Papers di DIRITTO EUROPEO

www.papersdidirittoeuropeo.eu
ISSN 2038-0461

2021, n. 1

Rivista scientifica online
Papers di diritto europeo
www.papersdidirittoeuropeo.eu

I contributi sono sottoposti ad un procedimento di revisione tra pari a doppio cieco (*double-blind peer review*).
Non sono sottoposti a referaggio esclusivamente i contributi di professori emeriti, di professori ordinari in quiescenza e di giudici di giurisdizioni superiori e internazionali.

Rivista scientifica online "*Papers di diritto europeo*"
ISSN 2038-0461
Registrazione al Tribunale di Verona n. 1875 del 22 luglio 2010

Rivista scientifica online
Papers di diritto europeo
www.papersdidirittoeuropeo.eu

Fascicolo 2021, n. 1

INDICE

Presentazione

Ad oltre dieci anni dalla prima pubblicazione, il presente fascicolo dei *Papers di diritto europeo* rappresenta una tappa significativa nella vita della Rivista online.

In linea di continuità con il progetto editoriale sino ad ora sviluppato, la Rivista si propone di raccogliere i contributi di docenti e, in generale, di esperti e di ricercatori interessati agli studi di diritto europeo, alla luce anche dei suoi riflessi sugli ordinamenti nazionali, in una prospettiva non limitata al Diritto dell'Unione europea, ma suscettibile di favorire un dibattito scientifico in chiave multidisciplinare.

Il progetto ha comportato un ampliamento degli organi esistenti, integrati per prevedere la partecipazione di un maggior numero di studiosi provenienti da prestigiose università sia italiane sia straniere, nonché un rinnovamento della veste grafica dei *Papers* e del sito web che li ospita.

Gli articoli continueranno ad essere sottoposti ad un processo di revisione tra pari a doppio cieco (*double-blind peer review*) e ad essere pubblicati, semestralmente, in modalità *open access*. Ciò risponde non solo alla volontà di espandere la loro fruibilità e diffusione, ma soprattutto all'obiettivo di stimolare in maniera quanto più efficace possibile il confronto sui molteplici argomenti connessi all'integrazione europea, nella convinzione di contribuire in tal modo a una più compiuta riflessione scientifica.

Il primo numero del 2021 della Rivista, in particolare, raccoglie i contributi dei relatori intervenuti al webinar "La transizione digitale e le sfide per l'Unione europea", organizzato in data 18 gennaio 2021 in collaborazione con il Corso di Dottorato in Scienze giuridiche europee ed internazionali dell'Università di Verona e rientrante nel Progetto 2020 della Rete italiana dei Centri di documentazione europea, dal titolo "Verso la Conferenza sul futuro dell'Europa". All'editoriale del prof. Bassan, seguono i contributi del prof. Cafari Panico in tema di protezione dei dati nello spazio cibernetico ed efficacia extraterritoriale del diritto UE; del prof. Caggiano sulla tutela dei diritti fondamentali nel quadro del *Digital Services Act*; e del prof. Contaldi sulla proposta della Commissione di *Digital Markets Act*. Infine, sono pubblicati gli articoli di tre dottorandi di ricerca dell'Università di Verona intervenuti nella seconda parte del webinar.

L'auspicio è che altri Colleghi, così come giovani studiosi, con i loro approfondimenti e le loro ricerche concorrano a rendere, con rinnovato slancio, la Rivista *Papers di diritto europeo* un attivo e dinamico spazio accademico di discussione e di divulgazione.

Il Direttore Responsabile
Maria Caterina Baruffi

Editoriale

Piattaforma Europa

Fabio Bassan*

Sembra il contrario di *lockdown* ma *lockUp* non lo è: in piedi, fuori di casa, ma sorvegliato. Nei mercati finanziari *lockUp* indica la fase di "sospensione" in cui i titoli non possono essere trattati. Sorvegliati e sospesi. Questo è il nuovo mondo, bellezza. E a dircelo non sono i CEO delle aziende che esercitano il controllo, che anzi, sono diventati i paladini della protezione dei nostri dati; ce lo dicono i governanti, che dell'uso dei nostri dati hanno bisogno per gestire l'emergenza pubblica. Al grido del "non si può fare diversamente" si invoca lo stato di necessità, che legittima deroghe ai diritti, da sempre. Le reazioni popolari sono diverse e dipendono in gran parte dal *welfare* cui sono state abituate e dai fondamenti (filosofico-religiosi) delle rispettive culture: diversa è la risposta confuciana fondata sulla prevalenza dell'interesse pubblico rispetto a quello dell'individuo, da quella occidentale, che l'individuo l'ha liberato ma lasciato solo a gestire la paura (della libertà o del controllo, a seconda dell'urgenza del caso).

La domanda che ci si pone è se quest'universo parallelo in cui siamo finiti quasi inconsapevolmente ma che – ormai è chiaro – sarà il nostro habitat futuro, consente lo sviluppo fisiologico del modello regolatorio che si stava delineando in Europa, o lo acceleri. O se, al contrario, l'evoluzione sarà superata da una rivoluzione necessaria.

Gli effetti della pandemia sugli sviluppi della regolazione sono studiati dagli economisti e dai giuristi. I primi seguono le tracce dei mercati, i secondi le interpretano, le classificano, le mettono nei cassetti che ci sono già. A volte, raramente (meno di quel che sarebbe utile o necessario) ne creano di nuovi. È quel provo a fare con queste brevi riflessioni, con maggiore difficoltà perché la pandemia le tracce le ha nascoste o confuse e ne ha create altre, molte false. Rappresento quindi qui un primo risultato, ovviamente preliminare e provvisorio, come sempre quando alla storia si deve sostituire la cronaca. Al centro, come d'abitudine nelle analisi contemporanee, mettiamo l'individuo che – lo dicevo negli anni scorsi sottovoce, ora è chiaro a molti – è il soggetto meritevole di tutela, ancor prima di diventare consumatore (o investitore, correntista, assicurato, utente di un *social network*, secondo gli schemi classici dei silos verticali e orizzontali posti a matrice).

* Professore ordinario di Diritto internazionale, Università degli Studi di Roma Tre.

Ai soli fini interpretativi, e per delineare lo scenario, muovo da alcuni presupposti. Il primo: siamo in una fase nuova dell'Unione europea: l'era della "politica di crescita europea solidale necessaria". La crescita deve essere sostenibile (*green*) e solidale: anche la Germania è consapevole ormai che la "regionalizzazione" della globalizzazione rende ancor più vitale il mercato europeo, per cui la concorrenza tra ordinamenti non è più un interesse da perseguire ma un pericolo da evitare. Questo produce effetti diretti anche sulla regolazione e sugli strumenti utilizzati per attuarla: sempre più regolamenti, sempre più un *corpus* normativo unico, generale.

Il secondo: la matrice regolatoria si sta sgretolando. I silos verticali (bancario, assicurativo, mercati finanziari, energetico, dei trasporti, ecc.) non sono più paralleli: s'integrano o si divaricano a seconda delle urgenze e delle necessità. Qualche esempio. Le banche vendono prodotti assicurativi, finanziari, misti, e il tema regolatorio si pone qui in termini di prevalenza o di *cross-regulation*. La convergenza tra telecomunicazioni e televisione è preistoria e la frontiera si è spostata sulle piattaforme digitali, cresciute nel loro *sandbox ante-litteram* (in Europa, la direttiva del 2000 sul commercio elettronico[1], che ha loro garantito negli anni, di fatto, l'esenzione da responsabilità) e sono ormai *too big to care*. Che dire poi della convergenza nei trasporti, dove il grado di sostituzione ha superato da tempo la soglia dei mercati. Quanto ai silos orizzontali (concorrenza, protezione dei dati personali e tutela del consumatore), cercano il modo di superare i vincoli storici divenuti ormai insopportabili. Così è la territorialità per la protezione dei dati[2], le soglie economiche e di fatturato per il diritto della concorrenza ("modernizzazione"), la definizione di consumatore quanto al beneficiario delle tutele.

Il terzo presupposto concerne la reazione regolatoria: la regolazione classica, per soggetti, si è trasformata rapidamente in regolazione per attività e ora per prodotti. Fino ad arrivare, in questi mesi, alla presa d'atto del fallimento di una regolazione che insegue l'evoluzione dei mercati, e inizia una nuova fase. Già prevista, dagli osservatori più attenti; gli eventi l'hanno accelerata. La nuova Commissione europea, insediatasi da diciotto mesi, ha adottato decisioni eccezionali per fronteggiare una crisi eccezionale, ma ha anche strutturato un intervento nel medio-lungo periodo per affrontare i mercati. Questa strategia è facilitata ora dal recesso della Gran Bretagna, che porta via con sé (anche) un'avversione alla codificazione dell'Europa continentale. Le tradizioni giuridiche tornano così alle origini, ciascuna per proprio conto. La Commissione UE può quindi ora proporre un nuovo paradigma regolatorio, non più spurio, fondato su una codificazione generale (applicabile a tutti i settori) e dunque per principi, con applicazioni

[1] 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»).

[2] Corte di giustizia, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems* c. *Data Protection Commissioner* (c.d. *Schrems I*) e 16 luglio 2020, causa C-311/18, *Data Protection Commissioner* c. *Facebook Ireland Limited e Maximillian Schrems* (c.d. *Schrems II*).

specifiche (non settoriali, ma in ragione dei singoli prodotti o servizi) che nascono dal mercato, secondo quel "circolo regolatorio" che ho illustrato di recente[3]. In sintesi: le *best practices* sul mercato vengono assunte dalle Autorità nazionali di regolazione e vigilanza come *benchmark* portati nel consesso delle autorità europee, che elaborano standard tecnici o, quando necessario, proposte alla Commissione UE la quale, se sufficiente, adotta atti esecutivi, altrimenti propone atti legislativi che poi Consiglio UE e Parlamento UE approvano, rendendoli vincolanti. Il vantaggio del "circolo regolatorio" è che le pratiche migliori sono vincolanti (auto-vincolanti le imprese che le adottano) da subito, o da quando le autorità nazionali e/o europee le propongono, come standard o linee-guida. Questo rileva anche su un fronte peculiare dell'innovazione tecnologica, non ignorato dalla dottrina ma tuttora senza soluzione: il rapporto tra norme etiche e regole giuridiche, separate dal velo creato in due secoli di teoria generale del diritto e ora strappato dall'intelligenza artificiale. Il circolo regolatorio fa parte delle soluzioni, non del problema: consente all'uomo di intervenire (così, l'algoritmo non fa da sé) per selezionare le pratiche che si trasformano in norme e, in questa prospettiva, diventano tali anche le regole di Asimov (3+1).

Il quarto presupposto: regolazione pubblica e privata sono due vasi comunicanti. Il pubblico interviene quando il privato non riesce o fallisce: sussidiarietà, applicata. È più di un'ipotesi ricostruttiva perché funziona sempre e assurge quindi a regola generale. Se inserita in questa prospettiva, si comprende la strategia della nuova Commissione europea, che affida l'applicazione concreta delle norme e dei principi al mercato e al circolo regolatorio. E si capisce anche la Corte di giustizia UE[4], che non si limita ad annullare la regolazione pubblica viziata ma suggerisce di sviluppare intanto quella privata (le clausole contrattuali-tipo), cui l'altra farà da cornice. E qui, il compito di regolatori, garanti e vigilanti diventa decisivo, nel ruolo che devono esercitare nel "circolo" e così le associazioni dei consumatori, che questo ruolo forse devono ancora prenderselo. Ma diventa nuovamente decisiva anche l'attività di soggetti ingiustamente ignorati nell'ultima fase storica, che la codificazione di diritto uniforme l'hanno prodotta e in modo efficace: UNIDROIT, UNCITRAL, sono le sedi in cui i contratti internazionali hanno trovato standard oggi comunemente applicati e tornano ad essere (le più) indicate nella fase attuale in cui le regole europee stanno strette, che hanno il vincolo territoriale. Analogamente, l'OCSE, sede idonea e adeguata per l'elaborazione di GAPPS (*General Accepted Practices and Principles*).

E veniamo così al quinto presupposto: le piattaforme digitali sono i nuovi soggetti nel mercato (ma non solo) e non possono essere destinatarie della regolazione classica, che è inefficace: è un radar rispetto al quale volano troppo alte, o troppo basse (a seconda dei casi e delle interpretazioni). Algoritmi e intelligenza artificiale, ecosistemi a-

[3] F. BASSAN, *Potere dell'algoritmo e resistenza dei mercati in Italia*, Catanzaro, 2019.
[4] Da ultimo, sentenza *Schrems II*, cit.

normativi, si sviluppano con una disciplina autonoma, in deroga. È legittimo qui l'intervento regolatorio, per garantire e tutelare i diritti sul piano contrattuale, e per individuare e ripartire le responsabilità su quello extracontrattuale (quando il danno è prodotto da un atto illecito). Regolazione pubblica, sussidiaria, via circolo regolatorio. La prima mossa spetta al mercato. Vecchi diritti non sono più azionabili, nuovi vanno garantiti.

Presupposto numero sei: questa impostazione regolatoria è avversata dalle "imprese di mezzo" (niente a che vedere con le imprese medie). Sono quelle che non hanno potere contrattuale con le piattaforme transnazionali digitali, e non possono contare su un *floor* normativo che da un lato le tuteli, dall'altro garantisca correttezza dell'operato, se conforme. Le soluzioni legislative, regolatorie, giudiziali – norme per principi, applicazioni "mercatorie" – le lasciano esposte ai rischi, sia negoziali (non hanno potere) sia di *compliance* (non hanno certezze). La soluzione qui esiste ed è indicata e praticata dalle istituzioni europee negli ultimi anni come prioritaria, se non ideale: si chiama co-regolazione e prevede la partecipazione alla formazione della *lex mercatoria* da parte delle autorità di regolazione per compensare le asimmetrie di mercato. Consente di garantire certezza, quanto alla *compliance* e forza, nella negoziazione.

Se questi sono i presupposti condivisi qual è l'impatto della pandemia? In altre parole, il *lockUp* permanente – i picchi ci sono e rilevano per noi umani, ci mancherebbe, ma anche la quiete è latente, per cui le abitudini cambiano in modo definitivo – come modifica il quadro? Da un lato, il potere delle piattaforme digitali è cresciuto in modo evidente, sino a superare la soglia psicologica dell'abuso (che anche la FTC statunitense abbia mosso contro Google è un evento storico e produrrà conseguenze, comunque). Non ha avuto l'eco che meritava il fatto che il governo tedesco abbia dovuto modificare in corsa una legge adottata pochi giorni prima (sulla notifica di esposizione al Covid-19) perché prevedeva un *database* centralizzato, incompatibile con il sistema decentrato imposto pochi giorni dopo da Google (Android) e Apple (anche) per meglio tutelare i dati personali. Un accodo tra operatori, da questi auto-giustificato in base all'emergenza, non notificato a nessuna autorità, che ha la forza di imporsi ai governi.

Dall'altro lato, il processo di trasparenza dell'operatività dell'intelligenza artificiale si è accelerato. Se questa sia o meno una buona notizia lo vedremo nei prossimi mesi: la trasparenza dei processi era ciò che mancava per consentire alle piattaforme transnazionali digitali di presentare prodotti e servizi alle autorità di regolazione e vigilanza ed entrare, finalmente, nei mercati. La battaglia sta per iniziare, la regolazione deve essere già pronta e la modernizzazione non basta.

E dunque: la Commissione europea accelera sul *Digital Services Act* (DSA)[5], il *Digital Markets Act* (DMA)[6], il *Data Governance Act* (DGA)[7], indirizzati anche alle piattaforme, alle quali si applica già il regolamento *Platform-to-Business*[8] che appunto, prevede regole generali e un'applicazione in via contrattuale. Il DSA si pone come nucleo di norme fondamentali per l'economia digitale, *pendant* del GDPR[9] e con lo stesso obiettivo di "globalizzazione" dei diritti. Regolazione specifica è dedicata all'intelligenza Artificiale, in base ai modelli *risk based*[10].

Contestualmente, la Commissione propone la modernizzazione delle regole sulla concorrenza, per renderle efficaci nel nuovo quadro e con i nuovi assetti dei mercati digitali.

Il Consiglio UE libera l'iniziativa per un *cloud* europeo (GaiaX), che tra i vari obiettivi si propone anche quello di garantire territorialità dei dati e quindi applicazione del *welfare* unionale, poiché il "*Brussels effect*" da solo non riesce ormai più a garantire l'extraterritorialità e a impedire le deroghe alla giurisdizione (e la Corte di Giustizia l'ha chiarito ormai a più riprese).

BCE elabora regole e standard per l'EURO digitale e si vedrà poi per le cripto-valute private.

Iniziative legislative stanno per essere lanciate dalla Commissione per definire – applicando i principi di sussidiarietà e proporzionalità certo, ma anche di precauzione – le responsabilità nell'ecosistema dell'intelligenza artificiale.

Parlamento e Consiglio si accingono a varare le regole per l'azione collettiva europea, legittimando così i rappresentanti dei consumatori come soggetti attivi del circolo regolatorio.

Il processo evolutivo – così è, tradizionalmente, il cammino legislativo – che prevede l'applicazione delle norme esistenti ai fenomeni nuovi, diventa rivoluzionario quando inserito nel percorso avviato dalla nuova Commissione europea: regole per principi e norme generali, applicazioni per "codificazione mercatoria". Come già per la

[5] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 final del 15 dicembre 2020.

[6] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), COM(2020) 842 final del 15 dicembre 2020.

[7] Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), COM(2020) 767 final del 25 novembre 2020.

[8] Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

[9] 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).

[10] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final del 21 aprile 2021.

Psd2[11], recentemente, e seguendo lo standard delle liberalizzazioni degli anni ’90 del secolo scorso, nelle fasi di crasi del sistema o di discontinuità tecnologica la regolazione smette di inseguire l’innovazione e si lancia avanti, dettando il nuovo perimetro di gioco su cui i mercati si potranno esercitare. Se è la tartaruga a inseguire Achille, il paradosso non è più utile. È un atto di coraggio, per quanto necessitato ormai dal ritardo, che definisce la politica industriale (oggi: politica di crescita solidale necessaria) e merita di essere sostenuto.

[11] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

Le imprese multinazionali, la protezione dei dati nello spazio cibernetico e l'efficacia extraterritoriale del diritto dell'Unione europea

Ruggiero Cafari Panico*

SOMMARIO: 1. Considerazioni introduttive: il declinare della sovranità statale nel mondo di Internet e la difesa dei valori fondamentali dell'Unione europea. – 2. I nuovi diritti digitali e il loro ambito di applicazione. – 3. La giurisprudenza della Corte di giustizia: l'efficacia extraterritoriale del diritto dell'Unione europea. – 4. *Segue*: le sentenze *Eva Glawinschnig-Piesczek/Facebook* e *Schrems II*. – 5. Conclusioni: la legislazione europea come modello per una regolamentazione su scala globale dei diritti di Internet.

1. Considerazioni introduttive: il declinare della sovranità statale nel mondo di Internet e la difesa dei valori fondamentali dell'Unione europea.

La difficoltà nel rapporto tra le imprese multinazionali e gli Stati nazionali, considerata la tendenza di tali imprese a sottrarre *potere* agli Stati nei quali si trovano ad operare, tanto da rendere far ritenere che sia divenuto *obsoleto* lo stesso concetto di Stato nazionale[1], costituisce un dato incontrovertibile che ha oggigiorno assunto una rilevanza del tutto particolare nel c.d. ciberspazio. Il progressivo espandersi dei poteri privati ha finito così per condizionare pesantemente l'effettivo esercizio della stessa giurisdizione statale sul territorio, come tradizionalmente intesa. Con riferimento specifico al mondo digitale, che interessa in questa sede esaminare, si è sviluppato un nuovo ecosistema in cui si assiste, grazie, in particolare, al ricorso a procedure algoritmiche e all'uso dell'intelligenza artificiale[2], ad una progressiva erosione della sovranità[3] (in specie digitale) degli Stati a favore, da un lato, delle organizzazioni internazionali, tra cui, seppur con le sue connotazioni particolari[4], l'Unione europea, e, dall'altro, dei c.d. "baroni" del web, quali Amazon, Apple, Facebook, Google e Microsoft, che, in taluni casi, agiscono,

* Già Professore ordinario di Diritto dell'Unione europea, Università degli Studi di Milano. Il presente scritto è destinato ad essere pubblicato, con le opportune modifiche, nel *Liber amicorum* per Gian Luigi Cecchini.

[1] In tal senso già G.L. CECCHINI, *Gli Stati e le imprese multinazionali*, in *Annali della Facoltà di Scienze Politiche*, 1982, 313 ss., spec. 376.

[2] F. BASSAN, *Potere dell'algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi*, Catanzaro, 2019, p. 15.

[3] A conclusioni analoghe perviene, in una più ampia prospettiva di rapporti tra sovranità e democrazia, E. CANNIZZARO, *La sovranità oltre lo Stato*, Bologna, 2020, per il quale, «[l]ungo il percorso della storia, la sovranità ha quindi finito per smarrire la propria ragion d'essere», p. 65.

[4] «Ordinamento giuridico di nuovo genere nel campo del diritto internazionale», secondo Corte di giustizia, sentenza del 5 febbraio 1963, causa 26/62, *van Gend en Loos*, EU:C:1963:1.

o almeno aspirano a comportarsi, alla stregua di soggetti di diritto internazionale tradizionali.

L'influenza degli operatori tecnologici attivi su scala mondiale nel settore digitale ("*Big Tech*" o "*Tech Giants*")[5] è tale che si è addirittura ipotizzato, per evitare una assimilazione fra essi e gli Stati, che, in realtà, a fianco degli ordini nazionali e di quello internazionale propriamente inteso, si sia affermato, a livello intermedio, un ordine transnazionale, popolato da organizzazioni non governative e imprese multinazionali, in cui enti non statali, di natura privata, concorrono al processo di *international law making*[6]. In questo nuovo contesto, che, per certi versi, configura una sorta di neofeudalesimo digitale[7], in cui un sistema Stato-centrico non si presenta più come una struttura adeguata a garantire il rispetto di diritti e principi a tutela della dignità umana, la sfida tra i giganti di Internet, da un lato, e, principalmente, l'Unione europea e, con in parte diverse visioni, gli Stati Uniti[8], dall'altro, diviene quella sulle regole, in cui i valori si traducono, e il terreno di confronto assume una dimensione di ubiquità che prescinde da un determinato ambito territoriale, quando si tratti di affermare i diritti dell'uomo nella realtà di Internet. A fronteggiarsi sono dunque i signori del web e, per quanto ci riguarda, l'Unione europea, quale espressione di valori comuni e tendenzialmente universali, propri di quell'umanesimo che da tempo identifica il tessuto connettivo dell'Europa e che nasce dalla condivisione di ciò che è comune e supera ogni «identità di razza, nazione, classe,

[5] Sulla crescita del fenomeno «of global tech giants» e sul loro impatto sulla vita civile e democratica, vedi M. MOORE, *Tech Giants and Civic Power*, 2016, reperibile *online*.

[6] S. SASSI, *Crisi della sovranità e diritto transnazionale*, in *Percorsi costituzionali*, 2017, pp. 248-284, a p. 256 ss., e *Diritto Transnazionale e legittimazione democratica*, Padova, 2018, pp. 44 ss. e 57. Vedi anche A. BOSIO e S. DELLAVALLE, *Crisi e ridefinizione della sovranità nel contesto plurilivellare*, in *Costituzionalismo.it*, 2016, n. 3, reperibile *online*.

[7] A. VENANZONI, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *Medialaws*, 2020, n. 3, reperibile *online*, per il quale, «a fronte della sovranità esercitata sul territorio da parte degli Stati-nazione, i grandi attori della società digitale si comportano come vassalli crescenti nel potere e nella influenza: dominano il campo digitale, ove detengono la modellazione del codice, ma nel reale sono ancora almeno parzialmente sotto-ordinati». Godendo peraltro i soggetti egemoni nel digitale «di un vantaggio competitivo assoluto basato sui flussi di dati, informazioni, conoscenze e sulla essenzialità di molti servizi da loro prestati», non può escludersi che essi perdano «lo *status* di vassalli per divenire sovrani a tutti gli effetti». Il risultato sarebbe «un radicale ribaltamento prospettico, con gli Stati ridotti, in molti casi, al vassallaggio», p. 194. Vedi anche, sempre con riguardo alle implicazioni economiche e sociali nella società contemporanea di questa sorta di ritorno occulto a forme feudali di economia, E. BAZZANELLA, *Il feudalesimo digitale. I nuovi poteri nel nostro presente/futuro*, Trieste, 2020. Con riguardo ai pericoli che l'eccessivo potere delle grandi imprese digitali, ovvero «the darker side of the digital world», pone per la democrazia, vedi U. VON DER LEYEN, *Special Address by President von der Leyen at the Davos Agenda Week*, reperibile *online*, con riferimento, in particolare, al bando di Donald Trump da parte di Twitter e Facebook, dove le piattaforme si sono arrogate il diritto di giudicare, costituendo una sorta di propria giurisdizione privata.

[8] R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 61-84, che, con riferimento alla divergenza tra il modello europeo e quello statunitense, esprime l'auspicio che si avvii una fase di dialogo «tra le due sponde» basata su quei valori comunque condivisi, p. 83 s.

religione e genere»[9]. Così facendo l'Unione, sempre più determinata ad assumere, nella sua evoluzione tendenzialmente federale[10], i connotati dello Stato-civiltà[11], svolge, con riguardo alla tutela dei diritti fondamentali, o almeno aspirerebbe a svolgere, il ruolo di regolatore universale[12], destinato a entrare inevitabilmente in rotta di collisione con le imprese multinazionali, la cui ambizione è di essere *legibus solutae*. Due "sovranismi", l'uno economico, l'altro valoriale, finiscono per scontrarsi e a fare premio è, auspicabilmente, la legittimazione democratica dell'una rispetto alle altre, che consentirebbe alla sovranità fondata sui valori di prevalere su quella mossa da considerazioni meramente economiche. Ma questo potrebbe essere il lieto fine di una storia tutta ancora da scrivere e che ha come sfondo il riconoscimento e l'attuazione dei diritti dell'uomo anche in uno spazio liquido quale è il ciberspazio[13].

La questione dei valori fondanti è divenuta dunque centrale per il futuro della disciplina del *web*[14]. Da sempre, del resto, l'Unione europea si rispecchia nei propri valori

---

[9] M. GOLDSCHMIT, *Un'altra umanità, il soggetto dell'inconscio europeo*, in C. CAPPA, P. PAESANO, P. TERRACCIANO (a cura di), *La singolarità europea. L'umanesimo tra crisi e futuro*, Pisa, 2020, p. 9 ss., spec. p. 10.

