10, la CGUE ha categoricamente escluso che sia possibile imporre ad un fornitore di servizi di accesso ad Internet di predisporre un sistema di filtraggio preventivo dei contenuti. La *ratio* del divieto era allora rinvenibile nell'eccessiva complessità e onerosità di tali sistemi, che avrebbero causato «una grave violazione della libertà di impresa del fornitore di cui trattasi, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico». Più o meno negli stessi termini («un'ingiunzione siffatta non rispetterebbe l'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e, dall'altro, quella della libertà d'impresa, di cui beneficiano operatori quali i prestatori di servizi di *hosting*») si è espressa la CGUE anche in *Sabam c. Netlog*, 16 febbraio 2012, causa C-360/10. Se si ragiona solo in termini di libertà di impresa, a distanza di un decennio da tale sentenza, in considerazione dell'enorme sviluppo che hanno avuto le tecnologie algoritmiche e del fatto che abitualmente ormai le piattaforme digitali adottano sistemi di monitoraggio e moderazione dei contenuti, si può per lo meno discutere dell'opportunità di mantenere in vita tale divieto. Se invece si ragiona in termini di libertà di manifestazione del pensiero, e si parte dal presupposto della rischiosità di affidare a *tech companies* private il ruolo di controllori/censori dei contenuti espressi online, la *ratio* del mantenimento del divieto è perfettamente giustificabile. Del resto, che oggi procedere a un monitoraggio selettivo dei contenuti non sia più un'operazione particolarmente onerosa per il provider è un elemento che la CGUE ha acquisito nella recente sentenza *Eva Glawischnig-Piesczek c. Facebook*, 3 ottobre 2019, causa C-18/18, in cui ha ammesso che l'intermediario digitale debba necessariamente operare in tal senso al fine di individuare i contenuti non solo identici, ma anche equivalenti a quelli contestati. Secondo la Corte, infatti, considerata la facilità di riproduzione delle informazioni in Internet, tale obbligo di sorveglianza attivo risulta necessario per assicurare la protezione efficace della vita privata e dei diritti della personalità e non comporta un onere eccessivo a carico dell'intermediario digitale. Così la Corte ha configurato un obbligo di sorveglianza anche rivolto al futuro, applicato a tutti gli utenti della piattaforma e a tutte le informazioni ivi presenti, volto anche a prevenire il successivo caricamento di informazioni identiche o equivalenti a quelle contestate e quindi il ripetersi di analoghe violazioni. Sulla sentenza *Glawischnig-Piesczek c. Facebook* si veda il commento di O. Pollicino, *op. cit.*

[46]L'art. 2 lett. f della proposta di regolamento definisce i prestatori di servizi di *hosting* come quelli che quelli che memorizzano le informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo. In questa categoria potrebbero rientrare, ad esempio, i fornitori di servizi di *cloud*.

[47]*Digital Millennium Copyright Act*, 1998.

[48]Con la proposta di DSA, l'allestimento di procedure di *notice-and-take-down* da parte degli *hosting provider* – al momento previsto solo nell'ambito della cooperazione volontaria instaurata mediante l'adesione ai codici di condotta promossi dalla Commissione europea per contrastare lo *hate speech* (2016) e la disinformazione (2018) online – diventerebbe un obbligo giuridicamente vincolante.

[49]Tale lacuna è stata quindi colmata per via giurisprudenziale. In Italia la giurisprudenza dominante ritiene che la diffida trasmessa dal soggetto danneggiato all'indirizzo del fornitore del servizio (*ex* art. 1219 c.c.) sia l'unico strumento idoneo a denunciare prontamente la lesione (attuale o potenziale) di una privativa industriale, del diritto d'autore o dei dati personali di un soggetto. Peraltro, qualora il diritto che si intende tutelare derivi da fatto illecito, la diffida sarebbe addirittura facoltativa. Tuttavia, non è chiaro il contenuto che la diffida deve avere per poter compiutamente mettere il provider nelle condizioni di potersi attivare rimuovendo il contenuto contestato senza pregiudicare il suo diritto o quello dell'utente a veicolare le informazioni. In varie occasioni, la giurisprudenza di merito in Italia ha affermato che una diffida priva dell'indicazione degli URL (*Uniform Resources Locator*) o dei link al materiale illecito sarebbe inidonea a individuare gli esatti contenuti illeciti contestati, ma va evidenziato che l'onere di indicare gli URL non è affatto previsto dalla direttiva 2000/31/CE e, anzi, può apparire in contrasto con il tenore delle sue disposizioni.