[10] Ad imporre nel settore digitale un approccio "federativo" è la stessa struttura del mercato, con pochissime grandi aziende che fungono da porta di accesso. In Europa non esiste tuttavia un *player* di dimensioni assimilabili alla taglia dei colossi americano e cinesi e perciò, nella pratica impossibilità di far sorgere un campione europeo, la Commissione sta lavorando per dare vita, in sinergia con i paesi membri interessati, ad una realtà, Gaia-X, destinata a gestire servizi *cloud* con una infrastruttura federata ed interoperabile; il tutto al fine di garantire la sovranità tecnologica europea sui propri dati, mantenendo la capacità di processarli e di consentire al contempo all'Unione di divenire leader nell'infrastruttura *cloud*: vedi conclusioni del Consiglio, *Plasmare il futuro digitale dell'Europa*, 9 giugno 2020, doc. n. 8711/20, specie punto 17. In tale documento si conviene che «l'accelerazione della trasformazione digitale rappresenterà una componente essenziale della risposta UE alla crisi economica generata dalla pandemia Covid-19» (punto 3) e si sottolinea «l'importanza, nel contesto post-crisi, di proteggere e rafforzare la sovranità digitale nell'UE e la leadership nelle catene del valore digitali internazionali strategiche in quanto elementi chiave per garantire l'autonomia strategica, la competitività a livello mondiale e lo sviluppo sostenibile, promuovendo al contempo i valori comuni dell'UE, la trasparenza, i diritti umani e le libertà fondamentali sul piano internazionale» (punto 5).

[11] Secondo la classificazione di C. COKER, gli Stati-civiltà, contrapposti agli Stati-nazione, sono quelli che si attribuiscono una funzione di civilizzazione, essendo portatori di un modello tendenzialmente universale sul piano culturale e dei valori. In realtà, l'A. ritiene che l'Unione europea, in ragione delle fratture culturali e geografiche al suo interno, non sia ancora assurta a tale ruolo, riconosciuto invece, pur con diverse sfumature, a Cina, Russia e, forse, Stati Uniti: *Lo scontro degli Stati-civiltà*, Roma, 2020.

[12] Sarebbe tuttavia errato scorgere nell'approccio universalistico una suggestione olistica. L'azione dell'Unione europea, benché nasca dalla individuazione di valori che si riflettono in regole destinate in una certa misura alla collettività universale, persegue sempre e comunque finalità in ultima analisi di connotazione economica, in quanto volte ad assicurare nel campo digitale l'indipendenza necessaria per la sovranità dello stesso e per il suo sviluppo, nel rispetto – ed è questa la sostenibilità che contraddistingue tale azione e la rende del tutto peculiare – dei valori umani.

[13] Sulla dimensione a-territoriale dello spazio cibernetico, per tutti, G. SCACCIA, *Il territorio fra sovranità statale e globalizzazione dello spazio economico*, in *Rivista AIC*, 2017, n. 3, p. 17 ss., reperibile *online*. Come è stato rilevato «[l]o spazio cibernetico come lo spazio marino e lo spazio del nomade non può essere né occupato, né ripartito, ma è parte del nomos planetario, in quanto diventa la via dell'espansione culturale, commerciale ed economica e il luogo della competizione e della spartizione della terra»: così S. ORTINO, *Il nuovo Nomos della terra. Profili storici e sistematici dei nessi tra innovazioni tecnologiche, ordinamento spaziale, forma politica*, Bologna, 1999, p. 24.

[14] Si vedano al riguardo le conclusioni della riunione straordinaria del Consiglio europeo del 1° e 2 ottobre 2020, EUCO 13/20, dove vengono così riassunti i prossimi obiettivi dell'azione dell'Unione: «[p]er

del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e della tutela dei diritti umani[15], in relazione in specie alla protezione dei dati personali, che la identificano sul piano sia interno sia internazionale, nei rapporti innanzitutto con gli Stati terzi e ora anche con le imprese multinazionali che popolano Internet. Se la prima dimensione, quella interna e costituzionale, è oggetto di continua attenzione e la realizzazione progressiva di quei valori ha segnato il percorso di crescita sociale e politica dell'Unione, la seconda è invece di più difficile valutazione. Soprattutto, non è agevole tracciare dei criteri generali che guidino l'interprete nel comprendere l'ambito territoriale di applicazione di quelle disposizioni che, essendo l'espressione di tali valori[16], l'Unione ritiene fondanti, tanto da pretenderne, ai fini di una loro piena tutela, il rispetto innanzitutto dai paesi terzi e ora anche dai giganti del web con cui deve quotidianamente confrontarsi. In questo contesto l'art. 2 TUE non costituisce un'affermazione simbolica, ma una previsione giuridicamente vincolante in cui risiede il nocciolo duro dell'integrazione europea[17].

---

acquisire sovranità digitale, l'UE […] farà leva sui suoi strumenti e i suoi poteri normativi, per contribuire a definire norme e regole *globali* […]. Lo sviluppo digitale deve salvaguardare i nostri *valori* nonché i nostri *diritti fondamentali* e la nostra sicurezza ed essere socialmente equilibrato. Tale approccio *antropocentrico* aumenterà l'attrattività del *modello europeo*» (i corsivi sono nostri), p. 4.

[15] Vedi art. 2 TUE. Indicati come «principi», essi già comparivano nel Trattato di Amsterdam, per poi essere ampliati nel contenuto e "promossi" a «valori»: B. NASCIMBENE, *Valori comuni dell'Unione europea*, in E. TRIGGIANI, F. CHERUBINI, I. INGRAVALLO, E. NALIN, R. VIRZO (a cura di), *Dialoghi con Ugo Villani*, Bari, 2017, pp. 631-636. I valori «universali e inalienabili della persona umana» sono indicati nel Preambolo al TUE come motivi di ispirazione dell'Unione. Questi stessi valori sono richiamati nella comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final dell'8 aprile 2019, dove la Commissione delinea la strategia europea per l'intelligenza artificiale che si manifesta tramite l'innovazione digitale, nei suoi rapporti con i diritti della persona in tema di protezione dei dati personali. A tale strategia digitale sono dedicati i tre documenti presentati dalla Commissione il 19 febbraio 2020, rispettivamente le comunicazioni: *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final; *Una strategia europea per i dati*, COM(2020) 66 final; *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final. Infine, il 15 dicembre 2020 la Commissione ha presentato un pacchetto di misure volte ad aggiornare la disciplina del settore digitale, che includono due proposte di regolamento: il *Digital Services Act* (COM(2020) 825 final), destinato a regolare la sicurezza, la trasparenza e le condizioni di accesso ai servizi *online*, e il *Digital Markets Act* (COM(2020) 842 final), relativo agli aspetti commerciali e di concorrenza: G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di AISDUE*, III, 2021, reperibile *online*; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, *ivi*, 2021, reperibile *online*; G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, p. 262 ss.

[16] C. KUNER, *The Internet and the Global Reach of EU Law*, in M. CREMONA AND J. SCOTT (edited by), *EU Law Beyond EU Borders. The Extraterritorial Reach of EU Law*, Oxford, 2019, pp. 112-145, p. 120 ss.

[17] Vedi Corte di giustizia (seduta plenaria), parere 2/13 del 18 dicembre 2014, EU:C:2014:2454, punto 167: la struttura istituzionale dell'Unione «poggia sulla premessa fondamentale secondo cui ciascuno Stato membro condivide con tutti gli altri Stati membri, e riconosce che questi condividono, una serie di valori comuni sui quali l'Unione si fonda, così come precisato all'articolo 2 TUE. Questa premessa implica e giustifica l'esistenza della fiducia reciproca tra gli Stati membri quanto al riconoscimento di tali valori e, dunque, al rispetto del diritto dell'Unione che li attua».

La sfida è a tutto campo e se il *soft power*, inteso quale forza dell'esempio (c.d. effetto Brussels)[18], è lo strumento principale col quale l'Europa intende far prevalere i propri valori[19], l'efficacia extraterritoriale delle sue norme ne è il necessario corollario[20]. Il rischio diversamente è che al di fuori dei confini territoriali dell'Unione si impongano, con le loro regole, le imprese multinazionali che operano su scala globale. In tal caso l'Unione finirebbe per rinchiudersi in se stessa, rimanendo di fatto inerte di fronte a forze centripete che, dall'esterno, punterebbero ad accerchiare e quindi soffocare la sua sovranità digitale[21], privandola di autonomia strategica, ovvero di una capacità di azione che tuteli gli interessi e i valori propri dell'Unione stessa. Il timore è che alla supremazia dei valori non si accompagni però una pari forza politica dell'Unione nella comunità internazionale che assicuri il loro rispetto fra gli Stati, dando forma ad un "ordine mondiale migliore", la cui costruzione esprime per la Presidente della Commissione, Ursula von der Leyen, «la vocazione»[22] dell'Europa. In tal caso più che di un effetto Brussels si tratterebbe di una sorta di effetto Bisanzio[23], entità sovrana che, non potendo fare affidamento, per salvaguardare i propri "valori", su una sua forza politica e militare, doveva contare su altri mezzi, quelli diplomatici, soggetti al variare continuo dei rapporti fra le potenze.

---

[18] Con tale locuzione si riassume il caso, per certi versi unico nell'odierno panorama delle fonti, per cui il potere regolatorio di un singolo attore della *governance* mondiale, nella specie l'Unione europea, finisce per influenzare unilateralmente gli altri Stati, le organizzazioni internazionali e le forze del mercato: A. BRADFORD, *The Brussels Effect*, in *Northwestern University Law Review*, 2012, pp. 1-67, reperibile *online*; EAD., *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020; sul legame fra l'ambito di applicazione (territoriale) e l'effetto Brussels, vedi anche, per tutti, J. SCOTT, *The Global Reach of EU Law*, in M. CREMONA AND J. SCOTT (edited by), *EU Law Beyond EU Borders*, cit., pp. 21-63, p. 31 ss.

[19] Il ruolo di «global regulatory power» che l'Unione europea intende svolgere distinguerebbe ontologicamente l'efficacia extraterritoriale della normativa europea da quella propria delle norme statunitensi: J. SCOTT, *Extraterritoriality and Territorial Extension in EU Law*, in *American Journal of Comparative Law*, 2014, pp. 87-126, p. 89.

[20] In senso critico, A. NERVI, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 161-177, per il quale «un eccessivo divario tra la disciplina e la soglia di tutela vigenti nella "fortezza Europa" e quelle praticate nelle altre parti del mondo rischia di rendere più difficoltose le relazioni (non solo commerciali) tra il Vecchio Contenente ed il resto del mondo […]. In un mondo sempre più globalizzato, in cui però il peso politico ed economico dell'Europa sembra più declinare che crescere, la questione non può essere sottovalutata» (p. 173).

[21] Con sovranità digitale dell'Unione ci si riferisce «ad un contesto in cui i dati personali generati dalle attività digitali vengono "convertiti in valore" per le imprese e i cittadini europei ed elaborati in conformità con le garanzie riconosciute dall'ordinamento dell'Unione». La formula viene anche usata «per indicare la necessità di accrescere l'autonomia produttiva dell'Unione di materiale informatico-digitale, quali microprocessori (*chips*) e la capacità di costruire reti 5G e *cloud* europei»: G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza* Schrems II *della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, pp. 563-585, a p. 564 s. La sovranità digitale compare anche fra i "principi guida" del programma del semestre di presidenza tedesca del Consiglio dell'Unione europea: *Insieme. Per rilanciare l'Europa*, dal 1° luglio al 31 dicembre 2020.

[22] Discorso alla seduta plenaria del Parlamento europeo, 27 novembre 2019, p. 7.

[23] C. COKER, *Lo scontro degli Stati-civiltà*, cit., p. 114.

Per evitare tale destino e acquisire invece una sovranità non solo morale, ma anche politica, che della prima sia il necessario supporto, occorrerebbe una riforma istituzionale dell'Unione. L'attribuzione di ulteriori competenze all'Unione è divenuta infatti condizione imprescindibile per una sovranità effettiva, sulla scia della dichiarazione congiunta franco tedesca del 26 novembre 2019, che ha aperto la strada per la convocazione di una nuova Conferenza allo scopo di modificare i Trattati. Iniziativa quest'ultima fatta propria dalla Presidente della Commissione nel suo programma che prevedeva l'avvio della conferenza sul futuro dell'Europa per il 9 maggio 2020, in concomitanza con il 70° anniversario della Dichiarazione Schuman, e la sua conclusione nel 2022[24]. Al di là dell'inevitabile rinvio imposto dalla crisi pandemica dovuta alla diffusione del Covid-19[25], il momento pare comunque propizio per una svolta che prenda le mosse dall'esigenza di un rilancio in senso solidaristico[26] del rapporto fra gli Stati come effetto della crisi economica provocata dalla pandemia. Le difficoltà incontrate nella gestione della crisi hanno messo ancor di più a nudo le carenze nell'assetto di attribuzioni dei poteri dell'Unione e l'inadeguatezza degli attuali strumenti, tanto da ricorrere, con l'approvazione del piano *Next Generation EU*, ad un nuovo «modo di gestione delle crisi» in cui «la ripresa economica è percepita come un valore fondamentale per il funzionamento dell'intero mercato interno»[27]. Non si tratterebbe peraltro di un evento inatteso. Da tempo ormai l'Unione, senza clamori, quasi in punta di piedi, si sta muovendo nella direzione di creare un nuovo progetto di società, che comprenda una economia più verde e digitale. Riecheggiano al riguardo le parole di Jean Monnet nella sua autobiografia, ovvero: «[h]o sempre pensato che l'Europa si sarebbe fatta nelle crisi e che sarebbe stata la somma delle soluzioni che si sarebbero trovate per queste crisi»[28]. Tale osservazione si adatta perfettamente alla presente situazione in cui si pongono le premesse per un ulteriore progresso sulla strada dell'integrazione, senza grandi gesti, ma con fermezza. Il percorso di tale rivoluzione silenziosa non è agevole e i passi da compiere per stabilire la sovranità strategica dell'Unione, anche nel campo dei diritti digitali,

[24] *Un'Unione più ambiziosa. Il mio programma per l'Europa: orientamenti politici per la prossima Commissione europea 2019-2024*, Bruxelles, 2019.

[25] Vedi *Conference on the Future of Europe - Council position*, 24 June 2020, 9102/20: «the Conference should be launched as soon as the conditions allow in the light of the COVID-19 pandemic», p. 7. Il cammino è di fatto ripreso con una dichiarazione comune sulla Conferenza sul futuro dell'Europa, del 5 marzo 2021, firmata dal Presidente del Parlamento europeo, David Sassoli, dal Presidente del Consiglio dell'Unione, António Costa, e dalla Presidente della Commissione europea, Ursula von der Leyen (*Conference on the Future of Europe - Joint Declaration*, 5 March 2021, 6796/21). La Conferenza sul futuro dell'Europa ha preso, infine, il via il 9 maggio 2021.

[26] F. MOLITERNI, *Crisi pandemica economico-sanitaria, il fenomeno del "mondo piccolo" e il paradigma* "common safety, common benefit" *come modello giuridico e strumento euristico: considerazioni introduttive*, in *Studi sull'integrazione europea*, 2020, pp. 613-627, a p. 626; nonché, in generale, F. CROCI, *Solidarietà tra Stati membri dell'Unione europea e* governance *economica europea*, Torino, 2020.

[27] G. CONTALDI, *Il* Recovery Fund, in *Studi sull'integrazione europea*, 2020, pp. 587-612, spec. p. 610.

[28] *Cittadino d'Europa. 75 anni di storia mondiale*, Milano, 1978, p. 311.

implicano scelte di più ampio respiro che non solo superano i confini dell'Unione stessa, ma mettono in gioco gli attuali assetti istituzionali.

La prima considerazione è che i diritti umani, laddove internazionalmente riconosciuti, come manifestazione della dignità umana nella sua dimensione di valore individuale, hanno, per loro natura, una connotazione di universalità, che prescinde, per la loro affermazione, dalla sovranità domestica. La seconda è che la loro applicazione senza confini può essere promossa dagli Stati, e ora dall'Unione, vuoi per tutelare propri interessi vuoi soprattutto per favorire la diffusione stessa di tali diritti[29].

Fin qui *nulla quaestio*. Il problema si pone invece per quei diritti, pure riconducibili ai diritti umani in senso lato, che, riconosciuti come fondamentali dall'Unione europea, non hanno però ad oggi una loro codificazione nel diritto internazionale consuetudinario e non sono stati neppure, o forse solo in parte, positivizzati in strumenti internazionali. Ciò non di meno tali diritti, intrecciati con le forme di rispettiva tutela, sono rispettivamente la trama e l'ordito del tessuto connettivo dell'Unione in una prospettiva tendenzialmente universale. Ci si riferisce a quell'insieme di valori propri dell'Unione che, individuati nel già ricordato art. 2 TUE, costituiscono il «"collante" che lega indissolubilmente in un progetto strategico comune Paesi che, pur dotati di storia e cultura diversi, hanno deciso di interpretare tali differenze come "valori" unificanti ben sintetizzati nel motto "Unità nella diversità"»[30].

Se è vero dunque che i valori hanno una valenza sensibilmente politica[31], lo è anche che, «nella misura in cui i suddetti valori corrispondono ai principi generali del diritto» dell'Unione[32], essi costituiscono una fonte di quel diritto e come tali, da un lato, sono applicabili dalla Corte di giustizia quale parametro di legittimità degli atti dell'Unione[33] e, dall'altro, in virtù della loro obbligatorietà, operano nei confronti degli Stati membri con efficacia diretta al loro interno, anche nei rapporti tra privati[34].

Sulla rilevanza nel sistema unionale di tali diritti non occorre soffermarsi ulteriormente. Va solo aggiunto che, se l'articolo 2 TUE, assumendo sotto questo profilo una valenza costituzionale[35], identifica, come già osservato, tali valori, il successivo articolo 3 indica fra gli obiettivi della stessa Unione quello di promuovere, per l'appunto,

---

[29] Nel senso che la proliferazione delle reti globali e di Internet possa rappresentare uno strumento di diffusione, in generale, dei valori democratici, A.L. VALVO, *Diritti umani e realtà virtuale. Normativa europea e internazionale*, Mestre, 2013, p. 102.

[30] E. TRIGGIANI, *Spunti e riflessioni sull'Europa*, 2ª ed., Bari, 2019, p. 23.

[31] U. VILLANI, *Istituzioni di diritto dell'Unione europea*, 6ª ed., Bari, 2020, p. 37.

[32] *Ibid.*

[33] *Ivi.*, p. 279.

[34] *Ivi.*, p. 279 s. Vedi, in generale, C. PERARO, *Diritti fondamentali sociali e tutela collettiva nell'Unione europea*, Napoli, 2020.

[35] L.S. ROSSI, *Il valore giuridico dei valori. L'Articolo 2 TUE: relazioni con altre disposizioni del diritto primario dell'UE e rimedi giurisdizionali*, in *federalismi.it*, 2020, reperibile *online*, per la quale «si può ritenere che, in quanto espressione dei principi fondanti e dei valori supremi dell'Unione, l'articolo 2 TUE si collochi a livello superiore rispetto a tutte le altre norme dei trattati» (v) e che pertanto esso possa «senza dubbio essere qualificato come principio costituzionale dell'Unione europea» (vi).

«i suoi valori», informando in tal senso, secondo quanto stabilito all'art. 21 TUE, la propria azione sul piano internazionale. Azione che è volta ad affermare e tutelare «nel resto del mondo» quegli stessi principi, quali i diritti dell'uomo e il rispetto della dignità umana, che sono espressione di quell'umanesimo europeo che è stato alla base della sua creazione, sviluppo e allargamento ed è oggi la cifra della sua singolarità[36] nel contesto mondiale. Singolarità che dal piano ideale si trasferisce su quello sostanziale in virtù dei caratteri preminenti nell'ordinamento europeo, come il primato rispetto al diritto interno e l'effetto diretto che consente alle norme europee di creare diritti che i singoli possono vantare nei confronti dei giudici nazionali anche con riguardo – ed è questa la novità – a fattispecie non esclusivamente interne all'Unione.

Il primo ambito in cui tali valori sono affermati è naturalmente quello interno[37], che però si rivela talvolta insufficiente per fornire un'adeguata tutela, tanto da indurre a ricercare in questi casi una diversa soluzione, soprattutto attraverso l'adozione di norme il cui ambito sia il più esteso possibile, anche al di fuori dei confini territoriali dell'Unione, ogniqualvolta sussista un possibile nesso che lo giustifichi[38]. Spesso accompagnata da affermazioni circa una valenza "mondiale", e comunque tendenzialmente senza limiti, di tali regole, l'introduzione di una disciplina siffatta non ha evidentemente nulla di "universale", non facendo parte i relativi precetti di un *corpus* normativo vincolante per gli Stati estranei all'Unione, bensì appartiene alla tipologia ben nota delle norme aventi efficacia extraterritoriale.

L'efficacia extraterritoriale delle norme dell'Unione, seppure eccezionalmente, costituisce una possibile connotazione del diritto derivato europeo[39]. Diviene perciò inevitabile chiedersi quale sia il nesso tra tale efficacia eccezionale e la dimensione valoriale che si intende proteggere. In realtà, la prassi esaminata dimostra che, al di là delle affermazioni di principio, le ragioni del ricorso a tale strumento possono essere le più varie. Talvolta esse sono rinvenibili nella necessità di assicurare la piena efficacia di norme poste a protezione di interessi, spesso economici, come nel caso delle norme sulla concorrenza, e comunque non facilmente riconducibili ai menzionati valori

[36] C. CAPPA, P. PAESANO, P. TERRACCIANO (a cura di), *La singolarità europea. L'umanesimo tra crisi e futuro*, cit.

[37] Sul mercato unico digitale, che rappresenta una delle realizzazioni di maggiore successo dell'integrazione europea, vedi G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, 2020, pp. 13-49, reperibile *online*.

[38] In generale, vedi M.C. MENEGHETTI, *The Different Shapes of Extraterritoriality in EU Data Protection Law and its International Justifications*, in *Diritto del commercio internazionale*, 2019, pp. 695-733.

[39] In generale, P. DE PASQUALE, *L'applicazione extraterritoriale dei divieti* antitrust, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, 2ª ed., Padova, 2020, pp. 201-211, oltre ai contributi in M. CREMONA AND J. SCOTT (edited by), *EU Law Beyond EU Borders. The Extraterritorial Reach of EU Law*, cit.

dell'Unione[40], mentre, altre volte, come nel caso delle disposizioni sulla protezione dei dati (personali), esse si giustificano con l'esigenza di salvaguardare tali valori ovunque vengano in gioco. Il problema, in realtà, si pone con riguardo ai principi contenuti nella Carta e alla loro possibile applicazione a soggetti (e territori) non appartenenti all'Unione, in assenza di una specifica normativa di attuazione. In merito occorre premettere che, come noto, di regola l'ambito di applicazione della Carta è nei limiti del diritto dell'Unione. Ne consegue che, «quando la regola dell'Unione applicabile alla fattispecie produce effetti al di fuori del territorio degli stati membri, anche la Carta si applicherà *extra*-territorialmente»[41]. Ovviamente, tuttavia, laddove la disposizione della Carta sia di per sé, come nel caso del principio di non discriminazione, dotata, in via eccezionale, di efficacia diretta, non occorre, perché essa produca effetti al di fuori del territorio dell'Unione, che il legislatore europeo sia intervenuto a disciplinare la materia. Si tratterà piuttosto di valutare la compatibilità di tale applicazione extraterritoriale della Carta alla luce dell'articolo 52, par. 3 della stessa, che con riguardo alle sue disposizioni che enunciano diritti fondamentali già garantiti dal sistema CEDU pone l'obbligo di una interpretazione parallela del significato e del portato dei diritti previsti dai due ordini di norme. Viene così in considerazione il disposto dell'articolo 1 della CEDU che stabilisce in merito alla necessaria applicazione parallela del portato dei due ordini di norme, propendendo peraltro la Corte di giustizia per una interpretazione che non tenga conto della limitazione desumibile dalla CEDU stessa[42].

L'efficacia extraterritoriale è espressione, dunque, della *vis* espansiva dei valori e dei diritti fondamentali dell'Unione. Del resto, quale sia la posizione dell'Unione in merito alla possibile applicazione extraterritoriale del diritto europeo è chiaramente desumibile dalla giurisprudenza della Corte di giustizia che ha più volte espressamente riconosciuto che talune sue norme, sulla concorrenza e in tema, ad esempio, di ambiente, possono avere un'applicazione extraterritoriale[43]. Lo stesso è avvenuto, a maggior ragione, per i nuovi diritti digitali, tra cui quelli relativi ai dati personali. In merito poi

---

[40] Unitamente alle norme in materia di concorrenza ed ambiente, rimangono parimenti estranee all'ambito della nostra indagine le questioni poste, dal punto di vista del diritto internazionale privato, da criteri di collegamento esorbitanti, che allarghino a dismisura la competenza giurisdizionale dei giudici dei paesi membri nei riguardi di fattispecie prevalentemente estranee al territorio dell'Unione. In merito, vedi, per tutti, F. RAGNO, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del* private enforcement *del GDPR*, in *Ordine internazionale e diritti umani*, 2020, pp. 818-838, reperibile *online*; B. HESS, *Protecting Privacy by Cross Border Injunction*, in *Rivista di diritto internazionale privato e processuale*, 2019, pp. 284-301; M.C. MENEGHETTI, *The Different Shapes of Extraterritoriality*, cit.; A. BARLETTA, *La tutela effettiva della* privacy *nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di internet*, in *Europa e diritto privato*, 2017, pp. 1179-1214; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis"*, in *Cuadernos de Derecho Transnacional*, 2017, pp. 448-464, reperibile *online*.

[41] N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Milano, 2018, p. 175, anche in relazione alla CEDU.

[42] *Ivi*, p. 178.