[50]Come spiegato nella nota precedente, la normativa attualmente vigente non prevede in alcun modo che l'effettiva conoscenza dell'illecito da parte dell'*hosting provider* possa avvenire solo se il soggetto leso, in sede di diffida cautelare, indichi precisamente gli URL corrispondenti ai contenuti di cui si chiede la rimozione, anche se ciò è stato più volte richiesto dalla giurisprudenza nazionale. Peraltro, in *Eva Glawischnig-Piesczek c. Facebook*, cit., la CGUE ha stabilito, in sede di rinvio pregiudiziale, che i giudici nazionali possono ordinare a un prestatore di servizi di *hosting* (nella fattispecie Facebook) di rimuovere o di bloccare l'accesso non solo a contenuti illeciti specificatamente indicati dal ricorrente, ma anche a informazioni "identiche" o "equivalenti" ad essi. Certamente, la nozione di contenuto equivalente possiede un'intrinseca vaghezza che si presta a interpretazioni discrezionali del provider. Per questo, dovendo necessariamente prescindere dall'esatta indicazione dell'URL, la Corte ha stabilito che il giudice, onde assicurare la certezza del diritto, dovrà individuare in maniera chiara, precisa e prevedibile i contenuti da rimuovere, individuando gli elementi specifici da prendere in considerazione (ad es. il nome della persona interessata dalla violazione, oppure le circostanze in cui è stata accertata tale violazione) e consentendo all'utente la possibilità di contestare la misura adottata dall'*hosting provider* nei suoi confronti. Su questa sentenza si leggano i commenti di R. Cosio, *op. cit.*, p. 897 ss.; G. De Gregorio, *Moderazione dei contenuti in rete: poteri privati tra prospettive locali e prospettive globali*, in "Quaderni costituzionali", 2020, n. 1, pp. 176-180; O. Pollicino, *op. cit.*

[51]Onde evitare condotte abusive, nel caso di utenti che con frequenza presentano notifiche o reclami manifestamente infondati, le piattaforme digitali potranno reagire sospendendo per un ragionevole periodo di tempo il trattamento di notifiche o reclami da essi presentati (art. 20 par. 2).

[52]Sulla attuale ambiguità normativa riguardo alla necessità di indicare o meno gli URL esatti si vedano le note nn. 49 e 50.

[53]Fin dal 2008, con la decisione-quadro 2008/913/Gai del Consiglio del 28 novembre 2008 sulla lotta contro talune for-

me ed espressioni di razzismo e xenofobia mediante il diritto penale, gli Stati membri dell'UE si sono impegnati a prevedere sanzioni penali per i comportamenti di stampo razzista e xenofobo, in particolare «l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica», nonché «l'apologia, la negazione o la minimizzazione grossolana dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra», quando però tali comportamenti siano posti in essere in modo atto a istigare alla violenza o all'odio nei confronti di gruppo – o di un suo membro – «definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica». A questa prima categoria di contenuti illeciti, che possono essere veicolati anche online, si aggiungono quelli previsti in alcune direttive settoriali approvate nello scorso decennio. In primo luogo, la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che ha introdotto sanzioni penali minime, che gli Stati membri possono eventualmente aggravare, per una serie di reati commessi ai danni di minori e che impone agli Stati membri (art. 25) l'adozione di misure per assicurare la tempestiva rimozione o il blocco delle pagine web che contengono o diffondono materiale pedopornografico. In secondo luogo, la direttiva antiterrorismo 2017/541/UE, che qualifica una cospicua serie di reati consistenti in attività terroristiche, collegati al terrorismo o riconducibili al terrorismo, imponendo agli Stati membri di prevedere nel proprio ordinamento giuridico la punibilità di tali condotte, nonché (art. 21) di adottare le misure necessarie a contrastare i contenuti online che incitano a commettere atti di terrorismo. In terzo luogo, la direttiva sui servizi di media audiovisivi 2018/1808/UE, che prevede (art. 28 ter) che i fornitori di piattaforme per la condivisione di video adottino misure adeguate contro quei contenuti audiovisivi che possono risultare nocivi per lo sviluppo fisico e mentale dei minori o, più in generale, che istigano alla violenza, all'odio o alla discriminazione. Infine, la direttiva copyright 2019/790/UE, che consente al provider (art. 17 par. 4) di rendere accessibili sulla propria piattaforma materiali coperti dal diritto d'autore solo a seguito della stipula di un contratto di licenza d'uso con il titolare del diritto. A queste quattro direttive, che vanno nel senso di una più chiara tipizzazione dei contenuti illeciti online, va aggiunta la proposta di regolamento relativo alla prevenzione della diffusione di contenuti terroristici online – doc. COM(2018) 640 del 12 settembre 2018 – che stabilisce una definizione di contenuti terroristici online in conformità alla definizione di reati di terrorismo di cui alla direttiva 2017/541/UE. In particolare, secondo la proposta di regolamento, i prestatori di servizi di hosting sono tenuti a prevenire la diffusione di contenuti terroristici attraverso misure proattive che possono comportare anche l'uso di strumenti automatizzati e, su richiesta delle competenti autorità, sono tenuti a rimuoverli. I contenuti terroristici sono definiti dall'art. 2 par. 5: messaggi che istigano alla commissione di reati di terrorismo, anche mediante l'apologia, o che incitano a contribuire alla loro commissione; contenuti che promuovono le attività di gruppi terroristici, incoraggiando la partecipazione o il sostegno nei loro confronti; istruzioni su metodi e tecniche da utilizzare per commettere reati di terrorismo.