[43] *Ivi*, p. 176.

alla compatibilità di tale pretesa di applicazione al di fuori del territorio dell'Unione con il diritto consuetudinario, valgono ad illustrare la posizione unionale le conclusioni dell'Avvocato generale Jääskinen, nel 2014, nella causa *Regno Unito* c. *Parlamento e Consiglio*[44], non giunta peraltro a sentenza per rinuncia agli atti da parte del Regno Unito[45]. Il Governo britannico aveva infatti sostenuto che l'art. 94, par. 1, lett. g) della direttiva CRD IV[46] violasse il principio consuetudinario di diritto internazionale pubblico relativo alla territorialità (*comitas gentium*), che impone agli Stati di non legiferare in relazione al comportamento di cittadini stabiliti in un altro Stato in assenza di una connessione adeguata che lo consenta[47]. L'Avvocato generale ricorda, anzitutto, che, per giurisprudenza consolidata[48], non vi è dubbio sul fatto che un comportamento avente luogo al di fuori dell'Unione che ha un impatto al suo interno possa essere disciplinato dal diritto dell'Unione. A ciò si aggiunge che il diritto internazionale non contiene alcun divieto generale di estensione della competenza di uno Stato ad emanare norme oltre il proprio territorio[49], essendo invece richiesto che lo Stato possa invocare una «connessione sufficiente»[50]. Diverso sarebbe il caso se si trattasse in effetti di una «rivendicazione di giurisdizione universale», in assenza di collegamenti con l'esercizio della competenza legislativa, che dovrebbe essere invece fondata su una norma positiva di diritto internazionale[51]. In conclusione, nei limiti così tracciati, l'extraterritorialità è non solo ammessa dal diritto dell'Unione, ma anche compatibile col diritto internazionale consuetudinario.

Va da sé che la scelta di attribuire una efficacia extraterritoriale può essere influenzata, come già osservato, da molteplici fattori, oggetto di un necessario bilanciamento. Di certo l'esigenza di affermare la tutela dei valori inalienabili e inviolabili della persona umana, affermati nel Preambolo al TUE, può costituire un valido motivo per attribuire alle relative disposizioni una siffatta efficacia se, come ricordato

[44] Avvocato generale Jääskinen, conclusioni del 20 novembre 2014, causa C-507/13, EU:C:2014:2394.

[45] Corte di giustizia, ordinanza del 9 dicembre 2014, causa C-507/13, EU:C:2014:2481, ai sensi dell'art. 148 del regolamento di procedura.

[46] Il c.d. "Pacchetto CRD IV" consiste in una direttiva sui requisiti patrimoniali, la direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE, e in un regolamento sui requisiti patrimoniali, il regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012.

[47] Conclusioni Avvocato generale Jääskinen, *Regno Unito* c. *Parlamento e Consiglio*, cit., punto 26.

[48] L' Avvocato generale ricorda al riguardo che, per giurisprudenza costante, «si è da tempo stabilito che un comportamento avente luogo al di fuori dell'Unione che ha un impatto al suo interno può essere disciplinato dal diritto dell'Unione»: *ivi*, punto 36, anche per i riferimenti giurisprudenziali.

[49] Come ricorda l'Avvocato generale, *ivi*, punto 37, depone in tal senso la sentenza della Corte permanente di giustizia internazionale del 7 settembre 1927 nella causa *Lotus (Francia/Turchia)*, in *Raccolta CPGI*, serie A, n. 10, 25 ss.

[50] Conclusioni Avvocato generale Jääskinen, *Regno Unito* c. *Parlamento e Consiglio*, cit., punto 38.

[51] *Ivi*, punto 39.

dall'Avvocato generale Mengozzi nella causa *X. e X.*, detti «valori devono avere un senso, concretizzarsi e guidare l'applicazione del diritto dell'Unione quando quest'ultimo presenta le condizioni per onorarli»[52]. Proprio in quel caso, tuttavia, la Corte ritenne che altre considerazioni d'ordine *lato sensu* "politico" dovessero prevalere. I giudici del Lussemburgo hanno perciò preferito non esprimersi sulle considerazioni svolte dall'Avvocato generale, limitandosi ad affermare che la questione oggetto di esame esulava dall'ambito di applicazione del diritto dell'Unione rientrando invece in quello del diritto nazionale[53]. Ad essere avallata è stata quindi «una percezione di un diritto che trova applicazione solamente nell'ambito dei confini spaziali europei»[54], ben lontana da ogni aspirazione universalistica, quasi che la tutela dei valori possa dipendere dalla significatività politica degli interessi in gioco.

2. I nuovi diritti digitali e il loro ambito di applicazione.

La questione dell'applicazione extraterritoriale delle norme dell'Unione è divenuta di estrema attualità con l'affermazione dei nuovi diritti digitali[55], per loro natura indifferenti alle limitazioni territoriali e oggi riconosciuti quali diritti fondamentali costitutivi dell'identità digitale. Quest'ultima assume due diverse accezioni, indicando, per un verso, l'identità "in rete" o "virtuale", e, per un altro, l'insieme delle informazioni reperibili in rete nei riguardi del soggetto interessato[56]. In una visione antropocentrica, propria della strategia europea nei confronti anche dell'ambiente digitale[57] nelle sue molteplici manifestazioni, l'identità digitale risponde ad una possibile declinazione dell'identità personale[58] nella nuova dimensione diacronica di Internet, divenendo tale

[52] Avvocato generale Mengozzi, conclusioni del 7 febbraio 2017, causa C-638/16 PPU, *X. e X.* c. *État belge*, EU:C:2017:93, punto 165.

[53] Corte di giustizia, sentenza del 7 marzo 2017, causa C-638/16 PPU, *X. e X.* c. *État belge*, EU:C:2017:173, punto 51.

[54] A. DEL GUERCIO, *La sentenza X. e X. della Corte di giustizia sul rilascio del visto umanitario: analisi critica di un'occasione persa*, in *European Papers*, 2017, pp. 271-291, reperibile *online*.

[55] M. MENSI, *La rete fra tecnologia e diritto*, in M. MENSI, P. FALLETTA, *Il diritto del web*, 2ª ed., Vicenza, 2018, pp. 1-59, spec. p. 30.

[56] G. RESTA, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 2017, pp. 511-531, p. 514 s.

[57] Si vedano, anche, da ultimo, conclusioni del Consiglio dell'Unione europea, *Plasmare il futuro digitale dell'Europa*, 9 giugno 2020, cit., punto 11.

[58] R. CAFARI PANICO, *L'identità digitale quale diritto del cittadino dell'Unione, fra tutela dei dati personali e concorrenza*, in AA.VV., *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, Bari, 2019, pp. 815-840, a p. 819 s., reperibile *online*. Vedi anche G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, pp. 11-33, spec. p. 16.

identità variabile nello spazio e nel tempo[59], come dimostrano il diritto all'oblio[60] e la c.d. successione digitale[61].

Sul piano spaziale, la nuova realtà, definita ciberspazio, o semplicemente rete, si articola in tre dimensioni, interna, europea e internazionale, con una vocazione ad evolvere in un possibile ordinamento universale o globale, dotato di una illimitata capacità di espansione nello spazio.

In questo spazio cibernetico, al centro di una realtà giuridica virtuale, dove chi opera viene identificato attraverso i suoi dati[62], da un lato, si è imposta la nozione di identità digitale come diritto fondamentale della persona ed elemento costitutivo della sua identità (personale), che si scompone in una varietà di situazioni giuridiche singolarmente tutelate; dall'altro, si è anche materializzato un sistema nuovo ed originale di tutela di tali diritti in un mondo virtuale, senza confini e che prescinde dall'appartenenza ad un determinato territorio.

La tutela del diritto all'identità (anche digitale) di una persona, nell'ambito del diritto al rispetto della vita privata, trova specifico fondamento nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea[63], in quanto i dati di carattere personale rappresentano un bene giuridico attraverso il quale le istituzioni tutelano l'identità della persona. Il riconoscimento del diritto alla protezione dei dati personali, come diritto

---

[59] Nel senso che la rivoluzione tecnologica di Internet abbia modificato le stesse «nozioni di spazio e di tempo», G. SCACCIA, *Il territorio fra sovranità statale e globalizzazione*, cit., p. 17.

[60] *Ex multis*, G. CIRILLO, *La deindicizzazione dai motori di ricerca tra diritto all'oblio e identità personale*, in *Nuova giurisprudenza civile commentata*, 2020, pp. 1235-1248; A. SPATUZZI, *Diritto all'oblio e revocazione storica. Il bilanciamento delle Sezioni Unite*, in *Il Diritto di famiglia e delle persone*, 2020, pp. 1260-1269; M.G. STANZIONE, *Libertà di espressione e diritto alla privacy nel dialogo delle corti. Il caso del diritto all'oblio*, in *Europa e diritto privato*, 2020, pp. 991-1004; V. CUFFARO, *Cancellare i dati personale. Dalla* damnatio memoriae *al diritto all'oblio*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati*, cit., pp. 219-236; F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 353-395; F. ZORZI GIUSTINIANI, *Il diritto all'oblio nella rete e i suoi limiti nell'attuale contesto europeo*, in AA.VV., *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, cit., pp. 919-929, reperibile *online*; A. VESTO, *La tutela dell'oblio tra intimità e condivisione senza filtri*, in *Medialaws*, 2018, n. 2, pp. 105-118, reperibile online; M. TAMPIERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Responsabilità civile e previdenza*, 2017, pp. 1010-1031; M.L. DAGA, *Diritto all'oblio: tra diritto alla riservatezza e diritto all'identità personale*, in *Danno e responsabilità*, 2014, pp. 274-278.

[61] G. MARINO, *La successione digitale*, in *Osservatorio del diritto civile e commerciale*, 2018, pp. 167-204; A. MAGNANI, *L'eredità digitale*, in *Notariato*, 2014, pp. 519-532.; G. RESTA, *La 'morte digitale'*, in *Diritto dell'informazione e dell'informatica*, 2014, pp. 891-920; M. CINQUE, *La successione nel "patrimonio digitale": prime considerazioni*, in *Nuova giurisprudenza civile commentata*, 2012, pp. 645-655.

[62] Sulla nozione di «dati» personali, nella loro dimensione sia morale sia economica, vedi, anche per ulteriori riferimenti, C. PERLINGIERI, *Data as the Object of a Contract and Contract Epistemology*, in *Italian Law Journal*, 2019, pp. 613-629, a p. 613 ss., reperibile *online*.

[63] «Il rispetto del diritto alla vita privata per quanto attiene al trattamento dei dati personali, riconosciuto dagli articoli 7 e 8 della Carta, è riferito a ogni informazione relativa a una persona fisica identifica o identificabile»: così Corte di giustizia, sentenza del 3 ottobre 2019, causa C-70/18, *Staatssecretaris van Justitie*, ECLI:EU:C:2019:823, punto 54, dove si specifica che «le impronte digitali e l'immagine facciale di una persona fisica» (punto 55) rientrano nella nozione di identità digitale.

fondamentale della persona, compare oggi sia nell'art. 6 TUE sia nell'art. 16 TFUE, che ricollega il diritto all'identità della persona alla protezione dei dati di carattere personale che lo riguardano. Tale protezione si declina in singoli diritti tra cui un rilievo particolare assumono quello alla riservatezza dei dati ed il corrispondente diritto all'oblio.

Quest'ultimo diritto, inteso in particolare nel suo significato di diritto alla deindicizzazione[64] dei propri dati personali da un motore di ricerca, non espressamente previsto né dalla legislazione ordinaria né da quella costituzionale, è stato dunque qualificato come una particolare declinazione della tutela dell'identità personale, ovvero come espressione del «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata»[65].

L'aspetto più rivoluzionario di Internet è sicuramente che le notizie diffuse in questo ambito abbiano natura ubiquitaria[66], il che, se presenta un indubbio vantaggio per i suoi utilizzatori, al contempo comporta rischi finora inesplorati per i titolari dei dati elaborati dai motori di ricerca quando essi riguardano la vita privata di tali persone.

Se, pur con fatica, il legislatore europeo e la giurisprudenza hanno elaborato strumenti per la protezione dei dati personali, individuando nel diritto all'oblio, o meglio, nella sua versione del diritto alla deindicizzazione, lo strumento al momento idoneo a conseguire il risultato perseguito, non altrettanto può dirsi per l'ambito di applicazione geografico della tutela così predisposta, ovvero se la deindicizzazione debba riguardare tutti i nomi di dominio di riferimento, oppure solo i nomi di dominio nazionali, o europei. È di immediata evidenza l'intrinseca contraddittorietà di una indagine volta ad accertare i confini fisici di uno spazio per sua natura globale ed universale come Internet. Di qui anche la difficoltà di formulare in termini relativi, ovvero specifici di un determinato sistema giuridico, una regola comportamentale per sua natura astratta. Non stupisce quindi che nella stessa giurisprudenza della Corte di giustizia si rinvengano riferimenti alla connotazione tendenzialmente universalistica della protezione dei dati personali, salvo poi ricondurre, a esito di una più matura riflessione, il problema entro le ben note

[64] Con il termine «deindicizzazione» si indica il procedimento messo in pratica dai motori di ricerca per permettere la rimozione di contenuti e informazioni che sono frutto del risultato di una ricerca nel web. In particolare, si tratta di una rimozione non propriamente dei contenuti presenti in rete, dei *link*, legati al singolo nominativo, ma della loro visibilità all'interno dei risultati ottenuti dai motori di ricerca.

[65] Così Corte di cassazione, sentenza del 9 aprile 1998, n. 3679; vedi anche, *ex multis*, Corte di cassazione, sentenza del 5 aprile 2012, n. 5525. Sul confine tra diritto all'oblio e diritto d'informazione, vedi Corte di cassazione, sezioni unite, sentenza del 22 luglio 2019, n. 19681: per un commento, M.C. PERCHINUNNO, *Identità personale, identità digitale e diritto di cronaca*, in *Contratto e impresa*, 2020, pp. 1430-1446. Sempre nel senso che il diritto alla protezione dei dati personali vada inteso come diritto al potere dell'interessato di controllare i propri dati consapevolmente, secondo il principio dell'autodeterminazione informativa, con uno spazio concettuale e operativo distinto dal diritto alla riservatezza, che si collega invece alla tutela dell'intimità della propria vita contro ingerenze esterne, Corte di cassazione, sentenza del 27 marzo 2020, n. 7559.

[66] G. BEVILACQUA, *La dimensione territoriale dell'oblio in uno spazio globale e universale*, in *federalismi.it*, 18 dicembre 2019, p. 3, reperibile *online*.

categorie degli effetti extraterritoriali. Non sorprende neppure lo stupore che si manifesta allorquando si tratta di giustificare, utilizzando categorie proprie del diritto pubblico[67], di massima, soggetto ad una applicazione rigorosamente territoriale[68], la tendenza all'esercizio dei poteri (sovrani) di giurisdizione, e quindi di controllo anche al di là dei tradizionali confini geografici del singolo Stato e dell'Unione nel suo complesso.

Nel caso specifico dell'identità digitale, ogni riferimento ai valori universali sarebbe dunque fuorviante se non addirittura errato. Valori universali sono infatti quelli relativi ai diritti umani comuni agli Stati e riconosciuti dalla comunità internazionale mediante il diritto consuetudinario o atti pattizi.

Diversa è la situazione nel caso dei diritti digitali, dove tale riconoscimento da parte del diritto internazionale, anche convenzionale, è assente o comunque limitato per numero di Stati[69]. In questo caso occorre perciò distinguere, da un lato, la portata della diffusione dei dati, che, unita alla ubiquità dei dati stessi e dei contenuti messi in rete su un sito Internet, è in linea di principio universale[70], e, dall'altro, l'ambito di intervento del legislatore europeo, che può estendersi, entro il limite della sufficiente connessione, anche in ambito extraterritoriale. Dopo di che si tratta di chiarire la natura dell'applicazione delle regole dell'Unione anche a fattispecie che si realizzano al di fuori dei confini geografici della stessa Unione, in una duplice prospettiva, ovvero come esercizio del potere sovrano attribuito al legislatore europeo dagli Stati membri, oppure come adeguamento, unilaterale ed autonomo, da parte degli Stati terzi al dettato di dette regole; in entrambi i casi siamo evidentemente al di fuori della nozione di applicazione universale di un diritto quale risultato della vigenza di una norma di diritto internazionale, qualsivoglia sia la sua natura. In realtà a creare l'equivoco è la nozione stessa di Internet quale spazio "liquido", aperto e globale, in cui gli Stati sovrani non avrebbero mai potuto esercitare la loro giurisdizione, tanto da richiamare la teoria della libertà dei mari[71]. Ma, come in quel caso, anche nel mondo virtuale gli Stati sono intervenuti per rivendicare il proprio controllo, entro limiti e con modalità ancora incerti e che rimangono da definire,

---

[67] 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*, 16 ottobre 2019, reperibile *online*.

[68] S. CARREA, *La cooperazione transfrontaliera e il principio di applicazione territoriale del diritto*, in A. DI STEFANO (a cura di), *Un diritto senza terra? Funzioni e limiti del principio di territorialità nel diritto internazionale e dell'Unione europea*, Torino, 2015, pp. 325-339, a p. 329 s.

[69] V. art. 8 CEDU sulla protezione dei dati personali. Per la sua applicazione riferita allo *cyberspace*, S. CARREA, *The ECHR in the Cyberspace: Does the Power to Infringe Always Entail the Duty to Protect?*, in *Diritti umani e diritto internazionale*, 2019, pp. 133-153. In merito alla auspicabile coerenza fra i diversi strumenti del sistema di Strasburgo e di quello di Bruxelles, vedi B. VAN DER SLOOT, *Legal consistency after the General Data Protection Regulation and the Police Directive*, in *European Journal of Law and Technology*, 2018, n. 3, reperibile *online*.

[70] Corte di giustizia, sentenza del 17 ottobre 2017, causa C-194/16, *Bolagsupplysningen OÜ*, EU:C:2017:766, punto 48, anche con riguardo ai diritti della personalità di cui è titolare una persona giuridica.

[71] G. BEVILACQUA, *La dimensione territoriale dell'oblio*, cit., p. 17.

specie alla luce del fatto che, in tema di diritti umani, è comune l'accettazione della possibilità di esercizio della relativa tutela in un ambito non necessariamente ristretto a quello territoriale dello Stato. Sotto questo profilo, è stata «utile»[72] la sentenza *Schrems*[73] con cui la Corte di giustizia (Grande Sezione), riaffermando l'attitudine extraterritoriale della normativa europea in materia di protezione dei dati[74], ha scartato una certa idea di a-territorialità del mondo di Internet, quando invece anch'esso è soggetto ad una progressiva espansione dell'intervento statale[75], inevitabile quando si tratti di violazioni dei diritti fondamentali, la cui tutela è insensibile alle frontiere territoriali. Indicazioni circa le potenzialità espansive della disciplina della protezione dei dati personali potevano già trarsi dalla sentenza della Corte di giustizia nel caso *Bodit Lindqvist*, del 6 novembre 2003, dove la Corte ha ritenuto, «a proposito della direttiva 95/46, fondata sull'art. 100 A, che il ricorso a questo fondamento giuridico non presuppone l'esistenza di un nesso effettivo con la libera circolazione tra Stati membri in ciascuna delle situazioni previste dall'atto fondato su tale base»[76].

La conseguenza è che quando la questione della circolazione e della sicurezza dei dati personali si è riproposta in occasione della pandemia causata dal Coronavirus, essa è stata affrontata negli stessi termini, e pertanto, con riguardo all'applicazione del GDPR, «the relevant considerations with regard to adequacy decisions are not whether third country measures involve data transfer from the EU, but rather what is the level of data protecion in the third country and what are the impact of such measures on data subjects»[77]. Ad essere rilevanti non sono dunque le modalità o le circostanze in cui si realizza il trasferimento dei dati, ma il livello, adeguato o meno, di protezione riservato ai (titolari dei) dati stessi nel paese terzo interessato.

Occorrerebbe piuttosto chiedersi, a questo punto, se i diritti digitali non trovino già ora il proprio fondamento in quel diritto transnazionale cui si è fatto cenno inizialmente,

---

[72] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso* Schrems: *la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016, pp. 7-22, spec. p. 10, reperibile *online*.

[73] Corte di giustizia (Grande Sezione), sentenza del 6 ottobre 2015, causa C-362/14, *Maximilian Schrems* c. *Data Protection Officer*, EU:C:2015:650, nota come *Schrems I*.

[74] L'ambito di applicazione oggettivo era stato peraltro già esteso in via interpretativa con la sentenza del 13 maggio 2014, causa C-131/12, *Google Spain*, EU:C:2014:317, che «ha proposto una lettura a compasso della clausola di giurisdizione iscritta nell'art. 4 della direttiva 95/46/CE», in modo da ampliare «il perimetro di operatività della disciplina europea in materia di protezione dei dati personali», tanto «da far parlare di una vera e propria applicazione extra-territoriale della normativa comunitaria»: G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali*, cit., pp. 23-48, spec. p. 40, reperibile *online*.

[75] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso* Schrems, cit., p. 10.

[76] Corte di giustizia, sentenza del 6 novembre 2003, causa C-101/01, *Bodil Lindqvist*, EU:C:2003:596, punto 40. V. anche Corte di giustizia, sentenza del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk*, EU:C:2003:294, punti 41-43.

[77] C. DOCKSEY, C. KUNER, *The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers*, in *European Law Blog*, 3 aprile 2020, reperibile *online*.

ovvero in una specifica declinazione della *lex mercatoria* il cui contenuto precettivo rappresenterebbe il reale termine di raffronto per i singoli Stati sia sul piano della tutela sia per i limiti dell'esercizio della potestà legislativa e giurisdizionale. La risposta è negativa, ma l'aver anche solo posto la domanda ha sollevato il velo su quanto, come avremo modo di osservare a conclusione di questa indagine, sta accadendo sul piano transnazionale.

In astratto, una applicazione extraterritoriale delle norme poste a protezione dei diritti di cui all'identità digitale potrebbe dunque trovare giustificazione nell'attuale disciplina internazionale dei diritti dell'uomo (art. 2 Patto e 1 CEDU), sempre che all'esercizio di tale giurisdizione si accompagni un corrispondente obbligo di tutela del diritto al rispetto della vita privata[78]. Ovviamente questa soluzione richiederebbe l'accertamento di una nozione comune relativa al contenuto del generico diritto al rispetto della vita privata, che viene declinato, o ancor prima riconosciuto, in maniera differente nella comunità internazionale. L'assenza di un diritto universalmente riconosciuto impedisce allo stato il parallelismo tra esercizio del potere sovrano e obbligo del rispetto del diritto nella sua accezione internazionalmente accolta. È vero invece che solo il *self restraint* di ciascuno Stato può evitare che l'esercizio esorbitante dei poteri di controllo determini l'insorgere di veri e propri conflitti fra le diverse giurisdizioni. Di qui la prudenza usata dalla Corte di giustizia quando, in più occasioni, si è confrontata con la questione dell'ambito di tutela del diritto all'oblio, anche se di certo in questo modo, "quando la deindicizzazione non è globale" l'effetto utile del diritto all'oblio non "si produce"[79].

3. La giurisprudenza della Corte di giustizia: l'efficacia extraterritoriale del diritto dell'Unione europea.

La Corte di giustizia ha avuto modo di pronunciarsi per la prima volta sul diritto all'oblio nella causa *Google Spain*[80]. La nostra narrazione inizia dunque nel 2014, quando la Corte di giustizia riconosce detto diritto, senza però precisarne i confini, prosegue con la sentenza *Schrems I*[81], che segna l'avvio della c.d. saga Schrems, ed arriva, passando

[78] G. BEVILACQUA, *La dimensione territoriale dell'oblio*, cit., pp. 23 e 25.
[79] *Ibid.*, p. 24.
[80] Sentenza *Google Spain*, cit.
[81] Sentenza *Schrems I*, cit.

per quattro sentenze del 2019[82] ed una del 2020[83], fino ai nostri giorni[84], quando è possibile trarre alcune conclusioni, peraltro non ancora di certo definitive, circa l'estensione dell'ambito di applicazione della normativa europea, in un quadro non solo tecnologico, ma anche giuridico, in continua evoluzione.

Nelle decisioni pronunciate nel corso del 2019, la Corte di giustizia ha avuto di nuovo modo di occuparsi del diritto alla deindicizzazione nelle sue varie sfaccettature e sotto prospettive diverse, proseguendo, da un lato, nella progressiva assimilazione, sotto

---

[82] Si tratta delle sentenze del 29 luglio 2019, causa C-40/17, *Fashion ID*, EU:C:2019:629; 24 settembre 2019, causa C-507/17, *Google LLC* c. *CNIL*, EU:C:2019:772; 24 settembre 2019, causa C-136/17, *GC e a.* c. *CNIL*, EU:C:2019:773; 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook*, EU:C:2019:821. Le prime tre sentenze sono relative all'applicazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, ora sostituita dal 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) (noto con l'acronimo GDPR), l'ultima riguarda invece la 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»). Per un commento, fra i tanti, vedi R. CAFARI PANICO, *Riflessioni sul diritto all'oblio e la libertà di espressione nel caso* Eva Glawischnig-Piesczek/Facebook, in A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA (a cura di), Liber Amicorum *per Massimo Panebianco*, Napoli, 2020, p. 57 ss.; T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, in *European Law Blog*, 21 luglio 2020, reperibile *online*; R.Á. COSTELLO, Schrems II: *Everything is Illumiminated?*, in *European Papers*, 2020, pp. 1045-1059, reperibile *online*; M. LEISER, B. SCHERMER, *GC & others vs CNIL and Google: This is a special case*, in *European Law Blog*, 20 novembre 2019, reperibile *online*; D. MESSINA, *Diritto all'oblio e limite territoriale europeo: la sentenza della Corte di Giustizia UE C-507/17 del 24 settembre 2019*, in *De Justitia*, 2020, reperibile *online*; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, pp. 733-759; Y. PADOVA, *Is the right to be forgotten a universal, regional, or 'glocal' right?*, in *International Data Privacy Law*, 2019, reperibile *online*; O. POLLICINO, *Diabolical Persistence. Thoughts on the Schrems II Decision*, in *Verfassungsblog*, 25 luglio 2020, reperibile *online*; E. ROSSI, *Forget me…or not? La Corte di giustizia torna sul diritto di farsi dimenticare. Prima lettura di due recenti pronunce sul «diritto all'oblio»*, in *Sidiblog.it*, 25 novembre 2019, reperibile *online*; M. SAMONTE, *Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law*, in *European Papers*, 2020, pp. 839-851 reperibile *online*; F. ZORZI GIUSTINIANI, *Cronache dal cyberspazio: due sentenze sul diritto all'oblio*, in *Nomos. Le attualità nel diritto*, 2019, reperibile *online*; e F.B. ROMANO, *La Corte di giustizia 'resetta' il diritto all'oblio*, in *federalismi.it*, 5 febbraio 2020, reperibile *online*. Per completare il quadro dell'intervento normativo della Corte di giustizia in tema di trattamento dei dati, va ricordata la sentenza del 1° ottobre 2019, causa C-673/17, *Planet49*, EU:C:2019:801, sul consenso dell'utente di un sito Internet alla installazione di *cookie* sulla sua apparecchiatura terminale e riguardante la direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, nota come direttiva *ePrivacy*.

[83] Sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner*, EU:C:2020:559, nota come *Schrems II*. Per un commento, vedi P. SWIRE, *The US, China, and Case 311/18 on Standard Contractual Clauses*, in *European Law Blog*, 15 luglio 2019, reperibile *online*; C. KUNER, *International data transfers, standard contractual clauses, and the Privacy Shield: the AG Opinion in Schrems II*, in *European Law Blog*, 7 gennaio 2020, reperibile *online*.

[84] V. Avvocato generale Bobek, conclusioni del 13 gennaio 2021, causa C-645/19, *Facebook Ireland e a.*, EU:C:2021:5, nonché il contenzioso pendente dinanzi la High Court di Dublino tra la Data Protection Commission di Dublino e Facebook a seguito della sentenza *Schrems II* della Corte di giustizia: cfr. *Facebook's EU-US data transfers face their final countdown*, 13 gennaio 2021, reperibile *online*.

il profilo della responsabilità, pur con diverse basi giuridiche, dei prestatori di servizi di *hosting*[85] e del titolare del trattamento dei dati[86], e, dall'altro, giungendo a conclusioni sostanzialmente analoghe, qualunque sia la base giuridica, per quanto riguarda i limiti spaziali della tutela accordata dalla disciplina dell'Unione europea, come effetto di un bilanciamento fra i diversi diritti in gioco.

Il risultato, come già osservato, è una sorta di *self restraint* da parte dei giudici del Lussemburgo che, se per un verso lascia un ampio margine di discrezionalità al legislatore nazionale, per un altro indica nell'ordinamento internazionale la sede idonea in cui ricercare le opportune soluzioni in grado di assicurare la necessaria tutela "universale" di diritti originatisi in uno spazio, quello del web, per sua natura illimitato e senza frontiere, ma la cui concreta realizzazione è oggi lasciata ai singoli Stati membri, cui viene rimessa la decisione in merito alla eventuale efficacia extraterritoriale, non esistendo un vincolo in tal senso a livello unionale. In merito sono significative le osservazioni svolte dall'Avvocato generale Szpunar nella causa *Google LLC* c. *CNIL*[87]. Richiesto di precisare l'ambito di applicazione territoriale del diritto alla cancellazione, quale sancito dalla direttiva 95/46, applicabile al caso di specie *ratione temporis*[88], l'Avvocato generale, richiamando il precedente rappresentato dalla sentenza *Google Spain*, afferma come al centro della protezione accordata dalla normativa europea vi siano i diritti della persona i cui dati personali devono essere protetti, che vengono così privilegiati. L'obiettivo della direttiva è infatti «garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali»[89]. Proprio però dalla loro natura di diritti fondamentali deriva l'esigenza che il diritto all'oblio debba essere bilanciato con altri diritti fondamentali[90]. Nel citato caso *Google Spain* la Corte aveva infatti attribuito grande importanza alla necessità che i diritti alla protezione dei dati e alla vita privata siano bilanciati «con l'interesse legittimo del pubblico ad accedere all'informazione ricercata»,

[85] Per *Internet Service Provider* (ISP) si intende l'operatore commerciale che, mediante l'uso di appositi computer con funzioni di server, fornisce ai suoi utenti la possibilità di accedere a Internet e di gestire un proprio sito e proprie caselle di posta elettronica (Treccani, Enciclopedia *online*).

[86] Per tale si intende, ai sensi dell'art. 4, n. 7, del regolamento 2016/679 «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità ei mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli Stati membri». In generale, vedi L. CONTI, *Il ruolo del responsabile del trattamento* (data processor) *prima e dopo il regolamento (UE) n. 2016/679 e il suo rapporto contrattuale con il titolare del trattamento* (data controller), in *Diritto del commercio e degli scambi internazionali*, 2019, p. 199 ss.; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018. Sotto l'autorità del titolare del trattamento può poi agire, ai sensi dell'art. 28 del GDPR, il responsabile del trattamento, che svolge per suo conto l'attività in oggetto: A. PISAPIA, *La tutela per il trattamento*, cit., p. 105 ss.

[87] Conclusioni del 10 gennaio 2019, causa C-507/17, EU:C:2019:15.

[88] *Ivi*, punto 31.

[89] *Ivi*, punto 42.

[90] *Ivi*, punto 57.

che trae anch'esso origine dalla Carta (art. 11)[91]. L'ulteriore osservazione dell'Avvocato generale è che i due ordini di diritti così contrapposti variano nel loro contenuto e nella corrispondente tutela a seconda del paese in cui operano, sicché, ove si ammettesse «una cancellazione a livello mondiale, le autorità dell'Unione non sarebbero in grado di definire e determinare un diritto a ricevere informazioni e, ancor meno, di bilanciarlo con gli altri diritti fondamentali alla protezione dei dati e alla vita privata»[92]. A ciò si aggiungerebbe il rischio di dare l'avvio ad una sorta di "corsa al ribasso" a danno della libertà di espressione a livello mondiale, fornendo ai paesi terzi l'alibi per disporre analogamente una cancellazione in forza delle proprie leggi, precludendo «alle persone che si trovano in uno Stato membro dell'Unione di accedere a un'informazione ricercata"[93]. Di qui la conclusione che la protezione accordata dalle disposizioni della direttiva sia di regola circoscritta al territorio dell'Unione, ovvero al mercato interno[94].

Lo stesso Avvocato generale Szpunar è conscio, da un lato, del fatto che il diritto dell'Unione conosce situazioni in cui sono ammessi gli effetti extraterritoriali delle sue norme e, dall'altro, di come Internet sia «per sua natura mondiale e, in un certo qual senso, presente ovunque», ma proprio da ciò desume l'impossibilità di «trovare analogie e compiere raffronti», pur introducendo in via eccezionale la possibilità per l'Unione «di adottare misure a livello mondiale»[95], senza definirne le circostanze e i limiti. Ciò che emerge è la consapevolezza della impossibilità di risolvere a livello esclusivamente regionale una questione che investe la tutela di un diritto che solo in un contesto universale può, per sua natura, trovare adeguata protezione. Ma ancora più importante è che appaia ormai consolidato il riconoscimento dello *status* di diritto fondamentale di uno dei contenuti principali della costruenda identità digitale.

Con la sentenza *Google LLC* c. *CNIL*[96], la Corte di giustizia, ripercorrendo le argomentazioni dell'Avvocato generale, è giunta ad una decisione che, seppure oggetto di numerose e vivaci critiche in rete da parte dei primi commentatori che vi hanno scorto un cedimento nei confronti di Google, ci sembra indichi invece una soluzione rispondente

[91] *Ivi*, punto 59.
[92] *Ivi*, punto 60.
[93] *Ivi*, punto 61.
[94] *Ivi*, punto 63.
[95] *Ivi*, punto 62. Con riguardo, infine, alla necessità di ricorrere alla tecnica detta del «blocco geografico», a livello europeo, indipendentemente dal nome dell'utente di Internet che effettua la ricerca, vedi punto 64 ss. In generale, sulla portata extraterritoriale del regolamento 2016/679, vedi F. JAULT-SESEKE, *La portée extraterritoriale ou a-territoriale du RGPD*, in *Revue des affaires européennes*, 2018, pp. 43-51.
[96] Causa C-507/17, cit. In stessa data la Corte si è pronunciata nella causa, strettamente connessa, C-136/17, *GC e a.* c. *CNIL*, cit., affermando che il divieto di trattare categorie particolari di dati sensibili si applica anche ai gestori di motori di ricerca e che nell'ambito di una domanda di deindicizzazione dev'essere effettuato un bilanciamento tra i diritti fondamentali del richiedente e quelli degli utenti di Internet potenzialmente interessati a tali informazioni.

a criteri di ragionevolezza, di proporzionalità[97], tenuto conto della normativa vigente, non solo nell'Unione, in tema di diritto all'oblio. La Corte ha infatti stabilito che, «allo stato attuale, non sussiste, per il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente, a seguito di un'ingiunzione di un'autorità di controllo o di un'autorità giudiziaria di uno Stato membro, un obbligo, derivante dal diritto dell'Unione, di effettuare tale deindicizzazione su tutte le versioni del suo motore»[98]. A fronte di questa limitazione dell'ambito territoriale, tuttavia, il gestore è obbligato ad effettuare la deindicizzazione nelle versioni del suo motore di ricerca corrispondenti agli Stati membri e non già «nella sola versione di tale motore corrispondente allo Stato membro di residenza del beneficiario» della stessa deindicizzazione[99], «al fine di assicurare un livello coerente ed elevato di protezione in tutta l'Unione e di rimuovere gli ostacoli alla circolazione dei dati all'interno della stessa»[100]. Infine, in merito alla questione relativa all'applicazione della tecnica del "blocco geografico", la Corte rinvia la scelta del mezzo tecnico di attuazione del *no-index* al prudente apprezzamento del giudice nazionale e al livello di *accountability* del motore di ricerca. Aggiunge che il gestore sarà anche tenuto ad adottare misure sufficientemente efficaci per garantire una tutela effettiva dei diritti fondamentali della persona interessata. In particolare, tali misure devono soddisfare, sulla base di un giudizio che spetta al giudice del rinvio, «tutte le esigenze giuridiche e avere l'effetto di impedire agli utenti di Internet negli Stati membri di avere accesso al link in questione a partire da una ricerca effettuata sulla base del nome di tal persona o, perlomeno, di scoraggiare seriamente tali utenti»[101] dall'accedere a detti *link* mediante una versione "extra UE" del suddetto motore.

Come rilevato, la decisione della Corte non è andata esente da critiche[102] anche severe. Sul contenuto della pronuncia si è espresso in particolare l'allora Garante della Privacy, Antonello Soro, denunciando l'aspetto «anacronistico» della «barriera territoriale» così imposta dalla Corte di giustizia, che rischierebbe di rallentare e rendere più difficile «l'effettività del diritto all'oblio»[103]. In realtà, le argomentazioni della Corte di giustizia non si discostano nella sostanza da quanto precedentemente concluso dall'Avvocato generale, dal momento che, da un lato, viene sottolineato «che il diritto dell'Unione, pur se […] non impone, allo stato attuale, che la deindicizzazione verta su tutte le versioni del motore di ricerca in questione, neppure lo vieta»[104], dall'altro, si

[97] H. MUIR WATT, *La portée territoriale du droit au déréférencement: un exercise de proportionalité dans l'espace*, in *Revue critique de droit international privé*, 2020, pp. 334-348.

[98] Sentenza *Google LLC* c. *CNIL*, cit., punto 64.

[99] *Ivi*, punto 66.

[100] *Ibid.*

[101] *Ivi*, punto 70.

[102] G. CALABRESE, *Bilanciamento ed estensione territoriale del diritto alla deindicizzazione*, in *La Nuova giurisprudenza civile commentata*, 2020, pp. 794-809, spec. p. 807.

[103] Intervista ad Antonello Soro, *Barriere territoriali anacronistiche, questa sentenza penalizza gli utenti*, 25 settembre 2019, reperibile *online*.

[104] Sentenza *Google LLC* c. *CNIL*, cit., punto 72.

riafferma la possibilità per i giudici degli Stati membri di superare, quando la legislazione nazionale lo consenta, tale limitazione, una volta effettuato, «conformemente agli standard nazionali di protezione dei diritti nazionali di protezione dei diritti fondamentali […], un bilanciamento tra, da un lato, il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali e, dall'altro, il diritto alla libertà di informazione. Al termine di tale bilanciamento, i giudici nazionali possono dunque richiedere, se del caso, al gestore di tale motore di ricerca di effettuare una deindicizzazione su tutte le versioni di suddetto motore»[105].

La Corte non ha dunque affatto escluso una applicazione della deindicizzazione a tutte le estensioni anche extra Unione europea del nome di dominio del motore di ricerca. Alla luce, tuttavia, delle differenze ancora esistenti all'interno dell'Unione, fra le legislazioni degli Stati membri, in merito alla valutazione dell'interesse pubblico ad accedere alle informazioni quando tale interesse è posto a confronto, in sede di bilanciamento con i diritti alla tutela della vita privata e alla protezione dei dati personali dell'interessato, i giudici del Lussemburgo hanno ritenuto di rimettere agli stessi Stati membri la decisione finale in merito ai possibili limiti alla libertà di informazione. Il rischio naturalmente è che, in assenza di una disciplina comune, l'aver lasciato l'effettiva applicazione del diritto all'oblio nei riguardi dei paesi terzi alla valutazione discrezionale dei singoli Stati membri dia luogo a fenomeni di *forum shopping* collegati alla ampiezza dei criteri cui far ricorso per la determinazione della giurisdizione competente.

Sarebbe invece errato dedurre dalla pronuncia della Corte, motivata dalla prudenza che si impone ogni qualvolta si tratta di estendere l'ambito di applicazione delle norme dell'Unione oltre i suoi confini territoriali, un atteggiamento intenzionalmente restrittivo del diritto all'oblio sancito dall'art. 17 del regolamento 2016/679. È infatti la stessa Corte a rilevare come «una deindicizzazione effettuata su tutte le versioni di un motore di ricerca»[106] sia l'unica idonea a garantire un elevato livello di protezione dei dati personali in tutta l'Unione. In altre parole, per una efficace tutela occorrerebbe superare le barriere territoriali, dal momento che «Internet è infatti una rete globale senza frontiere e i motori di ricerca conferiscono ubiquità alle informazioni e ai link contenuti in un elenco di risultati visualizzato a seguito di una ricerca effettuata a partire dal nome di una persona fisica»[107]. L'accesso da parte degli utenti di Internet localizzati al di fuori dell'Unione all'indicizzazione di un *link*, «che rinvia a informazioni concernenti una persona il cui centro di interessi si trova nell'Unione, può quindi produrre effetti immediati e sostanziali sulla persona in questione anche all'interno dell'Unione», tanto da giustificare di per sé la possibilità che il legislatore europeo intervenga prevedendo l'obbligo di una deindicizzazione a livello "mondiale", ovvero su tutte le versioni del motore di ricerca[108].

[105] *Ibid.*
[106] *Ivi*, punto 55.
[107] *Ivi*, punto 56.
[108] *Ivi*, punto 58.

Il legislatore europeo ha compiuto invece, ad avviso della Corte, una scelta diversa, vale a dire ha rinunciato ad imporre un obbligo di tale portata per una serie di ragioni, tra cui la constatazione di come molti Stati terzi non riconoscono «il diritto alla deindicizzazione o comunque adottano un approccio diverso per tale diritto»[109]. A ciò si aggiunge che il diritto alla protezione dei dati personali «non è una prerogativa assoluta»[110], ma va considerato alla luce della sua funzione sociale[111] e va contemperato con altri diritti fondamentali, in funzione del principio di proporzionalità[112] e sulla base di un bilanciamento tra tale diritto e, in particolare, la libertà di informazione degli utenti di Internet che «può variare notevolmente nel mondo»[113].

La conclusione della Corte è che il legislatore dell'Unione non ha per il momento proceduto a tale bilanciamento «per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione»[114] e neppure ha inteso attribuire ai diritti riconosciuti ai singoli «una portata che vada oltre il territorio degli Stati membri»[115]. Alla stessa stregua, il tenore letterale delle disposizioni vigenti esclude che il diritto comune imponga ad un operatore come Google un obbligo di deindicizzazione riguardante «anche le versioni nazionali del suo motore di ricerca che non corrispondono agli Stati membri»[116]. Per di più il diritto dell'Unione non prevede strumenti e meccanismi di cooperazione per quanto riguarda «la portata di una deindicizzazione al di fuori dell'Unione»[117].

In tali circostanze, la Corte non poteva far altro se non lasciare agli Stati membri, sulla base di distinte valutazioni, la possibilità di effettuare il necessario bilanciamento e di adottare, come già rilevato, le opportune misure destinate, nel caso, ad avere anche effetti extraterritoriali, visto che il diritto dell'Unione di per sé non lo esclude, pur rilevandone le difficoltà di realizzazione sul piano pratico.

La decisione della Corte nel caso *Google LLC* c. *CNIL*, del 24 settembre 2019, si pone in continuità con quel processo avviato con la pronuncia nel citato caso *Schrems I* e consolidato nel regolamento sulla privacy, per cui la liquidità dello spazio di Internet comporta necessariamente l'assenza di confini. Non si tratta infatti di spazi fisici, ma di spazi immateriali delimitati da frontiere prive di forme visibili, ma non per questo inesistenti, che il fine di tutelare i dati personali, per loro natura non connessi ad un determinato territorio, consente di superare ma solo in circostanze eccezionali, come lo sono tutte le circostanze nelle quali l'esercizio della "sovranità", dell'Unione, come degli

[109] *Ivi*, punto 59.
[110] *Ivi*, punto 60.
[111] Sul punto, vedi F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *I Post di AISDUE*, I, 2019, p. 145 ss., reperibile *online*.
[112] C. GENTILE, *La saga* Schrems *e la tutela dei diritti fondamentali*, in *federalismi.it*, 13 gennaio 2021, p. 52 s., reperibile *online*.
[113] F. ROSSI DAL POZZO, *La giurisprudenza*, cit.
[114] Sentenza *Google LLC* c. *CNIL*, cit., punto 61.
[115] *Ivi*, punto 62.
[116] *Ibid.*
[117] *Ivi*, punto 63.

Stati, esorbita i propri confini. Come si evince dall'art. 3 del regolamento 2016/679, la normativa europea trova applicazione ogniqualvolta l'attività di profilazione attiene alla elaborazione di dati che riguardano dati personali di soggetti che si trovano nel territorio dell'Unione, a prescindere se cittadini, residenti o meno[118], indipendentemente dal fatto che il trattamento sia effettuato nell'Unione e anche con riguardo a titolari e responsabili del trattamento non stabiliti nella stessa Unione europea. Fissato in tal modo il nuovo confine che segue il luogo in cui è situato il soggetto interessato, la linea di demarcazione così tracciata potrà essere superata, sul piano interno, solo quando il mantenimento del difficile equilibrio tra diritto alla privacy e libertà di espressione lo consenta, e, su quello esterno, ove circostanze eccezionali impongano e consentano una tutela "universale" della privacy, travalicando quei limiti che la stessa Unione si è posta nell'esercizio dei suoi poteri sovrani nella prospettiva di contribuire alla realizzazione «di uno spazio di libertà, sicurezza e giustizia e di un'unione economica» oltre che «al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche»[119].

Ma la storia riservava ancora delle sorprese e la nostra narrazione prosegue.

4. *Segue*: le sentenze *Eva Glawinschnig-Piesczek/Facebook* e *Schrems II*.

Quelle stesse difficoltà emerse nel caso *Google LLC* c. *CNIL* sono sottolineate nella decisione che di lì a qualche giorno, il 3 ottobre 2019[120], la stessa Corte ha pronunciato con riguardo ad una questione analoga che vedeva coinvolta ancora una volta Facebook Ireland, ma sotto un diverso profilo, ovvero non più con riguardo alla tutela dei dati personali, bensì in attuazione della direttiva sul commercio elettronico. Il caso *Eva Glawinschnig-Piesczek* c. *Facebook* ha offerto alla Corte di giustizia l'occasione per affrontare di nuovo, a distanza di pochi giorni, tra l'altro, la questione dell'estensione, sul piano soggettivo e oggettivo, degli obblighi di sorveglianza che la normativa dell'Unione pone in capo agli intermediari Internet (ISP). Il problema assume una particolare rilevanza perché la soluzione fornita dalla Corte è destinata ad incidere sia sui poteri così attribuiti alle autorità nazionali in sede di controllo sia sui limiti della loro giurisdizione in casi, come lo sono di regola quelli che riguardano il *web*, di rilevanza transfrontaliera delle attività in esame. Altrettanto evidente è che la pronuncia della Corte ha fissato i limiti reciproci di esercizio di diritti fondamentali quali quello all'oblio e quello, di certo non meno rilevante, alla libertà di espressione. Sotto quest'ultimo profilo già le considerazioni

[118] C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza nel tempo del web*, in *federalismi.it*, 3 luglio 2019, p. 14, reperibile *online*. Nel caso *Schrems I* l'attività di elaborazione riguardava cittadini dell'Unione europea.

[119] Secondo considerando regolamento 2016/679. Sul punto, vedi C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., p. 15.

[120] Sentenza *Glawischnig-Piesczek*, cit.

espresse dall'Avvocato generale, volte ad una ponderazione degli interessi sottesi dai diversi diritti fondamentali in gioco, avevano suscitato perplessità e preoccupazione nei commentatori[121]. Le stesse considerazioni critiche sono state espresse[122] immediatamente dopo la decisione della Corte, tanto da far parlare di una sorta di «schizofrenia giudiziale»[123].

Il caso aveva tratto origine dalla richiesta ai giudici austriaci, da parte della sig.ra Glawischnig-Piesczek, ex deputata alla Camera dei rappresentanti del Parlamento austriaco, presidente del gruppo parlamentare dei Verdi e portavoce nazionale di tale partito, di emettere una ordinanza cautelare nei confronti di Facebook Ireland[124] per porre fine alla pubblicazione di un commento diffamatorio nei suoi confronti. Un utente di Facebook aveva infatti condiviso, sulla sua pagina personale, un articolo relativo alla posizione politica assunta dai Verdi in merito al trattamento dei rifugiati. Tale pubblicazione ha avuto come effetto di creare su Facebook un «riquadro anteprima» del sito *online* della rivista su cui era apparso l'articolo, contenente il titolo e un breve riassunto dell'articolo stesso, nonché una fotografia della sig.ra Glawischnig-Piesczek unitamente ad un commento degradante nei suoi confronti. Siffatti contenuti potevano essere consultati da qualsiasi utente di Facebook.

Non avendo Facebook dato seguito alla richiesta di cancellare il suddetto commento, la sig.ra Glawischnig-Piesczek aveva chiesto ed ottenuto dal giudice di primo grado che venisse emessa un'ordinanza cautelare con cui veniva ordinato a Facebook di cessare la pubblicazione e/o diffusione di foto che la ritraessero qualora il messaggio di accompagnamento diffondesse affermazioni identiche al commento di cui si trattava e/o con contenuto equivalente.

Di conseguenza, Facebook disabilitava in Austria l'accesso al contenuto inizialmente pubblicato mentre della controversia veniva investita l'Oberster Gerichtshof

---

[121] P. CAVALIERE, *AG Opinion on C-18/18: Towards private regulation of speech worldwide*, in *European Law Blog*, 28 giugno 2019, reperibile *online*.

[122] Vedi Corriere della Sera, 4 ottobre 2019, p. 26, dove si evidenzia una apparente contraddizione con la precedente giurisprudenza.

[123] O. POLLICINO, *L'autunno caldo della Corte di giustizia*, cit. Vedi anche F. CALOPRISCO, *La Corte di giustizia si esprime sulla portata territoriale dell'obbligo di deindicizzare i dati personali* online. *Sul bilanciamento caso per caso tra* selfrestraint *ed espansionismo del diritto dell'Unione*, in *I Post di AISDUE*, I, 2019, reperibile *online*. Nel senso che non vi sia contraddizione con la sentenza *Google LLC* c. *CNIL* in merito alla territorialità della deindicizzazione, L.S. ROSSI, *Brevi osservazioni sulle recenti tendenze evolutive della giurisprudenza della Corte di Giustizia dell'Unione europea sulla protezione dei dati personali*, in F. ROSSI DAL POZZO F. (a cura di), *Mercato unico digitale*, cit., pp. 51-56, spec. p. 55: «mentre nella pronuncia Google, si trattava di una semplice richiesta formulata da un individuo a vedersi tutelato il diritto all'oblio, nella sentenza *Glawischnig*, era intervenuta una sentenza di un giudice, che presuppone un'indagine e un seguente accertamento. Non vi è dunque contraddizione fra le due sentenze: a situazioni diverse corrisponde un bilanciamento diverso dei diritti in gioco. Il diritto all'oblio si contempera con la libertà di espressione e con la libertà di stampa, ma quest'ultima non giustifica qualunque violazione e tantomeno il diritto all'odio».

[124] Facebook Ireland gestiva, quale filiale della Facebook Inc., una piattaforma elettronica unicamente per gli utenti situati al di fuori degli Stati Uniti e del Canada.

(Corte suprema austriaca), che, quale giudice del rinvio, ha chiesto alla Corte di giustizia di interpretare la direttiva sul commercio elettronico e, in particolare, di dichiarare se, nell'ambito di un'ingiunzione emessa dal giudice di uno Stato membro, un *host provider* possa essere costretto a rimuovere determinati contenuti non solo per gli utenti di Internet di tale Stato membro, ma anche a livello mondiale, e se il provvedimento inibitorio potesse essere esteso alle dichiarazioni testualmente identiche e/o dal contenuto equivalente di cui Facebook non era a conoscenza.

Il riferimento alla direttiva sul commercio elettronico in luogo di quella sulla privacy trovava giustificazione nella natura dell'attività svolta in questa circostanza da Facebook Ireland, cui non veniva imputata una responsabilità derivante dal trattamento dei dati, quanto piuttosto il mancato esercizio della dovuta sorveglianza che avrebbe dovuto comportare la deindicizzazione delle informazioni illecite, a prescindere dalla sussistenza o meno delle condizioni di esonero dalla responsabilità circa le informazioni memorizzate[125].

Chiamato a presentare le proprie conclusioni anche su queste questioni, che ripropongono il tema della a-territorialità della rete Internet che rischia di rendere di fatto inefficaci molte pronunce dei tribunali nazionali, l'Avvocato generale Szpunar[126] procede, anzitutto, a definire l'ambito delle informazioni che l'*host provider* può essere costretto a ricercare e individuare, riconducendo in esse anche quelle identiche a quella qualificata come illecita dal giudice che ha emesso il provvedimento ingiuntivo[127]. Tale approccio consente di garantire un giusto equilibrio tra i diritti fondamentali coinvolti, ovvero la protezione della vita privata e dei diritti della personalità, quella della libertà di impresa, nonché quella della libertà d'espressione e di informazione. Una valutazione più approfondita, sempre al fine di assicurare il dovuto equilibrio fra i diversi diritti fondamentali, si impone con riguardo all'obbligo eventualmente imposto all'*host provider* di ricercare ed individuare anche le informazioni equivalenti a quella qualificata come illecita[128]. Occorre infatti in tal caso che gli effetti della rimozione a seguito del provvedimento ingiuntivo siano chiari, precisi e prevedibili, tenendo conto del principio di proporzionalità, in modo da evitare, tra l'altro, un possibile limitazione della libertà di espressione e di informazione, assumendo le forme di una misura di censura. La fase della irresponsabilità delle piattaforme (e di chi le gestisce) sembra dunque volgere al termine, anche se si è ancora alla ricerca del giusto assetto degli interessi in gioco.