[54] Sulle ragioni alla base dell'opacità dei sistemi di *content moderation* utilizzati dalle piattaforme digitali e sulla necessità di una maggiore trasparenza in quest'ambito, anche attraverso la pubblicazione di una *content moderation notice* destinata agli utenti, si veda G. De Gregorio, *Democratising online content moderation: A constitutional framework*, in "Computer Law & Security Review", vol. 36, 2020, p. 1-17.

[55] Le piattaforme digitali sono considerate (art. 2 lett. h della proposta di regolamento) un tipo particolare di prestatori di servizi di *hosting*. Esse sono caratterizzate dal fatto che, oltre alla memorizzazione delle informazioni, provvedono anche alla loro diffusione al pubblico (come, ad esempio, è il caso dei social network) a meno che tale attività non sia una funzione minore e puramente accessoria di un altro servizio (come è il caso, ad esempio, dei commenti degli utenti che accompagnano gli articoli di un giornale online).

[56] Quelle, cioè, che rispondono alla definizione fornita nell'allegato alla raccomandazione 2003/361/CE.

[57] Al momento la trasparenza della pubblicità politica è prevista solo in via di autoregolamentazione e le piattaforme utilizzano in tale ambito policies molto differenziate fra loro. Si veda su questo M.R. Allegri, *Oltre la par condicio. Comunicazione politico-elettorale nei social media, fra diritto e autodisciplina*, FrancoAngeli, 2020, spec. pp. 102-104, 140-158, 175-185. Al di là dello specifico caso della pubblicità politica, al momento non vi sono indicazioni normative riguardanti la trasparenza dei messaggi pubblicitari *tout court* diffusi via Internet. Peraltro, la proposta di DSA incoraggia esplicitamente l'adozione di codici di condotta da parte degli intermediari digitali per favorire corretta applicazione del regolamento (art. 35), con un particolare riferimento alla predisposizione di codici di condotta specificamente dedicati alla trasparenza della pubblicità online (art. 36). La Commissione europea e il Comitato per i servizi digitali contribuirebbero alla definizione dei contenuti di tali codici di condotta, in modo che rispondano adeguatamente agli obiettivi previsti, e si occuperebbero del monitoraggio relativamente alla loro attuazione. La formula prescelta, dunque, è quella della co-regolamentazione, in luogo della mera *self-regulation*.

[58] La proposta di DSA prevede la creazione di nuove autorità nazionali (i Coordinatori nazionali dei servizi digitali) su cui si veda la nota successiva.

[59] Il Coordinatore dei servizi digitali, previsto dalla proposta di regolamento agli artt. 38-41, sarebbe una nuova autorità nazionale indipendente preposta alla vigilanza sul rispetto del regolamento e responsabile per tutti gli aspetti relativi alla sua applicazione, mediante l'esercizio di poteri sia investigativi che esecutivi.

[60] Il Comitato europeo dei servizi digitali (artt. 47-49) sarebbe un gruppo consultivo presieduto dalla Commissione europea e composto dai coordinatori dei servizi digitali, rappresentati da funzionari di alto livello. Il Comitato è definito "indipendente", ma è in realtà composto da Autorità nazionali, con la precisazione che al suo interno ogni Stato membro dispone di un voto, mentre la Commissione europea non ha diritto di voto. Quindi, a dispetto della dichiarata indipendenza, l'organo avrebbe le caratteristiche di una struttura intergovernativa di coordinamento. I suoi compiti consisterebbero nella consulenza e nell'assistenza prestata ai Coordinatori nazionali dei servizi digitali e alla Commissione europea.

[61] Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, 1999, p. 17.

The digital future of the European Union: new categories of online intermediaries, new forms of liability

Abstract: The "digital package" proposed by the European Commission in December 2020 marks the affirmation of the Union as a center of sovereign power over the digital environment, not only with respect to the large multinational companies that manage the flow of information on the Internet, but also with respect to the national States, which are gradually losing the possibility to regulate the phenomena occurring online independently. To achieve this goal, the European Commission has moved mainly along three lines: 1) the data sharing for the development of artificial intelligence systems; 2) a greater control over gatekeepers (i.e., digital platforms that can condition access to the market) in order to prevent them from abusing their dominant position; 3) a greater accountability of digital intermediaries for the contents produced and disseminated by the end users of their services, paying particular attention to large-scale platforms. This undermines the principle of provider neutrality, sanctioned by the European directive on electronic commerce dating back to 2000. Through the reaffirmation of its digital sovereignty, the European Union seems to reclaim its nature as an area of rights and freedom, capable to ensure an anthropocentric and personalist governance of innovation.

Keywords: European Commission – Digital Package – Online Intermediaries