[125] Secondo la direttiva 2000/31 un prestatore di servizi di *hosting* non è infatti responsabile delle informazioni memorizzate qualora non sia a conoscenza della loro illiceità o qualora agisca immediatamente rimuoverle o per disabilitare l'accesso alle medesime non appena ne venga a conoscenza (art. 14(b)).

[126] Conclusioni del 4 giugno 2019, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook*, EU:C:2019:458.

[127] *Ivi*, punto 55 ss.

[128] *Ivi*, punto 66 ss.

Da ultimo, l'Avvocato generale affronta il problema della portata territoriale di un obbligo di rimozione delle informazioni diffuse tramite una piattaforma di *social network*[129], rilevando come la direttiva sul commercio elettronico non osti a che un *host provider* sia costretto a rimuovere siffatte informazioni. Richiamando le osservazioni già svolte nella causa *Google LLC* c. *CNIL*, in merito alla analoga questione relativa alla portata territoriale di una cancellazione dei risultati di un motore di ricerca, con riferimento alle norme armonizzate sulla protezione dei dati, l'Avvocato generale sottolinea tuttavia la diversità di situazioni, in assenza di armonizzazione in tema di pregiudizio alla vita privata e ai diritti della personalità derivante da azioni di diffamazione[130]. Egli si esprime perciò nel senso che la questione è sottratta alla applicazione delle norme del diritto dell'Unione, non essendo stato fatto valere alcun diritto in materia di tutela dei dati personali, ed è quindi rimessa al diritto internazionale pubblico e privato nel caso applicabile dal giudice nazionale. Ciò non toglie che tale soluzione presenti degli inconvenienti sul piano della sua attuazione concreta. Ne consegue che se, in teoria, il giudice di uno Stato membro può «statuire sulla rimozione di informazioni diffuse a mezzo Internet a livello mondiale», ciò nondimeno, «a causa delle differenze esistenti fra le leggi nazionali, da un lato, e la tutela della vita privata e dei diritti della personalità da esse prevista, dall'altro, e al fine di rispettare i diritti fondamentali ampiamente diffusi, un siffatto giudice deve adottare piuttosto un atteggiamento di autolimitazione»[131].

La Corte, nell'esaminare le varie questioni, muove dalla premessa che sebbene l'art. 15, par. 1 della direttiva 2000/31 vieti agli Stati membri di imporre ad un *host provider* «un obbligo generale di sorvegliare le informazioni che trasmettono o memorizzano, o un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite […], tale divieto non riguarda gli obblighi di sorveglianza "in casi specifici"»[132], quale quello di cui si discuteva nel procedimento. Ne consegue che, così come già sostenuto dall'Avvocato generale, il giudice competente può ordinare ad un prestatore di servizi di hosting «di bloccare l'accesso alle informazioni memorizzate, il cui contenuto sia identico a quello precedentemente dichiarato illecito, o di rimuovere tali informazioni, qualunque sia l'autore della richiesta di memorizzazione delle medesime», non ponendo tale ingiunzione a carico dello stesso prestatore di servizi un obbligo di natura «generale» [133]. La Corte precisa inoltre, a questo riguardo, che, dovendosi stabilire un equilibrio fra i vari interessi in gioco[134], l'obiettivo della tutela della reputazione e dell'onore di una persona non può comportare per il prestatore di servizi di *hosting* «un

[129] *Ivi*, punto 76 ss.
[130] *Ivi*, punto 79.
[131] *Ivi*, punto 100.
[132] Sentenza *Glawischnig-Piesczek*, cit., punto 34.
[133] *Ivi*, punto 37.
[134] *Ivi*, punto 43.

obbligo eccessivo»[135]. La questione assume rilievo quando si tratti di valutare se l'obbligo posto a carico dell'*host provider* possa estendersi, per essere realmente efficace, anche alle informazioni equivalenti, ovvero a quelle «il cui contenuto, pur veicolando sostanzialmente lo stesso messaggio, sia formulato in modo leggermente diverso, a causa delle parole utilizzate o della loro combinazione, rispetto all'informazione il cui contenuto sia dichiarato illecito»[136]. L'opinione della Corte è che differenze nella formulazione delle informazioni equivalenti, che non siano tali da costringere il prestatore di servizi ad una «valutazione autonoma» del loro contenuto[137], non costituiscano un ostacolo ad una estensione dell'obbligo di sorveglianza, non rappresentando per lo stesso un onere eccessivo[138].

Infine, la Corte affronta la questione della portata territoriale dei provvedimenti adottati dagli Stati, concludendo che, stante l'ampia discrezionalità riconosciuta agli Stati dalla direttiva 2000/31 in merito ai ricorsi e alle procedure preordinati a porre fine a qualsiasi presunta violazione o a impedire qualsiasi ulteriore danno agli interessi in gioco[139], nulla osta «a che detti provvedimenti ingiuntivi producano effetto a livello mondiale»[140]. In realtà, la Corte interviene subito a precisare i confini di tale possibile efficacia extraterritoriale, osservando come il legislatore dell'Unione, stante la dimensione mondiale dei servizi elettronici, abbia comunque «ritenuto necessario garantire la coerenza delle norme dell'Unione in tal ambito con le norme applicabili a livello internazionale»[141]. In altri termini, come già rilevato dall'Avvocato generale, la questione esula dal diritto dell'Unione, ma non è neppure rimessa completamente alla discrezionalità degli Stati membri, in quanto il rispetto del diritto internazionale è imposto loro non solo dal diritto nazionale, ma anche da quello dell'Unione, nella misura in cui la direttiva ha previsto tale vincolo generale di coerenza, che per essa ha significato una autolimitazione del proprio potere di legiferare e che per gli Stati rappresenta un obbligo di adeguamento delle misure che volessero adottare in tale ambito.

Seppure in una prospettiva diversa, anche nella decisione del 3 ottobre 2019 la Corte ha dunque assunto un atteggiamento di prudenza per quanto riguarda l'estensione degli effetti della propria legislazione al di fuori dei confini dell'Unione[142], lasciando ancora una volta spazio alla competenza degli Stati, ma fissando al contempo dei paletti che, nel caso di specie, sono rappresentati dal diritto internazionale e, in quello precedente, dal

[135] *Ivi*, punto 44.
[136] *Ivi*, punto 41.
[137] *Ivi*, punto 45.
[138] *Ivi*, punto 46.
[139] *Ivi*, punti 29 e 30.
[140] *Ivi*, punto 50.
[141] *Ivi*, punto 51.
[142] Per considerazioni critiche in merito alle possibili restrizioni alla libertà di espressione, vedi P. CAVALIERE, *AG Opinion on C-18/18*, cit.

bilanciamento tra i vari diritti[143], che non può non tenere conto delle diverse discipline esistenti negli Stati terzi e delle conseguenze che un obbligo imposto dai giudici degli Stati membri a livello mondiale possono comportare.

L'occasione per verificare le conseguenze dell'attuale indirizzo giurisprudenziale, con riguardo in particolare al rapporto tra la disciplina europea della privacy e la c.d. "legge della piattaforma", è stata fornita dalla decisione *Schrems II*, del 16 luglio 2020[144], che costituisce l'ennesimo episodio di un confronto che ha condotto ad un mutamento della disciplina dei flussi informativi transfrontalieri fra l'Unione europea e gli Stati Uniti[145], che ora vengono eseguiti tramite un protocollo normativo denominato *Standard Contractual Clauses*[146]. Secondo il sig. Schrems anche questo protocollo non sarebbe stato tuttavia sicuro e di conseguenza ha chiesto al Garante irlandese della privacy di bloccare il flusso dei dati. Investita della questione, la Corte di giustizia si è di fatto pronunciata sulla possibilità che il traffico informativo debba avvenire unicamente tramite server allocati in Europa, con una inevitabile estensione della applicazione della disciplina europea a livello mondiale che non potrebbe non riguardare anche l'esercizio del diritto all'oblio. Con ciò siamo certamente ancora lontani dal poter prospettare l'esistenza di una sorta di *lex* elettronica europea[147], con l'aspirazione a imporsi come novella *lex mercatoria*[148] quale diritto universale di Internet, ma sicuramente il cammino che l'Unione europea sta compiendo su questa strada è sempre più significativo e soprattutto segnato da una profonda divaricazione con l'esperienza statunitense[149], in attesa di un ricongiungersi delle diverse esperienze in uno strumento di collaborazione internazionale la cui realizzazione appare al momento ancora tutta da costruire.

Nelle conclusioni presentate il 19 dicembre 2019[150] l'Avvocato generale Saugmandsgaard Øe pareva aver circoscritto le proiezioni "universalistiche" della disciplina dell'Unione, pur lasciando alla Corte ampio spazio per una propria diversa

---

[143] G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2018, n. 2, reperibile *online*.

[144] Corte di giustizia (Grande Sezione), causa C-311/18, *Data Protection Commissioner*, EU:C:2020:559, nota come *Schrems II*.

[145] Vedi, per ampie considerazioni critiche, F. ROSSI DAL POZZO, *L'accordo* Privacy Shield *non è un vero scudo per la* privacy: *scenari passati e futuri in merito al trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di diritto internazionale*, 2020, pp. 1112-1121.

[146] Per una panoramica delle norme che disciplinano il trasferimento dei dati personali verso paesi terzi, al di fuori dello Spazio Economico Europeo (SEE), vedi, per tutti, R. PANETTA, *Il trasferimento all'estero dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati*, cit., pp. 357-381.

[147] C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., p. 19.

[148] Sulla evoluzione del rapporto fra concorrenza e privacy e il progressivo affermarsi di una *lex mercatoria*, G. DE MINICO, Big Data *e la debole resistenza delle categorie giuridiche.* Privacy *e* lex mercatoria, in *Diritto pubblico*, 2019, pp. 89-115.

[149] C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., p. 20 s.

[150] Causa C-311/18, *Data Protection Commissioner*, EU:C:2019:1145.

valutazione. Veniva infatti precisato, con riguardo alla decisione 2010/87[151], che detta decisione e le clausole contrattuali tipo da essa previste non sono «vincolanti per le autorità del paese terzo di destinazione»[152]. Il diritto dell'Unione si applica, in realtà, unicamente «*al trattamento costituito dal trasferimento in quanto tale*»[153], fermo restando che tale trasferimento di dati personali, nel corso di attività commerciali, da Stati membri dell'Unione verso Paesi terzi può avvenire solo se in essi è assicurato un livello di protezione "adeguato". Ogni successiva attività di trattamento di quei dati nel paese di destinazione, anche per finalità che comprendono la protezione della sicurezza nazionale, esula dall'ambito di applicazione territoriale del GDPR[154].

In definitiva, l'oggetto del controllo operato al momento del trasferimento dei dati personali in forza di clausole contrattuali tipo comprende anche le eventuali norme imperative del paese terzo, che non saranno di ostacolo quando appaiano proporzionate alla luce delle finalità perseguite, tra le quali anche la sicurezza pubblica, riconosciuta dallo stesso ordinamento dell'Unione, e della necessita di salvaguardare i legittimi interessi dell'Unione nonché i diritti fondamentali garantiti dalla Carta. L'obiettivo è infatti quello di verificare se il paese di destinazione garantisce «un livello di tutela dei diritti e delle libertà fondamentali *sostanzialmente equivalente* a quello garantito all'interno dell'Unione»[155].

La Corte, da parte sua, ha fatto propria la posizione illustrata dall'Avvocato generale e proseguito secondo le medesime linee di ragionamento, senza rinunciare di fatto ad una pretesa di universalità, che si sarebbe estesa ad una valutazione di adeguatezza anche del trattamento successivo dei dati, ma riconducendo tale pretesa nella più tranquillizzante prospettiva dell'applicazione del principio di proporzionalità. Ad essere così affermata è una sorta di doppio binario di applicazione: uno, domestico, legato

---

[151] Decisione 2010/87 della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016.

[152] Conclusioni Avvocato generale Saugmandsgaard Øe, *Data Protection Commissioner*, punto 127.

[153] *Ivi*, punto 104 (corsivo nel testo originale).

[154] *Ibid.*

[155] *Ivi*, punto 112 (corsivo nel testo originale). Sempre in tema di protezione dei dati personali e di esigenze di sicurezza nazionale, ma con riguardo a fattispecie interne all'Unione, vedi, per considerazioni analoghe, a riprova dell'applicazione dei medesimi standard quando si tratta di tutelare i diritti delle persone rispetto alle esigenze di sicurezza, secondo un criterio di proporzionalità, a prescindere dall'ambito di impatto territoriale, Corte di giustizia, sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International*, EU:C:2020:790. Oltremodo significativa è, infine, la sentenza del Tribunale costituzionale federale tedesco (BVerfG), del 19 maggio 2020 (1 BvR 2835/17), dove, con riferimento all'attività informativa svolta sull'estero dai servizi segreti, viene attribuita ai diritti fondamentali un'efficacia extraterritoriale di cui può avvalersi anche il cittadino straniero all'estero per difendersi dall'esercizio di dette attività: per un commento, R. BIFULCO, *L'efficacia extraterritoriale dei diritti fondamentali in una storica sentenza del Tribunale costituzionale federale tedesco*, in *Medialaws*, 29 ottobre 2020, reperibile *online*; K. IRION, *Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law*, in *European Law Blog*, 24 luglio 2020, reperibile *online*.

al mercato interno[156], in cui ampio spazio è lasciato agli Stati, che possono estendere l'applicazione delle proprie norme sostanziali, così come richiamate dalle norme di conflitto[157], nei limiti fissati dalla possibilità concreta di esercizio della propria giurisdizione, nel rispetto comunque delle regole del diritto internazionale, come confermato dalle conclusioni dell'Avvocato generale del 13 gennaio 2021[158]. L'altro, frutto della globalizzazione e più prettamente europeo, dove il bilanciamento fra i diversi interessi in gioco viene effettuato dalla Corte di giustizia secondo criteri di ragionevolezza e proporzionalità[159]. Il rischio implicito è, da un lato, che, demandando l'ampiezza della tutela alle norme processuali del singolo Stato membro, si favorisca il forum shopping e, dall'altro, che l'azione statale, se fondata su criteri esorbitanti di giurisdizione, finisca per non godere dell'ombrello protettivo del diritto dell'Unione.

5. Conclusioni: la legislazione europea come modello per una regolamentazione su scala globale dei diritti di Internet.

Le conseguenze della giurisprudenza della Corte sono estremamente significative sul piano operativo, nei rapporti commerciali[160], come dimostrano la pubblicazione da parte dell'*European Data Protection Board* di proprie raccomandazioni[161] sul comportamento che le imprese devono tenere e, soprattutto, le iniziative immediatamente

[156] J. MEEUSEN, *The "Logic of Globalisation" versus the "Logic of the Internal Market": a New Challenge for the European Union*, in *Acta Universitatis Carolinae-Iuridica*, 2020, pp. 19-29, spec. p. 28, reperibile *online*.

[157] Così M. SZPUNAR, *Territoriality of Union Law in the Era of Globalisation*, in D. PETRLÍK, M. BOBEK, J.M. PASSER (cor.), *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux. Liber amicorum Jiří Malenovský*, Bruxelles, 2020, pp. 149-168.

[158] Conclusioni *Facebook Ireland e a.*, cit., per il quale l'autorità per la protezione dei dati dello Stato in cui il titolare del trattamento o il responsabile del trattamento ha il suo stabilimento principale nell'Unione europea detiene una competenza generale per agire in sede giudiziale per violazioni del GDPR in relazione al trattamento transfrontaliero dei dati. Le altre autorità nazionali per la protezione dei dati interessate hanno tuttavia il diritto di intentare tali azioni nel rispettivo Stato membro nei casi in cui il GDPR consenta loro specificamente di farlo. Tali considerazioni sono state accolte dalla Corte di giustizia (Grande Sezione), sentenza del 15 giugno 2021, causa C-645/19, *Facebook Ireland e a*, ECLI:EU:C:2021:483.

[159] D. KLOZA, L. DRECHSLER, *Proportionality has come to the GDPR*, in *European Law Blog*, 9 dicembre 2020, reperibile *online*.

[160] Vedi P. MARINI, *Il 'Lato B' della sentenza 'Schrems II' è un pesante 'caveat' sul ricorso alle clausole tipo*, 31 luglio 2020, reperibile *online*; M. MASNADA, *Privacy Shield, ecco le conseguenze commerciali della sentenza "Schrems II"*, 30 luglio 2020, reperibile *online*; e I. OLDANI, *The Future of Data Transfer Rules in the Aftermath of Schrems II*, in *SIDIBlog*, 23 ottobre 2020, reperibile *online*.

[161] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with EU level of protection of personal data, e Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, documenti entrambi del 10 novembre 2020: per un commento, T. CHRISTAKIS, *"Schrems III"? First Thoughts on the EDPB post- Schrems II Recommendations on International Data Transfers (Part 1)*, in *European Law Blog*, 13 novembre 2020, reperibile *online*; ID., *"Schrems III"? First Thoughts on the EDPB post- Schrems II Recommendations on International Data Transfers (Part 2)*, in *European Law Blog*, 16 novembre 2020, reperibile *online*. Si vedano anche, sempre dell'EDPB, le Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. Version 2.0, adottate il 15 dicembre 2020.

avviate dalla *Irish Data Protection Commission* che, proprio sulla base della sentenza della Corte di giustizia, nell'agosto 2020, ha ingiunto (*preliminary order*)[162] a Facebook, di interrompere[163] il trasferimento dei dati dei clienti europei verso i server con sede negli Stati Uniti.

L'insufficienza dei mezzi tradizionali è però di tutta evidenza, come lo è il rilievo che una soluzione non può che essere ricercata sul piano internazionale. Il tutto non esclude poi che in futuro la legislazione europea possa divenire, in virtù del c.d. effetto Brussels, modello per altri sistemi giuridici, realizzando così una uniformità sostanziale di soluzioni, quale unico strumento per una effettiva e completa tutela dei dati personali anche oltre i confini dell'Unione, in un mondo virtuale dove l'anacronismo delle barriere fisiche deve sempre e comunque misurarsi con la sovranità dei singoli Stati.

Indubbiamente per il legislatore nazionale ed europeo sono innumerevoli le sfide, di non facile soluzione, poste dall'avanzata della tecnologia e in questo contesto significativi sono gli sforzi compiuti in particolare dal legislatore europeo in materia di libero accesso al web, di neutralità della rete, di alfabetizzazione digitale e, più in generale, in materia di digitalizzazione della società, in un confronto sempre più serrato con i nuovi e complessi problemi che derivano dalla globalizzazione.

Le prospettive poste da Internet impongono dunque una rilettura degli schemi tradizionali che finisce per generare nuovi diritti e nuove forme di estrinsecazione delle libertà fondamentali dell'individuo che già sono tutelate dai Trattati e che ora divengono strumentali all'affermarsi di questi diritti della persona di ultima generazione, destinati ad essere esercitati dal cittadino dell'Unione nell'ecosistema che la stessa Unione si è impegnata a sviluppare, avvalendosi degli strumenti che le libertà fondamentali pongono a sua disposizione.

La narrazione non è però giunta al termine con queste osservazioni. Riavvolgendo il filo delle analisi e delle considerazioni finora svolte e rileggendole sotto una diversa prospettiva, ci si rende purtroppo conto che la soluzione ai problemi emersi nel corso dell'indagine non può essere rappresentata dal mero rinvio agli strumenti tradizionali di regolamentazione forniti dal diritto internazionale convenzionale. Tale conclusione sarebbe infatti corretta se quello virtuale del *web* fosse effettivamente uno spazio giuridicamente vuoto, in quanto spazio libero su cui gli Stati a vario titolo e in vario modo avanzano pretese di sovranità che, secondo meccanismi ben noti alle relazioni internazionali, finiscono per limitarsi vicendevolmente, in modo da evitare esercizi

[162] A seguito del ricorso presentato da Facebook, che ha comportato, il 14 settembre 2020, la sospensione della ingiunzione, la questione è pendente dinanzi la High Court di Dublino ed una decisione è attesa per i primi mesi del 2021: M. CAROLAN, *High Court to decide on Facebook's data commissioner challange as soon possible*, in *The Irish Times*, 13 January 2021, reperibile *online*.

[163] S. SCHECHNER, E. GLAZER, *Ireland to Order Facebook to Stop Sending User Data to U.S.*, in *The Wall Street Journal*, 9 September 2020, reperibile *online*.

esorbitanti di potere. Non a caso si è fatto riferimento al regime degli spazi marini[164]. In questo contesto, ogni Stato potrebbe pretendere di far valere i propri principi ed affermare i propri valori nella misura in cui essi non trovino un ostacolo nei differenti principi e valori parimenti affermati da un altro Stato. In tali circostanze, l'unica soluzione diverrebbe quella della definizione sul piano internazionale di regole pattizie comuni, vista la assenza di norme consuetudinarie, oppure il completarsi di quel processo di sostanziale armonizzazione delle soluzioni normative che in parte viene raggiunto con l'effetto trainante esercitato da una legislazione dominante rispetto alle altre.

In realtà, il quadro così descritto non risponde pienamente alla realtà virtuale, ma al contempo estremamente concreta, di Internet. Una chiave diversa di lettura ci viene del resto offerta dalla giurisprudenza della Corte di giustizia relativa alle pretese di extraterritorialità del diritto dell'Unione. Le ragioni del *self restraint* adottato al riguardo dalla Corte di giustizia sono speculari alla irragionevolezza delle affermazioni di chi pretende un'ulteriore estensione, tendenzialmente universale, dell'ambito di applicazione delle regole di un singolo ordinamento, quello unionale nella specie, o, nel caso, quello statale. I giudici del Lussemburgo quando affermano che non è nelle competenze dell'Unione, semmai dei singoli Stati, estendere l'efficacia extraterritoriale delle proprie norme, non compiono un gran rifiuto, ma semplicemente prendono atto, non si sa quanto consapevolmente, del fatto che la realtà virtuale con cui ci si confronta è già popolata da entità aliene (le piattaforme) dai mille tentacoli (motori di ricerca) che, come insaziabili idrovore, aspirano i nostri dati personali e non, per poi ingurgitarli in una sorta di buco nero, di vuoto pneumatico, in cui i diritti fondamentali si dissolvono, perdendosene ogni traccia. I dati personali riappaiono poi casualmente, una volta rielaborati da misteriosi algoritmi, in forme nuove e non più distinguibili, nei luoghi e nei modi più disparati, rendendo vana ogni forma di protezione *ex post*.

Responsabili di tali comportamenti sono pochi soggetti in perenne conflitto tra loro[165], per l'affermazione del diritto del più forte, anche col supporto dello Stato di appartenenza[166], che operano assumendo le vesti di imprese transnazionali, dotate ciascuna di connotazioni proprie tipiche di un ordinamento giuridico distinto e indipendente da quelli statali, cui è di fatto impossibile imporre obblighi che verosimilmente non si è in grado di far rispettare. Il mondo di Internet ha formato le sue regole, di cui le piattaforme digitali sono sia i costituenti che i destinatari. In virtù di una autolegittimazione di fatto, ottenuta sul mercato transnazionale, esse sono i veri interlocutori con cui gli Stati devono fare i conti. Il problema non è dunque (solo) quello

[164] A. MANEGGIA, *La giurisdizione negli spazi marini non sottoposti a sovranità territoriale*, Padova, 2018.

[165] G. FERRAINO, *Big Tech, tra Microsoft e Google è guerra aperta*, in *Corriere della Sera*, 14 marzo 2021.

[166] Sul rischio di balcanizzazione di Internet, V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso* Schrems, cit., p. 13 s.

di affermare i diritti, quanto piuttosto quello di assicurare che, in una situazione di progressiva privatizzazione[167] della tutela dei dati personali, coloro cui di fatto è affidata la loro protezione acconsentano a farlo. I rapporti di forza fra gli Stati e le grandi piattaforme che popolano Internet, purtroppo, si sono rovesciati, finendo i primi per subire una gestione privatistica del ciberspazio da parte delle seconde.

Occorre allora ricercare, in prima battuta, una nuova via che non può che essere quella di una regolamentazione che raccolga il consenso degli Stati, sempre che questi siano ancora in grado di imporla ai nuovi Moloch, perché da potenziali demoni divengano angeli protettori di quei valori della persona che noi riteniamo fondamentali, ma che non necessariamente sono tali in quel nuovo ordinamento transnazionale che si viene man mano a creare su Internet. Diversamente non si potrà fare a meno di coinvolgere nella negoziazione delle nuove regole anche tali imprese transnazionali che saranno ben liete di partecipare, forti della legittimazione così ottenuta. Il progressivo imporsi nel diritto internazionale di soggetti non statali, le imprese multinazionali, cui è riconosciuta una pur non completa, quindi speciale, personalità giuridica internazionale è un fenomeno ben noto in dottrina[168], che vi ha scorto un effetto della avvenuta globalizzazione[169] delle relazioni economiche e di cui è stato considerato soprattutto il profilo della responsabilità per violazione dei diritti umani. Ne conseguono sia lo spostarsi del potere reale al di fuori prima dello Stato e poi dell'Unione, con un depotenziamento della nozione stessa di «sovranità», in un sistema di interrelazioni transnazionali «ove un ruolo importante svolgono centri di potere che non possiedono la forma-Stato»[170], sia un progressivo impoverimento delle regole di democrazia su cui si fonda l'Unione[171]. In tale contesto, Internet ha fatto da detonatore perché quello che era un processo in corso divenisse una realtà, in modo talmente rapido che quasi con stupore gli Stati si sono prima resi conto del fenomeno e ora quasi con fastidio cercano di regolarlo, muovendosi con difficoltà in un contesto che sfugge alle normali categorie del diritto.

In questo scenario, apparentemente fantascientifico, ma che tale non è, l'Unione europea sembra aver ora trovato l'energia necessaria per «fare le sue scelte, basate sui

---

[167] In merito alle preoccupazioni suscitate dall'aver affidato agli stessi operatori del mercato digitale il compito, in assenza di una decisione della Commissione, di verificare se il paese terzo garantisca una adeguata tutela dei dati personali, vedi A. CRISTOFANO, *La sentenza Schrems II e il judicial activism della Corte di Giustizia dell'Unione Europea. Verso un GDPR a vocazione universale?*, in *Medialaws*, 15 febbraio 2021, reperibile *online*; nonché, con riguardo alla «questione dell'attribuzione di poteri para-costituzionali a soggetti privati nel mondo digitale», CAGGIANO G., *La proposta*, cit., p. 10.

[168] S.M. CARBONE, *I diritti degli individui e delle imprese nell'evoluzione del diritto internazionale dell'economia: alcuni cenni,* in E. TRIGGIANI, F. CHERUBINI, I. INGRAVALLO, E. NALIN, R. VIRZO (a cura di), *Dialoghi con Ugo Villani*, cit., t. I, pp. 252-259.

[169] C. CARELLA, *La responsabilità giuridica delle multinazionali per violazione dei diritti umani: fata Morgana o vaso di Pandora?*, *ivi*, pp. 261-271.

[170] L. GAROFALO, *È in atto un processo di "costituzionalizzazione" del diritto internazionale? Alcune riflessioni*, *ivi*, t. II, pp. 1205-1212, spec. p. 1208.

[171] E. TRIGGIANI, *Rilegittimare il processo d'integrazione europea*, *ivi*, t. I, pp. 677-684, spec. p. 683.

propri valori, rispettando le proprie regole». Così ha scritto sul suo profilo Twitter la Presidente della Commissione europea, Ursula von der Leyen, rivendicando il ruolo di «un'Europa tecnologicamente sovrana», in occasione della presentazione, il 19 febbraio 2020, della strategia digitale dell'Unione europea. La Presidente ha quindi aggiunto, in generale, che «l'intelligenza artificiale non è buona o cattiva in sé: tutto dipende dal perché e da come viene usata. Consentiamo il miglior uso possibile e controlliamo i rischi che l'intelligenza artificiale può rappresentare per i nostri valori – nessun danno, nessuna discriminazione».

Che si ritorni quindi alla lettera degli artt. 2 e 3 TUE, dal momento che il cammino dei diritti fondamentali nel mondo del *web* potrà proseguire con efficacia, anche ma non esclusivamente nell'ambito dell'Unione europea, solo se e in quanto all'interno di una più ampia regolamentazione comune che trascenda i confini della stessa Unione e sia basata – è questo l'auspicio – sul diritto della stessa Unione[172]. La migliore dimostrazione dell'efficacia del sistema di garanzie dei diritti fondamentali a livello europeo la troviamo nella circostanza che, pur con le sue difficoltà e limiti, esso ha rappresentato uno strumento di positivizzazione e affermazione dei diritti umani a livello, questo sì, mondiale. Per la difesa dei suoi valori, rappresentati nella specie dai diritti fondamentali connessi alla identità digitale, occorre dunque non tanto e non solo uno sforzo regolatorio unilaterale dell'Unione, quanto piuttosto che essa promuova, come auspicato nel Trattato UE, iniziative volte alla definizione sul piano internazionale di strumenti comuni.

A tale auspicio si accompagna l'invito a fare in fretta. Il tempo a disposizione potrebbe essere poco ed occorre agire prima che le varie piattaforme digitali, vere proprie comunità aperte, nel caso di motori di ricerca o di piattaforme di vendita, o chiuse, come i *social networks* o simili, acquistino una forza ed una consapevolezza tale di questo loro potere da accordarsi tra loro per poi imporre agli Stati i loro valori. Sanzioni milionarie, per violazioni vuoi della normativa sulla concorrenza vuoi di quella sulla privacy[173], hanno finora apparentemente evitato che ciò accadesse, rallentando un processo di evoluzione in senso ordinamentale della loro presenza in ambito transnazionale, senza però determinare una inversione di tendenza.

Potremmo in realtà, come inizialmente osservato, essere alla vigilia del riconoscimento di una forma di personalità giuridica transnazionale per tali soggetti. Non ve ne è la sicurezza, o piuttosto, per essere sinceri, non si vuole neppure prendere in considerazione tale suggestione di un mondo, quello del diritto internazionale, in cui opererebbero anche questi attori non statali, realtà indefinite, prive di qualsiasi connotato di democraticità e rappresentatività, non tenute a rispettare diritti che non siano quelli da esse autonomamente riconosciuti. Per contro, non si può certo immaginare che quello

[172] Risoluzione del Parlamento europeo del 12 settembre 2018 sullo stato delle relazioni UE-USA (2017/2271 (INI)), punto 34.

[173] Per tutti, G. BELLITTI, *Big Data e abuso di posizione dominante*, in A. CATRICALÀ, C.E. CAZZATO, F. FIMMANÒ (a cura di), *Diritto antitrust*, Milano, 2021, pp. 472-499.

meramente repressivo e sanzionatorio sia lo strumento idoneo per ottenere una adesione sostanziale ai valori difesi dall'ordinamento dell'Unione. Di certo, ad esempio, una maggiore consapevolezza nelle dichiarazioni di consenso da parte degli interessati alla memorizzazione delle informazioni relative ai dati personali tramite l'installazione di marcatori (*cookies*)[174] potrebbe essere già un significativo passo avanti nel circoscrivere l'invadenza dei signori di Internet.

A questo punto però si possono solo esprimere dubbi e formulare ipotesi, nel convincimento, da un lato, che il mondo virtuale è di fatto sempre più reale e per di più sempre più affollato e che, dall'altro, il vero vuoto è semmai quello normativo in cui le piattaforme digitali stanno costruendo, nel silenzio, si spera non complice, degli Stati, un loro distinto ed originale ordinamento giuridico. Il governo di uno spazio richiede certamente che si determini un catalogo con l'individuazione e l'affermazione di diritti individuali, ma anche con la specificazione di obblighi, regole, rimedi per risolvere le eventuali controversie. Da questo punto di vista, da una prospettiva internazionale, siamo ancora molto lontani anche solo da una loro definizione, per quanto embrionale. Molto si parla, ad esempio, in questo periodo dell'intelligenza artificiale e della sua etica, senza peraltro che vi sia ancora chiarezza sui criteri da adottare. Il problema diviene in tal modo epistemologico ed investe la natura della conoscenza prodotta dalla intelligenza artificiale, in un dibattito i cui contorni divengono talmente sfumati da far sorgere il rischio che dall'impossibilità di certezze la lobby delle piattaforme tragga la forza per opporsi anche agli sforzi, ancora timidi, della Commissione che di tali temi si è occupata nel suo documento strategico del febbraio 2020[175].

In tale contesto, è difficile se non impossibile immaginare reali strumenti di tutela dei diritti connessi all'identità digitale, che rischiano così di rimanere mere affermazioni, se non si interviene *ex ante*, nel momento in cui ciascuno di noi acconsente inizialmente all'uso dei propri dati, spesso con una leggerezza colpevole, cui solo una maggiore consapevolezza potrebbe porre rimedio. La strada che l'Unione intende percorrere è dunque diversa da quella che da sempre hanno imboccato gli Stati Uniti, in una contrapposizione ideologica di cui purtroppo gli unici a trarre beneficio sono i grandi operatori digitali. Il modello europeo è basato sui diritti fondamentali, cui è riconosciuta una applicazione orizzontale, e un ruolo assiologicamente sovraordinato è riservato alla tutela della *data privacy*; nel modello statunitense l'ordine è rovesciato, a favore dell'iniziativa economica e della libertà contrattuale. Se dunque in Europa si assiste alla ricerca di un difficile bilanciamento che abbraccia tanto il settore privato quanto quello

[174] Sull'utilizzo dei *cookies* e sull'espressione del relativo consenso vedi la sentenza della Corte di giustizia *Planet49*, cit.

[175] Libro Bianco sull'intelligenza artificiale, 19 febbraio 2020, cit. Per uno studio dei problemi posti sul piano etico dalla intelligenza artificiale, si vadano, per tutti, le conclusioni del gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018, *Orientamento etici per un'IA affidabile*, dell'8 aprile 2019, reperibile *online*.

pubblico, negli Stati Uniti[176], sull'assunto che le minacce alla riservatezza dell'individuo possano pervenire solo dal potere pubblico, il settore privato è sostanzialmente rimesso per la sua disciplina alla potestà auto regolatoria dei privati stessi, o comunque a regole lasche e non coordinate, anche se una possibile inversione di tendenza pare prospettarsi negli ultimi tempi.

Come indicato nel Libro Bianco del 19 febbraio 2020, l'Unione non rinuncia a perseguire i propri valori mediante la conclusione di accordi internazionali o il progressivo ravvicinamento delle legislazioni dei vari paesi a quella europea, che si pone come modello virtuoso, demandando alla logica dei diritti ciò che non si riesce a compiere attraverso la forza della politica. Forse, in realtà, quest'ultima via può risultare la più proficua per giungere ad una positivizzazione e generalizzazione dei diritti di Internet ai fini di una loro regolamentazione su scala globale. Le affermazioni da parte dei vari signori del *web*, Google piuttosto che Facebook od Apple, di voler rispettare i diritti sanciti dalle norme europee sulla privacy[177] dimostrano, infatti, quanto l'osservanza delle regole dettate dall'Unione sia divenuta talmente importante per l'operare di tali soggetti, da indurli ad autoregolarsi aderendo volontariamente al modello europeo. Non è possibile sapere se tali affermazioni esprimano una effettiva volontà di cambiamento, o non siano piuttosto un modo di "guadagnare" tempo in attesa che si chiariscano i rapporti di forza. Certamente, ove alle parole seguissero i fatti, si tratterebbe in tal caso di un prodotto del c.d. effetto Brussels, più volte evocato, e quindi di una vittoria non solo morale dell'Unione, i cui valori hanno una forza ben maggiore di quella politica normalmente riconosciuta alla stessa Unione. Altrettanto certamente, in questo modo l'Europa riaffermerebbe la propria «sovranità tecnologica», in campo digitale, ovvero la capacità che essa ha di compiere, anche in questo ambito, «le proprie scelte, sulla base dei propri valori e nel rispetto delle proprie regole»[178].

[176] G. RESTA, *La sorveglianza elettronica*, cit., p. 36 s.

[177] K. IRION, *Remarks*, in *Proceedings of the ASIL Annual Meeting*, reperibile *online*, dove l'autrice si interroga sulla serietà della volontà espressa dal Mark Zuckerberg di «adapt the GDPR […] for the entire world».

[178] Così U. VON DER LEYEN, *La via europea al digitale passa dai diritti dei cittadini*, in *Il Sole 24 Ore*, 19 febbraio 2020, p. 16, reperibile *online*.

ABSTRACT: Oggetto del lavoro è il rapporto sempre più conflittuale tra i giganti di Internet e l'Unione europea con riguardo alla protezione dei diritti digitali, tra cui la stessa identità digitale, riconosciuti e tutelati in quanto diritti fondamentali della persona. L'esigenza di salvaguardare tali diritti giustifica l'efficacia extraterritoriale delle norme dell'Unione europea. La ricostruzione della giurisprudenza della Corte di giustizia mostra tuttavia l'insufficienza degli strumenti tradizionali di tutela e come la soluzione vada ricercata sul piano del diritto internazionale, senza con ciò escludere che la legislazione europea possa divenire, in virtù del c.d. effetto Brussels, modello per altri sistemi giuridici.

PAROLE CHIAVE: protezione dei dati; ciberspazio; diritti fondamentali della persona; efficacia extraterritoriale del diritto dell'Unione europea; effetto Brussels.

Multinational corporations, personal data protection in the cyberspace and the extraterritorial effect of European Union law

ABSTRACT: The paper addresses the increasingly conflicting relationship between the Internet giants and the European Union in relation to the protection of digital rights, among which the digital identity itself, recognised and protected as fundamental human rights. The need to guarantee these rights provides justification to the extraterritorial effect of EU law provisions. The analysis of the case law of the Court of Justice of the EU shows, however, the inadequacy of traditional instruments for protection and that the solution must be found from the perspective of international law, without ruling out that the EU legislation may serve as a model for other legal systems by means of the so-called Brussels effect.

KEYWORDS: data protection; cyberspace; fundamental human rights; extraterritorial effect of EU law; Brussels effect.

Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme *online* e tutela dei diritti fondamentali nel quadro del *Digital Service Act* e della co-regolamentazione

Giandonato Caggiano*

SOMMARIO: 1. Introduzione. – 2. Inquadramento della regolazione del fenomeno sul binario della regolamentazione e della autoregolazione. – 3. La definizione dei concetti di moderazione e disinformazione. – 4. Dai "termini di servizio della Comunità" al carattere pubblicistico delle attività e il ruolo para-costituzionale delle piattaforme *online*. – 5. Libertà di espressione e social network. – 6. La responsabilità del provider nel *Digital Service Act*. – 7. *Segue*: i nuovi obblighi di trasparenza delle "grandi piattaforme *online*". – 8. Il Codice di buone pratiche contro la disinformazione (2018) e il Piano di azione per la democrazia (2020). – 9. La previsione di codici di condotta e la co-regolazione nel DSA. – 10. La proposta di un Codice "rivisto e rafforzato" contro la disinformazione nel quadro giuridico del DSA. – 11. Le indicazioni della Commissione per il nuovo Codice. – 12. Conclusioni.

1. Introduzione.

Nell'ambito del pacchetto legislativo su servizi e piattaforme digitali nel Mercato Unico digitale[1], la proposta di *regolamento relativo a un mercato unico dei servizi* (legge sui servizi digitali, DSA)[2] affronta, tra l'altro, la questione della «moderazione dei contenuti o informazioni illegali *online*».

* Già Professore ordinario di Diritto dell'Unione europea, Università degli Studi di Roma Tre.

[1] Sullo stato di avanzamento dell'armonizzazione legislativa, v. G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, in *Eurojus.it*, *Suppl.* 2020, p. 13 ss. Sul piano di azione della Commissione per il digitale, v. COM(2020) 67 final, 19.2.2020, Plasmare il futuro digitale dell'Europa.

[2] La necessità di riforme e le principali soluzioni erano già state individuate dalla Commissione europea, COM(2017) 555 final, 28.9.2017, Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online

Il pacchetto dei servizi digitali comprende ad oggi tre proposte di regolamento: la legge sui servizi digitali (DSA), la Legge sui mercati digitali (DMA), l'Atto sulla governance dei dati (DGA). Per la prima proposta, v. COM(2020) 825 final del 15 dicembre 2020, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (DSA); EDPB Opinion 1/2021 on the Proposal for a Digital Services Act, 10 febbraio 2021. Per un'analisi complessiva, v. G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post* di AISDUE, III (2021), *Focus "Servizi e piattaforme digitali*, 2021, p. 1 ss., reperibile *online*.

Sulla seconda proposta (DMA) che definisce e disciplina il ruolo degli intermediari soprattutto nella prospettiva della concorrenza, v. COM(2020) 842 final del 15 dicembre 2020, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (Legge sui mercati digitali); per un'analisi, v. P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in *Post AISDUE, Focus "Servizi e Piattaforme digitali"*, 2021, p. 30 ss., reperibile

La comunicazione tramite *social media* (*social network*, *social*) coinvolge milioni di cittadini dell'Unione, superando ormai la diffusione e le risorse pubblicitarie dei media tradizionali (stampa, televisione e radio)[3]. In quest'ultimo ambito, le agenzie di comunicazione e i giornalisti professionisti filtrano le notizie, garantendone qualità e affidabilità, mentre nei social media sono gli stessi utenti a produrre e condividere le notizie.

La comunicazione sulle piattaforme-social *online* esclude la diffusione unidirezionale della televisione e della radio (diffusione da punto a multi-punto), difettando pertanto dei meccanismi di controllo, di selezione dei contenuti e/o delle barriere tecnico- economiche all'esercizio dell'attività che incombono sugli editori. Il fenomeno della miriade di contenuti creati e postati da parte degli utenti non sarebbe tecnicamente sostenibile se i *service provider* avessero l'onere di una responsabilità editoriale, anche vagamente assimilabile a quella dei media tradizionali. A tale evidenza, occorre aggiungere che i servizi digitali a copertura quasi-mondiale si confrontano con sfide senza precedenti nell'analisi contestuale e culturale da applicare a contenuti in formati diversi (testo, immagini, video o audio) e relativi a qualsiasi argomento in qualsiasi lingua.

Alcune forme di manipolazione delle informazioni non implicano necessariamente lo sfruttamento di notizie false, ma piuttosto un uso strategico dei servizi *social*. Le teorie complottistiche sono spesso costruite in successive operazioni tramite risorse diversificate (siti Web fasulli, media marginali, forum di discussione, blog, ecc.). Tali teorie vengono poi esposte/proposte nei *social media*, con l'aiuto di *account* falsi o *social bot*, al fine di legittimare la narrazione di una tesi o una posizione ideologica estrema o totalmente falsa, potenzialmente dannosa.

In premessa, occorre ricordare che le piattaforme non sono (e non possono essere) neutrali rispetto ai contenuti dei terzi, proprio per il loro "modello di profitto". Infatti, la durata dell'attenzione e il coinvolgimento degli utenti sono quantificabili come una

---

online; G. CONTALDI, *Il DMA* (*Digital Markets Act*) *tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, 2021, p. 292 ss., reperibile *online*.

Sulla terza proposta (DGA), v. COM(2020) 767 final del 25 novembre 2020, Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (Atto sulla *governance* dei dati), su cui F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Post di AISDUE, Focus "Servizi e piattaforme digitali"*, 2021, p. 58 ss., reperibile *online*.

[3] *Social media* (o social network o social) indica tecnologie e pratiche su web per condividere contenuti testuali, immagini, audio e video, consentendo la creazione e lo scambio di contenuti generati dagli utenti (*user-generated content* o *consumer-generated media*). Tante sono le statistiche consultabili sul mix di fonti di informazione nel mondo, ma basta sottolineare che la metà di colori che hanno uno *smartphone* vi ricercano le notizie e che vi è stato il sorpasso fra risorse pubblicitarie destinate ai new media rispetto ai media tradizionali. A livello mondiale sono 4,20 miliardi gli utenti delle piattaforme social; almeno sei le piattaforme social che contano oltre un miliardo di utenti attivi su base mensile, e quasi una ventina quelle che vedono oltre 300 milioni di utenti attivi ogni mese, cfr. Global Report Digital 2021, prodotto da We are social (disponibile *online*). Sui vari aspetti delle piattaforme digitali, v. il sito dell'Observatory on the Online Platform Economy, istituito da Commission Decision, C(2018) 2393 final del 26 aprile 2018.

risorsa economica che determina il profitto delle piattaforme. Pertanto, i *social media* e i motori di ricerca curano i propri *feed* di notizie e i risultati di ricerca per determinare argomenti di tendenza e/o contenuti raccomandati, "amplificando" i contenuti a carattere sensazionale[4].

2. Inquadramento della regolazione del fenomeno sul binario della regolamentazione e della autoregolazione.

Nonostante l'incremento del pluralismo delle opinioni, è evidente che l'assenza di verifiche *ex-ante* dei fatti e dell'attendibilità delle informazioni rende più difficile riconoscere le notizie vere da quelle false, con rischi evidenti per la violazione delle libertà di informazione ed il rispetto dei suoi limiti Pertanto, la qualità e sostenibilità dell'ecosistema dei nuovi *media* è strettamente collegato alla definizione di regole e limiti dell'azione delle piattaforme in relazione ai contenuti caricati/postati dagli utenti[5].

Rispetto ai contenuti digitali, le regole e le modalità dell'intervento delle piattaforme sono definiti nei "termini e nelle condizioni di servizio" ai quali gli utenti devono aderire. L'intervento delle principali piattaforme origina per lo più dalla segnalazione da parte di utenti dei contenuti ritenuti inappropriati o, in qualche modo offensivi di cui viene verificata la (in)compatibilità con gli "standard della Community" e, nel caso di valutazione negativa, ne consegue la rimozione a cui non è possibile opporsi, se non con ordini giudiziari in base alla configurazione degli ordinamenti nazionali.

Tuttavia, il controllo esercitato sinora dai gestori delle piattaforme non appare più adeguato al rilievo pubblico della comunicazione sui *social* mentre cresce a livello dell'Unione europea la richiesta e aspettativa di un maggiore livello di responsabilizzazione (*accountability)* delle "piattaforme molto grandi". Appare ormai condivisa la necessità di obblighi di trasparenza della attività delle piattaforme per la moderazione sui contenuti illegali e/o indirizzati alla disinformazione, verificabili anche tramite controllori indipendenti e ricercatori data la necessità di controllo pubblico.

Il DSA rappresenta il contesto giuridico nel quale discutere e approvare gli strumenti per ridurre il rischio di complicità delle piattaforme *online* con i contenuti postati dagli utenti (quando restano neutrali o estranee rispetto ad azioni di

[4] Ad esempio, la tecnica di *click baiting* per catturare l'interesse degli utenti si può considerare a metà strada tra la persuasione e l'inganno. In questa definizione rientra l'utilizzazione di tutti gli elementi capaci di catturare (*hacking*) l'attenzione dell'utente che naviga in rete e portarlo a cliccare sui link predeterminati.

[5] Resta fuori dall'ambito di questo contributo l'utilizzazione da parte delle piattaforme, quali Google o Facebook, delle informazioni dei media tradizionali ai quali sono stati attribuiti i diritti di proprietà intellettuale collaterali o ancillari per la pubblicazione di brevi stringhe di poche parole o segni (*snippets*), v. art. 17 della Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

disinformazione di terzi) o, alternativamente, il "rischio di censura" (quando le medesime adottino misure per rimuovere o bloccare gli account a causa di contenuti ritenuti "legali ma dannosi", basati su "presupposti di fatto" non adeguatamente o erroneamente verificati). In assenza di una regolamentazione sovranazionale nei confronti delle decisioni delle piattaforme *online* sui contenuti illegali o di contrasto della disinformazione, esse hanno seguito le proprie politiche di profitto nella generale e diffusa convinzione che il *laissez-faire* ad ogni loro azione sarebbe stato tollerato quale compensazione dei progressi sul piano dell'innovazione.

Accanto agli sviluppi normativi e istituzionali del DSA, l'approccio della Commissione verso la disinformazione continua a rafforzarsi e articolare con gli strumenti di soft law e della co-regolamentazione, nel quasi-contemporaneo Piano d'azione a sostegno della democrazia europea (EDAP) che dedica ampio spazio alla questione in parola, specialmente a livello politico ed elettorale[6]. La rivoluzione digitale ha trasformato le forme di partecipazione alla vita democratica, dimostrando la vulnerabilità dell'opinione pubblica alle azioni di manipolazione, tramite la profilazione e le tecniche di *microtargeting* degli elettori. In mancanza di regole vincolanti al riguardo, le piattaforme possono svolgere un'attività di censura o alternativamente, di complicità, svolgendo in definitiva un ruolo di arbitro della democrazia e dello spazio del dibattito pubblico. In particolare, una specifica centralità assumono i contenuti divulgati in Rete che mettono a rischio i processi elettorali, come evidenziato nel Piano d'azione per la democrazia che sottolinea la necessità di garantire la trasparenza dei messaggi di natura politica e di intraprendere azioni contro i falsi profili e i robot istruiti a tal fine.

In estrema sintesi, si può premettere che la politica dell'Unione in materia appare complessivamente orientata verso un sistema di co-regolamentazione: da un lato, l'armonizzazione legislativa dell'azione contro i contenuti illegali; dall'altro, l'auto-regolamentazione dei soggetti interessati per i contenuti legali ma dannosi, sulla base di "indicazioni" (con aspetti di *soft-law*) della Commissione europea.

3. La definizione dei concetti di moderazione e disinformazione.

Il concetto di "moderazione dei contenuti" comprende: «Le attività svolte dai prestatori di servizi intermediari al fine di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le loro condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o di dette informazioni, quali la loro retrocessione o rimozione o la disabilitazione dell'accesso agli stessi, o sulla capacità dei destinatari di fornire tali informazioni, quali la cessazione o la sospensione dell'account

[6] COM(2020) 790 final del 3 dicembre 2020, sul piano d'azione per la democrazia europea.

di un destinatario del servizio» (art. 2, lett. p), DSA)[7]. Vale la pena di sottolineare che, sulla base di una siffatta definizione, la moderazione dei contenuti da parte dei *social* può essere applicata anche a contenuti legali ma inappropriati, secondo le condizioni generali di una piattaforma (applicate da un algoritmo) oppure solo in un particolare contesto[8].

Per quanto riguarda la definizione "disinformazione" (che non è contenuta nel DSA) si riferisce ad informazioni false o tendenziose, volte ad influenzare e determinare, per motivi politici o di profitto, un danno sulla formazione dell'opinione pubblica e lo svolgimento delle competizioni elettorali[9].

Tale definizione appare ben più precisa e articolata di quella dell'espressione di "notizie false" (*fake news*). Infatti, il bilanciamento fra libertà di espressione e il diritto ad un'informazione appare ugualmente complesso per l'espressione "notizie false" senza la sussistenza di un primo elemento oggettivo (un'informazione falsa) e di un secondo oggettivo (una divulgazione intenzionale)[10].

I rischi legati alla disinformazione sono collegati ad una manipolazione intenzionale dei servizi digitali che normalmente utilizza meccanismi automatizzati. Per il filtro dei contenuti, a seconda del contenuto da analizzare variano le tecnologie, fra cui quelle di *machine learning* (o apprendimento automatico). Tali tecniche consentono un adattamento delle informazioni al profilo personale dell'utente. I fornitori di servizi digitali (in particolare le piattaforme di *social media* e i motori di ricerca) utilizzano sistemi di intelligenza artificiale per "modellare" il flusso dei contenuti *online*, sia nella "cura dei contenuti", sia nella rimozione dei contenuti illegali o "leciti ma dannosi"[11]. A tal fine soccorre una serie di tecniche di amplificazione artificiale dell'informazione, come l'uso di account falsi, social bot, identità rubate, ma occorre tener conto che la

[7] La moderazione è diventata ormai un meccanismo imprescindibile nell'ecosistema digitale. La moderazione non è solo un servizio, ma un costo il cui investimento tecnologico non è possibile sviluppare in autonomia da parte di molte aziende di piccole/medie dimensioni. Spesso, quindi, la soluzione viene demandata a terzi, attraverso contratti di servizi o consulenza.

[8] La leggenda popolare vuole che l'algoritmo di Facebook avesse censurato, nel 2017, la statua di Rodin sul bacio, ispirata ai versi di Dante su Paolo e Francesca, collocata nel Musée Rodin.

[9] Il concetto di disinformazione è collegato ma autonomo rispetto a quello di "fake news", v. European Commission, A multi-dimensional approach to disinformation, Report of the independent High Level Group on Fake News and Online Disinformation, 2018 (reperibile *online*): «all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit». Il DSA contiene invece la definizione dei contenuti illegali: «qualsiasi informazione che, di per sé o mediante riferimento a un'attività, compresa la vendita di prodotti o la prestazione di servizi, non sia conforme al diritto dell'Unione o al diritto di uno Stato membro, indipendentemente dall'oggetto o dalla natura precisa di tale legge» (art. 2 (g)).

[10] La dichiarazione congiunta adottata da ONU, OSCE, Organizzazione degli Stati Americani (OAS) e l'African Commission on Human and Peoples' Rights, Vienna, 3 marzo 2017, afferma che «divieti generici di diffusione delle informazioni basati su fattispecie vaghe e ambigue, incluse quelle relative alle "false notizie" o alle "informazioni non obiettive", sono incompatibili con gli standard internazionali sulle restrizioni della libertà di espressione [...] e dovrebbero essere aboliti» (reperibile *online*).

[11] Nella moderazione dei contenuti, l'intelligenza artificiale (AI) si riferisce all'uso di una varietà di processi automatizzati in diverse fasi; può comprendere diversi concetti, dall'algoritmo" (un software che esegue una serie di istruzioni per i computer che elaborano i dati) all'esecuzione automatica del processo decisionale tramite apprendimento automatico.

disinformazione è un fenomeno complesso e in continuo cambiamento. Il suo impatto sulla comunicazione digitale dipende dall'evoluzione tecnologica, dalle vulnerabilità specifiche delle diverse tipologie dei servizi digitali e dalle strategie e tattiche manipolative.

Nella gestione dei dati digitali, la moderazione dei contenuti illegali si intreccia con l'ordinaria "cura dei contenuti" (*content curation*) che consiste nella pratica di selezionare, dare priorità o consigliare contenuti in base ai profili dei singoli utenti allo scopo di ottimizzare la pubblicità mirata, determinando la visibilità dei contenuti da parte dell'utente sulla base della sua precedente navigazione o alla tracciabilità dei suoi dati su siti web di terzi[12].

Al difficile confine tra contenuti legali e illegali, si collocano i concetti di disinformazione e di cattiva o mala-informazione (o misinformazione, secondo un brutto ma ormai inevitabile neologismo). I due termini distinguono la diffusione di notizie false (*fake news*) al fine di produrre danni in modo intenzionale, da quella realizzata in modo involontario (per superficialità). Nel sistema di informazione *online* radicalmente decentralizzato, i contenuti digitali non veritieri o manipolativi della realtà sono facilmente prodotti e diffusi. La propagazione delle notizie false è determinata dalla dinamica di condivisione (*sharing*) dei social media e dal ruolo di *gatekeepers* delle grandi piattaforme *online*. In tale contesto, azioni di disinformazione e manipolazione possono dar luogo a contenuti potenzialmente dannosi o nocivi per i diritti fondamentali.

Lo sviluppo e l'uso dell'AI ha espanso la raccolta di grandi quantità di dati da parte delle piattaforme che ne fanno il proprio modello di business. Accanto alla revisione umana, l'automazione è utilizzata, sia per la generazione di contenuti da parte di soggetti che svolgono azioni di disinformazione, sia da parte delle piattaforme nella rilevazione proattiva di contenuti dubbi o problematici e nella decisione di rimuovere, etichettare, assegnare priorità. L'utilizzo dell'AI può violare la libertà di espressione, l'accesso all'informazione o il dialogo democratico. Dopo aver applicato un filtro automatico a tutti i contenuti, un successivo intervento manuale/umano può servire per confermare la decisione sul materiale classificato come inappropriato. Nel caso di decisioni errate sui contenuti è fondamentale attuare e rendere disponibili dei meccanismi per il ricorso da parte degli utenti[13].

[12] Al riguardo, si ricorda l'effetto di "bolla autoreferenziale" (*buble filter*) creato dagli algoritmi delle piattaforme che predispongono e inviano, in base alle ricerche effettuate dagli utenti, una selezione di notizie disegnata sulle opinioni personali di ciascuno.

[13] I "Santa Clara Principles on Transparency and Accountability in Content Moderation", adottati dalla Conferenza del 2 febbraio 2018 (reperibili *online*), rappresentano un primo schema di autoregolamentazione che è stato poi seguito anche a livello dell'Unione europea. Nell'aderirvi, le aziende che fanno uso di sistemi automatici di moderazione si impegnano a renderlo pubblico al fine di mantenere una corretta relazione e comunicazione con gli utenti. Tra i vari principi: pubblicare il numero di *post* rimossi e di *account* sospesi a causa di violazioni; assicurare un meccanismo di notifica agli utenti di tali infrazioni e della relativa azione correttiva intrapresa nei loro confronti o del loro contenuto; fornire in ogni

La regolamentazione dell'Unione europea diventa fondamentale per evitare situazioni estreme ed evitare l'applicazione di controlli troppo stringenti o l'insufficienza di filtri automatici o della valutazione umana[14].

4. Dai "termini di servizio della Comunità" al carattere pubblicistico delle attività e il ruolo para-costituzionale delle piattaforme *online*.

Ad oggi, la gestione dei contenuti da parte dei *social media* (piattaforme di *hosting*) implica l'applicazione di "termini e condizioni della comunità" ai contenuti generati dagli utenti al fine di garantire la conformità ai requisiti di legge (contenuti illegali).

È opinione diffusa che i soggetti gestori delle piattaforme *social* (in posizione certamente dominante sui mercati digitali) esercitino al momento dell'accesso degli utenti un potere sostanzialmente pubblicistico, in quanto consentono l'accesso ad un canale di comunicazione indispensabile per raggiungere la maggior parte dell'opinione pubblica. La condizioni generali e i termini di contratto consentono all'utente (contraente debole) solo l'accettazione in blocco. Peraltro, l'assetto totalmente asimmetrico delle situazioni giuridiche soggettive ivi previste è stato concepito dal contraente forte.

A fronte della valenza pubblicistica della loro azione, per ampiezza e incidenza nella vita di tutti, appare incongrua una regolamentazione interna di una comunità legata da "vincoli sociali" assunti al momento della richiesta e dell'accesso/ammissione degli utenti. In linea di principio, quest'ultimi dovrebbero poter concorrere a definire condizioni contrattuali eque per facilitare la condivisione dei propri dati digitali, anche al fine di affrontare gli squilibri del potere di mercato. Del resto, l'asimmetria informativa tra le piattaforme di social media e le autorità pubbliche postula l'introduzione di misure di trasparenza e il riconoscimento del diritto a procedure di ricorso indipendente e giudiziarie al fine di prevenire, garantire e sanzionare le violazioni dei diritti fondamentali.

Al riguardo si è persino parlato dell'attribuzione di poteri para-costituzionali ai motori di ricerca quando la Corte di giustizia, nella sentenza *Google Spain*[15], ha attribuito al motore di ricerca, il ruolo di arbitro del bilanciamento tra diritti fondamentali (bilanciamento fra diritto all'informazione e diritto all'identità personale). L'ambito

caso un meccanismo per appellarsi contro l'azione intrapresa e permettere così una seconda verifica dei contenuti.

[14] P.M. BARRETT, *Who Moderates the Social Media Giants?*", Center for Business and Human Rights, New York, 2020, reperibile *online*; G. SARTOR, A. LOREGGIA, *The impact of algorithms for online content filtering or moderation – Upload filters*, European Parliament, 2020, reperibile *online*.

[15] Corte di giustizia (Grande Sezione), sentenza della 13 maggio 2014, causa C-131/12, *Google Spain*, ECLI:EU:C:2014:317. V. A.L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione "digitale"*, in *Studi sull'integrazione europea*, 2/2015, p. 347 ss.; O. POLLICINO, M. BASSINI, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo?: il ruolo degli Artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Il diritto dell'informazione e dell'informatica*, 2014, p. 569.

territoriale dello svolgimento di tale ruolo per i social network è stato poi ridefinito nella sentenza *Google c. CNIL* e, in relazione alla notizia della condanna per diffamazione, già rimossa in un Paese e riprodotta in altri Paesi, nella sentenza *Glawischnig-Piesczek*[16].

Il DSA procede ad un ridimensionamento di siffatti poteri delle piattaforme tramite la trasparenza delle procedure di rilevamento dei contenuti problematici e di ricorso, l'istituzione di organismi pubblici nazionali e sovranazionali *di controllo sulle loro attività* e il conferimento di specifici poteri esecutivi alla Commissione. Per questa via si riduce, pur senza eliminarla, la tendenza alla delega di funzioni pubbliche alle società private proprietarie delle piattaforme.

5. Libertà di espressione e social network.

Il DSA intende creare un ambiente digitale in coerenza con la protezione dei diritti fondamentali in un mercato unico digitale tramite nuove regole armonizzate e un'architettura istituzionale a livello dell'Unione[17]. La proposta è di grande rilevo politico-istituzionale perché riguarda gli effetti dei servizi digitali sull'esercizio dei diritti fondamentali tutelati dalla Carta, compresi la libertà di espressione e di informazione, il diritto alla vita privata, il diritto alla non discriminazione e i diritti del minore. Tali diritti possono essere messi a rischio tramite la progettazione dei sistemi algoritmici o dall'abuso dei servizi digitali a seguito di notifiche abusive.

L'obiettivo principale del DSA è l'introduzione di un adeguato apparato e di procedure di contrasto ai contenuti illegali online (incitamento all'odio, incitamento alla violenza, informazioni diffamatorie) o attività illegali (ad es. vendita di merci pericolose o contraffatte) che sono oggetto di specifica regolamentazione a livello dell'Unione e nella legislazione nazionale. La Commissione europea afferma che le piattaforme online possono essere «utilizzate in modo tale da influenzare fortemente [...] la formazione dell'opinione pubblica e del discorso» (considerando 56). Una specifica categoria di rischi riguarda la "manipolazione intenzionale e spesso coordinata" del servizio della piattaforma, con effetti prevedibili sulla salute pubblica, sul dibattito civico, sui processi elettorali (…). Tali rischi possono sorgere, ad esempio, dalla creazione di account falsi, dall'uso di bot e da altri comportamenti automatizzati o parzialmente automatizzati (considerando 57).

---

[16] Sentenze *Google Spain*, cit.; del 24 settembre 2019, causa C-507/17, *Google LLC* c. *CNIL*, EU:C:2019: 772; del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig- Piesczek* c. *Facebook Ireland*, EU:C:2019:821. Per un commento v. F. CALOPRISCO, *La Corte di giustizia si esprime sulla portata territoriale dell'obbligo di deindicizzare i dati personali online*, in *Annali Aisdue*, vol. I, 2020, p. 357 ss., reperibile *online*; 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*, 16 ottobre 2019, reperibile *online*.

[17] COM(2020) 825, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali, cit.

Senza definire la nozione di "contenuto legale ma dannoso", il DSA fa espressamente riferimento nei considerando alla disinformazione come uno dei gravi danni che emergono dall'attuale ambiente online e affronta i danni legati alla disinformazione di cui prevede il contrasto combinando prudentemente tre elementi: una serie di requisiti di *due diligence*, una base giuridica per l'autoregolamentazione e meccanismi indipendenti di controllo e controllo pubblico.

Le piattaforme di *social media* consentono ai propri utenti di esprimersi, creare, trasmettere e accedere a informazioni ma conservando il potere di disciplinare i profili degli utenti, determinando così i limiti soggettivi e oggettivi del diritto di espressione e di informazione. Nell'attuale contesto, tali società private possono dunque decidere quali sono i contenuti leciti escludendo alcuni argomenti o determinate immagini e/o dare un'attestazione di "cattiva condotta" a determinati utenti senza il previo accertamento giurisdizionale o amministrativo delle violazioni di leggi e procedure nell'ordinamento nazionale. Spesso, le piattaforme adottano decisioni non-trasparenti e senza motivazioni, procedendo alla rimozione del contenuto o alla cancellazione/sospensione dell'account, grazie al filtro di mezzi automatizzati e/o la valutazione degli operatori umani (moderazione automatica o manuale). Viene attribuito così, ad un potere privato, la decisione fortemente discrezionale su quali contenuti postati dagli utenti possano restare visibili *online*.

Queste caratteristiche dell'azione dei *social media* hanno un evidente impatto sui diritti fondamentali degli utenti. La moderazione dei contenuti persegue un difficile bilanciamento tra libertà di espressione, libertà di informazione e libera prestazione dei servizi tramite l'adozione di obblighi di trasparenza e *due diligence* per gli intermediari *on line* sotto il controllo delle istituzioni degli Stati membri e dell'Unione. Le minacce ai diritti fondamentali tramite le varie possibili tecniche che si concretizzino in azioni di disinformazione possono essere comprese e affrontate tramite accurate indagini e valutazione da parte delle piattaforme stesse, insieme alla predisposizione di misure di trasparenza a favore degli utenti e di ricercatori indipendenti.

Il DSA pone al centro la tutela della libertà di espressione, ivi compresa la protezione dall'interferenza dei governi. La autovalutazione dei rischi sistemici deve comprendere: la diffusione di contenuti illegali; eventuali effetti negativi per l'esercizio dei diritti fondamentali (rispetto della vita privata e familiare, diritto alla libertà di espressione e di informazione, alla non discriminazione e dei diritti del minore, *ex* articoli 7, 11, 21 e 24 della Carta).

In relazione alla libertà di espressione, gli articoli 10 della CEDU e 11 della Carta sono applicabili alle attività dei media *online*[18]. Come affermato negli Orientamenti del

[18] Corte europea dei diritti dell'uomo, sentenza del 5 maggio 2011, ricorso n. 33014/05, *Editorial Board of Pravoye Delo e Shtekel* c. *Ucraina*: «(…) the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit

Consiglio dell'Unione in materia di diritti umani per la libertà di espressione *online* e *offline*[19], le innovazioni nel settore *media* correlate alla tecnologia hanno ampliato la possibilità di diffondere informazioni a un pubblico di massa, rendendo al contempo più pressante l'esigenza di tutela della libertà di espressione nelle attività *online*; in specifico riferimento al bilanciamento con il diritto alla riservatezza e al diritto d'autore, effettuato dalla giurisprudenza della Corte di giustizia e della Corte EDU[20].

Entrambe le norme riconoscono il diritto di espressione, inteso sia come libertà di manifestare, diffondere o divulgare le proprie opinioni e idee con il divieto del potere pubblico di interferire con il suo esercizio (libertà "attiva"), sia come il diritto di accedere alle opinioni altrui (libertà "passiva") da cui derivano il diritto di dare notizie, raccontare fatti ai mezzi di informazione, vale a dire il diritto di cronaca e di critica. Per quanto riguarda le limitazioni e le deroghe alla tutela della libertà di espressione, l'art. 10 CEDU precisa le limitazioni tassative che corrispondono a un "imperativo bisogno sociale" nell'ambito dei principi di proporzionalità e adeguatezza[21]. In altri termini, tali limitazioni devono essere "proporzionate agli scopi legittimi perseguiti" e giustificate dai motivi pertinenti e sufficienti invocati dallo Stato contraente[22]. L'assenza di analoghe limitazioni e deroghe alla libertà di espressione nella Carta dei diritti fondamentali non esclude che

information. The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control».

[19] Consiglio dell'Unione europea, doc. n. 9647/14, Orientamenti dell'UE in materia di diritti umani per la libertà di espressione online e offline, del 12 maggio 2014, reperibili *online*.

[20] La Commissione europea ricorda che "I contenuti legali, anche quelli presunti dannosi, sono generalmente tutelati dalla libertà di espressione e devono essere gestiti in maniera diversa rispetto ai contenuti illegali, per i quali la rimozione del contenuto stesso può essere giustificata. Come ha sottolineato la Corte europea dei diritti dell'uomo, ciò è particolarmente importante quando si parla di elezioni" COM (2018) 236 final, cit., par. 2.1. Per un inquadramento generale, v. B. NASCIMBENE, F. ROSSI DAL POZZO, *L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea e orientamenti giurisprudenziali*, in *Eurojus.it*, 4/2019, p. 132 ss., reperibile *online*. V. anche P. DE SENA, M. CASTELLANETA, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su Casapound c. Facebook*, in *SidiBlog* 20 gennaio 2020, reperibile *online*; O. POLLICINO, *Freedom of Expression and the European Approach to Disinformation and HateSpeech: The Implication of the Technological Factor*, in *Liber Amicorum per Pasquale Costanzo*, 2020, p. 9 ss.; M. BASSINI, *Internet e libertà di espressione*, Roma, 2019; V. SALVATORE, *L'Unione Europea. La libertà di espressione, una prospettiva di diritto comparato*, Parlamento europeo, Bruxelles, 2019, reperibile *online*.

[21] Le misure restrittive devono essere necessarie in una società democratica per garantire la protezione dell'interesse generale o la protezione di diritti individuali confliggenti, ovvero: la sicurezza nazionale; l'integrità territoriale; la pubblica sicurezza e l'ordine pubblico; la prevenzione dei reati; la protezione della salute; la protezione della morale; la protezione della reputazione o dei diritti altrui (ad es. la tutela della riservatezza; il divieto di divulgazione di informazioni confidenziali; la garanzia dell'autorità e imparzialità del potere giudiziario

[22] Sull'art. 11 della Carta, v. R. MASTROIANNI, G. STROZZI, *Art. 11 Libertà di espressione e di informazione*, in R. MASTROIANNI et AL. (a cura di), *Commentario alla Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 219 ss.; P. PIRODDI, *Commento all'art. 11 della Carta dei diritti fondamentali dell'Unione europea*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, 2ª ed., Padova, 2014, p. 1693 ss.

vengano in rilievo sulla base della regola generale di cui agli articoli 52, paragrafi 3[23] e 1 della Carta[24].

Nella sentenza *Funke Medien,* la Corte di giustizia ha sottolineato che al fine di effettuare un bilanciamento fra interesse dei titolari dei diritti d'autore e la tutela degli interessi e dei diritti fondamentali degli utenti di accedere ai materiali protetti, deve tenersi conto della «circostanza che il tipo di "discorso" o di informazione di cui trattasi rivesta un'importanza particolare, segnatamente nell'ambito del dibattito politico o di un dibattito che tocca l'interesse generale»[25]. Con la parallela sentenza *Spiegel online*, la Corte osserva che «i collegamenti ipertestuali contribuiscono al buon funzionamento di Internet, che riveste un'importanza particolare per la libertà di espressione e di informazione, garantita dall'articolo 11 della Carta, nonché allo scambio di opinioni e di informazioni in tale rete, caratterizzata dalla disponibilità di innumerevoli quantità di informazioni»[26].

6. La responsabilità del provider nel *Digital Service Act.*

La direttiva e-commerce 2000/31/CE dell'8 giugno 2000, che pure ha svolto un ruolo determinante per lo sviluppo dell'economia digitale, non appare più adeguata alla dimensione economica e al potere sui mercati digitali delle più grandi piattaforme. In relazione ai contenuti e alle informazioni online, il processo di armonizzazione legislativa non è agevole, considerata la divisione delle competenze in materia di diritti fondamentali fra Unione europea e Stati membri e la resistenza di questi ultimi ad ampliare l'ambito di applicazione della Carta dei diritti fondamentali. Ancor più problematico l'attribuzione a livello sovranazionale di alcune misure esecutive di controllo ed *enforcement* che sono attualmente nella competenza verticale degli Stati membri.

Il DSA propone importanti regole sulla trasparenza delle decisioni delle piattaforme sulla moderazione dei contenuti. Soprattutto, per le piattaforme molto grandi, gli utenti

[23] La Carta contiene diritti corrispondenti a quelli garantiti dalla CEDU, «senza che ciò pregiudichi l'autonomia del diritto dell'Unione e della Corte di giustizia dell'Unione europea».

[24] v. Corte di giustizia, sentenza del 4 maggio 2016, causa C-547/14, *Philip Morris Brands*, EU:C:2016:325, punto 149. In argomento v. R. CISOTTA, *Brevi note sulla giurisprudenza sull'art. 52, par. 1 della carta dei diritti fondamentali dell'UE in materia di limitazioni ai diritti fondamentali …con uno sguardo in avanti*, in *Osservatorio sulle fonti*, 2021, p. 19 ss., reperibile *online*; F. FERRARO, N. LAZZERINI, *Commento all'art. 52*, in R. MASTROIANNI et AL (a cura di), *Commentario alla Carta*, cit., p. 1061 ss., spec. p. 1063; P. MORI, *La "qualità" della legge e la clausola generale di limitazione dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE*, in *Il Diritto dell'Unione Europea*, fasc. 2, 2014, p. 243; P. MANZINI, *La portata dei diritti garantiti dalla Carta dell'Unione europea: problemi interpretativi posti dall'art. 52*, in L. S. ROSSI, (a cura di), *Carta dei diritti fondamentali e Costituzione europea*, Milano, 2002, p. 127 ss.

[25] Corte di giustizia, sentenza del 29 luglio 2019, causa C-469/17, *Funke Medien*, EU:C:2019:623.

[26] Corte di giustizia, sentenza del 29 luglio 2019, causa C-516/17, *Spiegel Online*, EU:C:2019:625. Per un commento, v. S. GARBEN, *Fundamental rights in EU copyright harmonization: Balancing without a solid framework: Funke Medien, Pelham, Spiegel Online*, in *Common Market Law Review*, 2020, p. 1909 ss.

potranno avere una migliore comprensione del modo di operare attraverso rapporti di audit e ricerche indipendenti. Attraverso le regole proposte su come le piattaforme moderano i contenuti, sulla pubblicità, sui processi algoritmici e sulla mitigazione del rischio, mirerà a garantire che le piattaforme - e in particolare quelle molto grandi - siano più responsabili e si assumano la responsabilità delle azioni che intraprendono e del sistema rischi che comportano, compresa la disinformazione.

Per ottenere un livello di collaborazione fra i vari attori coinvolti, il DSA non accresce la soglia di responsabilità delle piattaforme di *hosting service*, attualmente prevista dalla direttiva *e-commerce*, secondo cui i prestatori intermediari di servizi non sono responsabili dei contenuti che ospitano purché mantengano al riguardo un comportamento di rigorosa passività, intervenendo solo per rimuovere i contenuti illeciti[27]. La giurisprudenza della Corte di giustizia aiuta a tracciare il limite dell'intervento che gli intermediari possono operare sui contenuti che trasmettono, conservano o ospitano, oltre il quale perdono il beneficio dell'esenzione dalla responsabilità.

Per contrastare informazioni/contenuti falsi e fuorvianti, il DSA contiene disposizioni sulla trasparenza a tutela dei diritti di espressione e di informazione tramite obblighi di *due diligence* per le "piattaforme online molto grandi"[28]; un inquadramento giuridico dei codici auto-regolamentari settoriali, meccanismi di controllo pubblico, una maggiore trasparenza nell'uso degli algoritmi di classificazione e raccomandazione.

La soluzione regolamentare verso un migliore equilibrio degli interessi in gioco consiste l'adozione di misure asimmetriche con obblighi più rigorosi per le piattaforme online di dimensioni molto grandi, insieme a precisazioni sul regime di responsabilità per gli intermediari *online* ed al potenziamento della sorveglianza e dell'applicazione delle norme.

Il DSA intende conferire maggiori poteri agli utenti per la tutela dei loro diritti fondamentali online, istituire una vigilanza efficace sui servizi digitali e una collaborazione tra le autorità. In generale, il DSA prevede l'armonizzazione di una serie di nuovi obblighi per i soggetti che erogano i servizi digitali, quali la rimozione di beni, servizi o contenuti illegali online; le garanzie per gli utenti i cui contenuti siano stati rimossi; nuove misure basate sul rischio al fine di prevenire abusi (solo per piattaforme di grandi dimensioni); nuove misure di trasparenza, anche per quanto riguarda la pubblicità online e l'utilizzo degli algoritmi per consigliare/indirizzare gli utenti verso i

[27] Un servizio di hosting è un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio. Tale categoria può comprendere diverse tipologie dai mercati online, le piattaforme di condivisione di video, i social network, i siti web di blogging o i siti web di recensioni, fino alle sezioni dei commenti degli utenti sulle pagine delle notizie.

[28] Servizi che raggiungono 45 milioni di utenti mensili attivi nell'UE, o il 10% della popolazione dell'UE.

contenuti; nuovi poteri di verifica del funzionamento delle piattaforme, anche tramite l'accesso di ricercatori qualificati.

La proposta non modifica il principio della direttiva sul commercio elettronico secondo cui i prestatori di servizi (intermediari) online non sono responsabili della trasmissione e dell'archiviazione di informazioni originate dagli utenti, a meno che non abbiano l'effettiva conoscenza dei contenuti illeciti e, in tal caso, non agiscano rapidamente per rimuoverli (articoli da 3 a 5). La circostanza che l'intermediario svolga indagini di propria iniziativa al fine di individuare e rimuovere contenuti illegali non pregiudica il suo status di ampia esenzione di responsabilità rispetto ai contenuti postati dagli utenti (art. 6). In ogni caso, i fornitori di servizi non sono soggetti ad alcun obbligo generale di monitoraggio in relazione alle informazioni trasmesse o archiviate nella prestazione dei loro servizi (art. 7). Il DSA subordina però tale esenzione di responsabilità a una serie di obblighi di *due diligence* (meccanismi di rilevamento, azioni correttive e procedure di rinvio), corrispondenti e proporzionate alle dimensioni degli intermediari e alla natura dei servizi forniti. In particolare, le piattaforme online molto grandi sono soggette a condizioni più rigorose a causa dell'impatto sociale più elevato. In questo quadro sono integrati adeguati procedure e controlli, compreso un sistema interno di trattamento dei reclami e procedure di ricorso extragiudiziale. Ciò al fine di garantire che i diritti fondamentali, in particolare la libertà di espressione, siano debitamente tutelati nel caso in cui le piattaforme rimuovessero contenuti legittimi e disabilitassero gli account. Alle autorità nazionali e alla Commissione sono conferiti ampi poteri investigativi ed esecutivi con caratteristiche simili a quelle delle indagini antitrust, ivi compreso il potere di imporre multe, per perseguire i casi di non conformità alle disposizioni regolamentari.

Il DSA riprende i medesimi criteri che determinano la responsabilità degli intermediari secondo la direttiva e-commerce, cioè l'"effettiva conoscenza" delle violazioni segnalate dagli aventi diritto, ma cerca di eliminare i disincentivi esistenti nei confronti delle indagini volontarie di propria iniziativa intraprese dai prestatori di servizi di intermediazione (art. 6)[29]. È confermato l'obbligo generale di monitoraggio o un obbligo attivo di accertamento dei fatti, né un obbligo generale per i fornitori di adottare misure proattive in relazione a contenuti illegali (art. 7), fatte salve eventuali ingiunzioni contro determinati contenuti illegali, emessi dalle competenti autorità nazionali o giudiziarie ai sensi (art. 8). Tale esenzione non pregiudica la possibilità per i giudici o le autorità amministrative nazionali di esigere dal prestatore di servizi di hosting di porre

[29] «Art. 6, Indagini volontarie promosse di propria iniziativa e rispetto degli obblighi normativi: I prestatori di servizi intermediari non sono considerati inammissibili all'esenzione dalla responsabilità (…) per il solo fatto di svolgere indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione, comprese quelle stabilite nel presente regolamento».

fine ad una violazione o di impedirla, anche rimuovendo le informazioni illecite o disabilitando l'accesso alle medesime (considerando 45). La proposta conferisce agli utenti e ai consumatori la possibilità di contestare le decisioni prese dalle piattaforme online per rimuovere il loro contenuto, anche quando tali decisioni si basano sui termini e sulle condizioni delle piattaforme. Gli utenti possono presentare reclamo direttamente alla piattaforma, scegliere un organo di risoluzione extragiudiziale delle controversie o chiedere un risarcimento in tribunale. La proposta introduce il contraddittorio degli utenti nei confronti delle decisioni tramite procedure extragiudiziali e reclami interni per consentire la protezione dei diritti fondamentali *online*[30]. Un prestatore di servizi di hosting può essere destinatario di ingiunzioni emesse in base al diritto nazionale di uno Stato membro, anche se soddisfa una delle condizioni alternative, vale a dire anche nell'ipotesi in cui non sia considerato responsabile[31].

7. *Segue*: i nuovi obblighi di trasparenza delle "grandi piattaforme *online*".

Un ulteriore tema riguarda la conoscibilità e la trasparenza dei dati dei soggetti esercenti i servizi digitali, anche i nominativi dei fornitori delle inserzioni pubblicitarie, essendo altresì imposto alle grandi piattaforme l'obbligo di svolgere attività di "risk assessment" e di adottare misure atte volte a proteggere i consumatori dai contenuti illeciti. Per la pubblicità online, compresa la pubblicità politica., tutte le piattaforme online - grandi o piccole - che visualizzano annunci pubblicitari sulle loro interfacce sono obbligate a garantire che ogni annuncio sia etichettato come tale e a identificare gli sponsor e i criteri di targeting utilizzati per ogni singolo destinatario (art. 24).

In questo senso, il DSA riduce l'attuale potere discrezionale delle piattaforme, introducendo la previsione di "segnalatori attendibili" (*Trusted Flaggers*) da parte del Coordinatore dei servizi che può revocarli a determinate condizioni (art. 19). Resta di difficile comprensione perché gli esperti eleggibili a questo ruolo debbano rappresentare "interessi collettivi" oltre che essere indipendenti da qualsiasi piattaforma online (ivi, par. 2 lett. c).

---

[30] E.M. MAZZOLI, *Online content governance: Towards a framework for analysis for prominence and discoverability*, in *Journal of Digital Media & Policy*, 2020, pp. 301-319; R. GORWA, R. BINNS, C. KATZENBACH, *Algorithmic content moderation: Technical and political challenges in the automation of platform governa*nce, in *Big Data and Society*, 2020, pp. 1-15, reperibile *online*; T. GILLESPIE, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven & London, 2018.

[31] Sentenza *Eva Glawischnig-Piesczek*,cit. Ne consegue che, come rilevato dall'Avvocato generale Szpunar nelle conclusioni della medesima causa (presentate il 4 giugno 2019, EU:C:2019:458, punto 32): «(…), risulta dall'articolo 14, paragrafo 3, della direttiva 2000/31 che l'immunità accordata ad un prestatore intermediario non osta a che un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, esiga che tale prestatore ponga fine ad una violazione o la impedisca. Discende da tale disposizione che un prestatore intermediario può essere il destinatario di ingiunzioni, anche se, secondo le condizioni enunciate all'articolo 14, paragrafo 1, di tale direttiva, detto prestatore non è esso stesso responsabile delle informazioni memorizzate sui suoi server».

La proposta si concentra sulla correzione delle vulnerabilità delle piattaforme contro la manipolazione al fine di amplificare comportamenti dannosi, che danneggia i gruppi vulnerabili. Un approccio basato sul rischio obbligherà piattaforme molto grandi a valutare e mitigare i rischi che i loro meccanismi comportano, anche per proteggere i diritti fondamentali, gli interessi pubblici, la salute pubblica e la sicurezza, e di sottoporre le loro valutazioni e misure a un audit indipendente. Inoltre, al fine di prevenire rischio sistemico, impone ai VLOP di «mettere in atto misure di mitigazione ragionevoli, proporzionate ed efficaci» (art. 27). Tali misure possono includere aggiustamenti alla moderazione dei contenuti o ai sistemi di raccomandazione, adattamenti ai termini e alle condizioni del servizio, restrizioni alla visualizzazione di annunci sulle interfacce online dei servizi, il rafforzamento dei processi di sicurezza interna e la partecipazione a codici di condotta.

Il DSA aumenta la trasparenza dei sistemi di raccomandazione riducendo così i rischi per gli utenti di essere selettivamente esposti ai contenuti promossi dagli algoritmi della piattaforma e catturati in bolle di filtro (art. 29)[32]. In particolare, obbliga le piattaforme molto grandi a «esporre nei loro termini e condizioni, in modo chiaro, accessibile e facilmente comprensibile, i parametri principali utilizzati nei loro sistemi di raccomandazione» e fornire agli utenti le opzioni «per modificare o influenzare tali parametri principali includendo almeno un'opzione che non si basi sulla profilazione»[33].

Inoltre, tali piattaforme devono conservare archivi dedicati di tutti gli annunci visualizzati sulle loro interfacce online, renderli pubblicamente accessibili durante un anno e consentire l'identificazione degli sponsor, i parametri utilizzati per indirizzare specifici gruppi di destinatari e il coinvolgimento degli utenti aggregati (art. 30).

La autovalutazione dei rischi sistemici deve comprendere: la diffusione di contenuti illegali; eventuali effetti negativi per l'esercizio dei diritti fondamentali; la "manipolazione intenzionale del servizio", anche mediante "un uso non-autentico o uno sfruttamento automatizzato del servizio", con ripercussioni negative sulla tutela della salute pubblica, dei minori, del dibattito civico o con effetti sui processi elettorali e sulla sicurezza pubblica (art. 26 DSA).

Al riguardo, l'accesso ai dati delle piattaforme ai ricercatori abilitati (per contribuire all'individuazione e alla comprensione dei rischi sistemici) è subordinato a una richiesta

[32] Espressione coniata da Eli Pariser nel suo saggio *The Filter Bubble: What the Internet Is Hiding from You* (2011).

[33] «Art. 29, Sistemi di raccomandazione: 1.Le piattaforme online di dimensioni molto grandi che si avvalgono di sistemi di raccomandazione specificano nelle loro condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione che possano avere messo a disposizione dei destinatari del servizio per consentire loro di modificare o influenzare tali parametri principali, compresa almeno un'opzione non basata sulla profilazione ai sensi dell'articolo 4, punto 4), del regolamento (UE) 2016/679».

del coordinatore del servizio digitale dello Stato membro di stabilimento (nella maggior parte dei casi l'Irlanda) (art. 31)[34].

Inoltre, la proposta definisce un quadro di co-regolamentazione in cui i fornitori di servizi possono lavorare secondo codici di condotta per affrontare gli impatti negativi relativi alla diffusione virale di contenuti illegali e attività manipolative e abusive, che sono particolarmente dannose per i destinatari vulnerabili del servizio, come bambini e minori.

8. Il Codice di buone pratiche contro la disinformazione (2018) e il Piano di azione per la democrazia (2020).

Secondo il *Codice di buone pratiche dell'Unione sulla disinformazione*[35], il fenomeno in parola riguarda un'informazione rivelatasi falsa o fuorviante ove sia: a) concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico e b) idonea ad arrecare un "pregiudizio pubblico", inteso come «minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'UE». In negativo la definizione esclude satira e parodia, o notizie e commenti di parte chiaramente identificati (propaganda politica), non pregiudicando gli obblighi di legge e i codici pubblicitari di autoregolamentazione. In sostanza, il Codice inquadra il fenomeno della disinformazione come l'insieme di contenuti falsi e ingannevoli che siano creati, presentati e diffusi per ragioni economiche o politiche e che possano causare minacce ai processi democratici e a determinati beni pubblici (salute, ambiente, sicurezza).

---

[34] Su richiesta motivata del coordinatore dei servizi digitali del luogo di stabilimento o della Commissione, le piattaforme online di dimensioni molto grandi forniscono, entro un termine ragionevole specificato nella richiesta, l'accesso ai dati ai ricercatori abilitati che soddisfano i requisiti di cui al paragrafo 4 del presente articolo, al solo scopo di condurre ricerche che contribuiscano all'individuazione e alla comprensione dei rischi sistemici di cui all'articolo 26, paragrafo 1.

[35] Cfr. il sito https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation; nonché Joint Communication, *Action Plan against Disinformation*, JOIN(2018) 36 final del 5 dicembre 2018; Relazione della Commissione sull'attuazione della comunicazione "Contrastare la disinformazione online: un approccio europeo", COM(2018) 794 final del 5 dicembre 2018; Comunicazione della Commissione, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final del 26 aprile 2018; Report of the independent High Level Expert Group on fake news and online disinformation (chairman Madeleine de Cock Buning), *A multi-dimensional approach to disinformation*, 12 March 2018, reperibile *online*. Sul monitoraggio, v. Assessment of the Code of Practice on Disinformation, Achievements and areas for further improvement, SWD(2020) 180 final del 10 settembre 2020; ERGA Report on disinformation: Assessment of the implementation of the Code of Practice, 4 May 2020, reperibile *online*. Per un commento e i numerosi riferimenti bibliografici, v. G. PAGANO, *Il Code of Practice on Disinformation. Note sulla natura giuridica di un atto misto di autoregolazione*, in *Federalism.it*, n. 11/2019, reperibile *online*; nonché M. MONTI, *La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation), ivi*, 11/2020, reperibile *online*; e P. CESARINI, *Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward*, in *MediaLaws*, 1/2021, p. 288 ss., reperibile *online*.

Nella comunicazione digitale, considerata la possibile confusione fra notizie diffuse dai partiti e notizie di fonte giornalistica assumono particolare valore gli obblighi di trasparenza in relazione ai contenuti politici. Il Codice consiglia un ecosistema da risanare: chiudere gli account falsi, regolare l'uso dei bot, garantire l'integrità del servizio rispetto agli account che diffondono disinformazione; incentivare e dare priorità a informazioni pertinenti, autentiche, accurate e autorevoli; favorire la reperibilità delle fonti autorevoli ed espressione di diversi punti di vista. Il Codice propone quindi alle piattaforme firmatarie un'auto-regolamentazione secondo linee predeterminate dall'Unione. Ciò accresce la loro *accountability* sul tema della libertà di informazione ma ne riconosce, al contempo, un ruolo costituzionale in assenza di forme di regolamentazione, responsabilità editoriale o di controllo da parte di soggetti pubblici (giudici o autorità indipendenti).

A distanza di tre anni dall'entrata in funzione dell'autoregolamentazione, la Commissione europea[36] sottolinea, l'assenza di sistemi di *enforcement* in caso di mancato rispetto degli impegni assunti dalle piattaforme e dagli altri soggetti interessati. Al riguardo, la Commissione evidenzia che nel Codice «there is no requirement for compliant procedures or other remedies to prevent or redress the erroneous treatment of content (e.g. demotion) or unwarrented actions against users (e.g. suspension of accounts) which platforms consider to be in violation of their policies on disinformation»[37]. Inoltre, il rischio di lasciare alle piattaforme stesse la scelta dei *fact-cheker* presenta evidenti elementi di criticità che dovrebbero essere limitati con procedure diverse[38].

L'approccio di *governance* della disinformazione è rilanciato nel *Piano d'azione a sostegno della democrazia europea* (EDAP) del 5 dicembre 2020 che dedica ampio spazio alla questione, specialmente a livello politico ed elettorale[39]. Il Piano di azione definisce una serie di fenomeni contigui alla disinformazione in senso stretto: la *cattiva informazione* (contenuti falsi o fuorvianti, condivisi senza intenzione fraudolenta, anche se gli effetti possono comunque essere dannosi); la *disinformazione* in senso stretto (un contenuto falso o fuorviante, diffuso con l'intento di ingannare o ottenere un guadagno economico e che può provocare danni a interessi pubblici); l'*operazione di influenza delle informazioni* (sforzi coordinati da parte di soggetti nazionali o esterni volti a influenzare il pubblico destinatario utilizzando una serie di mezzi ingannevoli, tra cui la

[36] SWD (2020) 180 final, cit.

[37] *Ivi*, p. 11.

[38] «(…) online platforms have not considered other cooperative models such as open and non-discriminatory collaborations with independent fact checking initiatives that fulfil relevant ethical and professional standards», *ibidem*. Il ruolo delle piattaforme è considerato anche nel parallelo Piano d'azione (Media & Audiovisual Action Plan, MAAP) la cui Sezione denominata "Trasformazione" si occupa del sostegno alla creazione di spazi europei di dati per i mezzi di informazione per la condivisione e l'innovazione, v. Comunicazione della Commissione, *I media europei nel decennio digitale: un piano d'azione per sostenere la ripresa e la trasformazione*, COM(2020) 784 final del 3 dicembre 2020.

[39] COM(2020) 790 final, cit.

soppressione di fonti di informazione indipendenti in combinazione con la disinformazione); nonché l'*ingerenza di Stati stranieri nell'ambito di operazioni ibride*, comprensive di misure coercitive e ingannevoli per ostacolare la libertà di informazione e manipolare il voto in occasione delle elezioni. Oltre a tentativi di manipolazione dell'elettorato, le azioni delle piattaforme tendono a nascondere o travisare informazioni quali l'origine, l'intento, le fonti e i finanziamenti dei messaggi politici[40].

9. La previsione di codici di condotta e la co-regolazione nel DSA.

Nel programma "Legiferare meglio"[41], la Commissione europea include, oltre agli strumenti normativi. anche a quelli "non-normativi", come l'autoregolazione e la co-regolazione.

Il DSA prevede l'integrazione e il completamento delle disposizioni legislative tramite "codici di condotta" da applicare da parte delle piattaforme e dagli altri attori della comunicazione digitale che sottoscrivano impegni sui limiti dei contenuti e le modalità di attuazione. Pertanto, "(…), il Consiglio invita la Commissione a elaborare e, successivamente, applicare ulteriori requisiti in materia di trasparenza per le piattaforme online. L'obiettivo di tali requisiti sarebbe promuovere una sfera pubblica digitale ben funzionante, una maggiore responsabilità e un aumento della trasparenza nel contrasto della disinformazione. Le misure dovrebbero basarsi sul primato dei diritti fondamentali, specialmente la libertà di espressione, e su un dibattito pubblico democratico"[42].

Tra le disposizioni trasversali del DSA in materia di obblighi di diligenza, si prevede l'elaborazione di codici di condotta sui servizi digitali, con uno specifico rilievo per la pubblicità *online* (articoli 35 e 36). Tali sistemi di auto- e co-regolazione appaiono particolarmente auspicabili a fronte di "rischi sistemici" riscontrabili nell'attività delle

[40] Nel piano si sottolineano i rischi legati alle attività di soggetti esterni e di alcuni Paesi terzi (in particolare Russia e Cina) tramite operazioni di influenza mirate e campagne di disinformazione. In tale contesto il Piano prevede che venga sviluppato il pacchetto di strumenti dell'UE per rafforzare le attività e le task force di comunicazione strategica del SEAE.

[41] Comunicazione della Commissione, *Legiferare meglio per ottenere risultati migliori - Agenda dell'UE*, COM(2015) 215 final del 19 maggio 2015. Un confronto fra i diversi attori, strutturato in sette sessioni fra il 2013 e il 2017, si è svolto nella CoP (Community of Practice for self- and co-regulation) che ha prodotto numerosi documenti fra cui: *The "Principles for better self- and co-regulation"* (disponibili sul sito "Shaping the digital" della Commissione europea, reperibili *online*). Sulla *better regulation*, v. Comunicazione della Commissione, *Legiferare meglio: bilancio e perseveranza nell'impegno*, COM(2019) 178 final del 15 aprile 2019; Comunicazione della Commissione, *Legiferare meglio: unire le forze per produrre leggi migliori*, COM(2021) 219 final del 29 aprile 2021. Per un'analisi del dibattito in corso, v. G. LISTORTI et AL., *Towards an Evidence-Based and Integrated Policy Cycle in the EU: A Review of the Debate on the Better Regulation Agenda*, in *Journal of Common Market Studies*, 2020, p. 1558 ss. Sulla futura governance dell'Unione nel digitale, v. Comunicazione della Commissione, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final del 9 marzo 2021.

[42] Conclusioni del Consiglio sul rafforzamento della resilienza e il contrasto delle minacce ibride, compresa la disinformazione nel contesto della pandemia di COVID-19, Doc 14064/20 del 15 dicembre 2020, par. 4.

grandi piattaforme *online* secondo tre diverse categorie relative a: contenuti illegali (art. 26, lett. a)); situazioni negative per l'esercizio dei diritti fondamentali (*ivi*, lett. b)); manipolazione intenzionale con ripercussioni sulla tutela della salute pubblica, dei minori, del dibattito civico o sui processi elettorali e sulla sicurezza pubblica (*ivi*, lett. c)). La disinformazione, che non è esplicitamente menzionata, rientra certamente sia nella seconda e terza categoria, ma anche nella prima quando un contenuto sia erroneamente classificato come illegale mentre è un atto di disinformazione.

Tali rischi sistemici rilevabili nella prassi delle grandi piattaforme sono di interesse generale e riguardano tutti i server provider e gli altri protagonisti della comunicazione digitale. Al riguardo il DSA prevede che la Commissione europea promuova l'elaborazione dei codici di condotta (art. 35), «anche stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un quadro di comunicazione periodica sulle misure adottate e sui relativi risultati» (*ivi*, par. 2). Analogamente, si prevede l'elaborazione di un codice di condotta specificamente dedicato alla pubblicità *online* (art. 36).

Il limite principale di tale tipologia di strumenti è la mancanza di effetti nei confronti dei soggetti che svolgano le attività in oggetto senza esserne siano firmatari. Pertanto, pur rappresentando strumenti idonei a garantire una maggiore flessibilità per il conseguimento degli obiettivi, è necessario che raggiungano il massimo livello di rappresentatività dei soggetti coinvolti e restino nella cornice di principi e criteri fissati nel DSA che ne promuove l'adozione e dalla Commissione europea che guida il processo di adozione del codice da parte delle piattaforme. Nell'ambito del processo di co-regolazione, il Codice rivisto e rafforzato svolgerà un ruolo sostanziale di attuazione esecutiva della legislazione, pur conservando la sua natura di atto non-normativo.

In conclusione, nell'attesa dell'accordo fra Parlamento europeo e Consiglio sul testo del DSA, dovrebbe intensificare gli impegni a limitare il comportamento manipolativo, rafforzare gli strumenti di responsabilizzazione degli utenti, aumentare la trasparenza della pubblicità politica e potenziare la comunità dei ricercatori e del *fast-checker* (verificatori dei fatti).

10. La proposta di un Codice "rivisto e rafforzato" contro la disinformazione nel quadro giuridico del DSA.

In questo ambito, si inserisce la comunicazione della Commissione del 26 maggio 2021 per il rafforzamento del Codice di buone prassi della disinformazione[43]. La

[43] Comunicazione della Commissione, *Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*, COM(2021) 262 final del 26 maggio 2021. Sulle riunioni preparatorie, v. *Summary of the stakeholder discussions for the Guidance for strenghtening the Code* (first event, integrity of service and user empowerment; second online event, fact-checking and

Commissione fissa gli elementi fondamentali di un codice di co-regolamentazione "rinforzato" (rispetto a quello del 2018) per superarne la ridotta efficacia dimostrata, dovuta all'assenza di un quadro legislativo per i servizi digitali (a parte il limitato coordinamento della direttiva e-commerce) e di sanzioni vincolanti dell'Unione[44].

Per una valutazione della iniziativa in parola occorre, in primo luogo, confrontare lo schema proposto con quello del "Codice di buone pratiche contro la disinformazione" che si adatta al modello giuridico della co-regolamentazione o della "regolazione di tipo cooperativo". Infatti, il Codice in vigore travalica le forme dell'autoregolamentazione condivisa e applicata da soggetti privati, presentando elementi caratteristici della *soft-law*[45]. Malgrado il titolo lasci intendere che si tratti di una "standardizzazione dal basso" della prassi, un'analisi evidenzia il potere esercitato dalla Commissione europea. Il modello utilizzato prevede contenuti "predeterminati" tramite indicazioni/ raccomandazioni dell'Unione, soprattutto per quanto riguarda le *Roadmap* per l'attuazione degli impegni da parte delle singole piattaforme. Inoltre, in caso di "mancato allineamento" agli impegni, la Commissione può rendere pubblico il comportamento della piattaforma con presumibili danni di reputazione. Il controllo sull'attuazione resta comunque nel recinto delle modalità di *moral suasion*, cioè priva di effetti giuridici e, pertanto, di sanzioni applicabili.

Un secondo modello utilizzato per coinvolgere le piattaforme è quello del "Codice di Condotta per lottare contro le forme illegali di incitamento all'odio *online*"[46] i cui impegni "di carattere pubblico[47] (così definiti nel testo) riguardano l'adozione di procedure interne alle piattaforme per garantire una rapida ed incisiva risposta[48]. I soggetti firmatari sono tenuti a sviluppare un sistema di notifiche delle rimozioni di contenuti effettuate che consenta di rivedere le richieste alla luce dei termini di servizio, del Codice

research; third event, scrutiny of ad placements and transparency of political and issue-based advertising; fourth online event, key performance Indicators and monitoring of the Code of Practice), reperibile *online*.

[44] Più convincenti sono apparsi i risultati del programma di monitoraggio sulle azioni durante la pandemia da COVID-19, v. Comunicazione congiunta, *Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti*, JOIN(2020)8 final del 10 giugno 2020.

[45] Codice di Condotta per lottare contro le forme illegali di incitamento all'odio *online*, adottato dalla Commissione il 30 maggio 2016, firmato dalle maggiori piattaforme (Code of Conduct on Countering Illegal Hate Speech Online ountering illegal hate speech online, reperibile *online*). Sull'applicazione del Codice, v., da ultimo, Factsheet 5th evaluation of the Code of Conduct, June 2020, reperibile *online*.

[46] Facebook, Google, Microsoft e Twitter, cui si sono aggiunti nel 2018 anche Instagram, Google+, Snapchat, Dailymotion e jeuxvideo.com.

[47] Raccomandazione (UE) 2018/334 della Commissione, del 1° marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online, C/2018/1177. La raccomandazione faceva seguito alla Comunicazione della Commissione, *Lotta ai contenuti illeciti online Verso una maggiore responsabilizzazione delle piattaforme online*, COM(2017) 555 final del 28 settembre 2017. In tale contesto, la Commissione europea considerava la necessità di misure aggiuntive rispetto alla direttiva e-commerce, anche monitorando e consolidando i progressi compiuti sulla base di accordi volontari.

[48] In particolare, il Codice richiede che le società «valutino la maggior parte delle notifiche valide per la rimozione delle espressioni di odio illegale in meno di 24 ore e rimuovano o disabilitino l'accesso a tali contenuti, se necessario».

stesso e delle leggi nazionali che recepiscono la decisione quadro 2008/913/GAI[49]. In questo caso, l'approccio europeo alla formulazione e gestione del Codice di co-regolamentazione è collegato all'attuazione di uno strumento legislativo ex terzo pilastro GAI, anche se le modalità di rimozione del contenuto illegale sono definite nella Raccomandazione *ad hoc* della Commissione[50]. In assenza di garanzie procedurali a livello dell'Unione, applicabili ai servizi digitali, il Codice si limita a stabilire un rapporto fra la piattaforma e l'utente sul contenuto rimosso. Nel caso il contenuto sia stato erroneamente qualificato come illegale, la piattaforma dovrebbe ripristinarlo senza ritardo oppure consentire all'utente di postarlo nuovamente; mentre, in caso di conferma della rimozione da parte della piattaforma, sarà necessario fornirne la motivazione. Nonostante l'adesione al codice sia volontaria e gli impegni non obbligatori, il Codice sembra aver prodotto risultati apprezzabili, perché si tratta di contenuti illegali contrari alla legge di uno Stato membro e/o ad un atto legislativo dell'Unione[51] che in certo numero di casi richiede la denuncia alle autorità di polizia e giudiziaria.

Un terzo esempio di co-regolamentazione si ritrova nella direttiva europea sui servizi media audiovisivi (rivista nel 2018) che aggiorna la disciplina in materia all'impatto dell'attività delle piattaforme di video *sharing*[52] per effetto della convergenza nel mercato dei servizi di media audiovisivi fra televisione e piattaforme digitali. La direttiva prevede espressamente che gli Stati membri, al fine di adottare le misure volte a tutelare gli interessi dei minori[53], debbono incoraggiare il ricorso alla co-regolamentazione[54] mediante l'adozione di codici di condotta adottati a livello nazionale

[49] G. PITRUZZELLA, O. POLLICINO, *Disinformation and hate speech. A European Constitutional Perspective*, Milano, 2020; V. NARDI, *I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider?*, in *Diritto penale contemporaneo*, 2019 (estratto); G. PITRUZZELLA, O. POLLICINO, S. QUINTARELLI, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017; G. ZICCARDI, *L'odio* online. *Violenza verbale e ossessioni in rete*, Milano, 2016; T. M. MOSCHETTA, *La decisione quadro 2008/913/GAI contro il razzismo e la xenofobia: una «occasione persa» per l'Italia?*", in G. CAGGIANO (ed.), *Percorsi giuridici per l'integrazione*, Torino, 2014, p. 781 ss.

[50] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, 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 - SMAV), in considerazione dell'evoluzione delle realtà del mercato.

[51] Factsheet, The fifth evaluation on the Code of Conduct on Countering Illegal Hate Speech Online, 22 June 2020, cit. Il rapporto dimostra che è stato rimosso, entro 24 h dalla segnalazione, il 71 % dei contenuti ritenuti un illecito incitamento all'odio; il tasso medio di rimozione dimostra che «(…le piattaforme continuano a rispettare la libertà di espressione ed evitano di rimuovere contenuti non necessariamente classificabili come illecito incitamento all'odio (…)».

[52] V. Art. 4 bis, par. 2: «(…) La Commissione agevola, in cooperazione con gli Stati membri, la messa a punto di codici di condotta dell'Unione, ove appropriato, conformemente ai principi di sussidiarietà e di proporzionalità. I firmatari dei codici di condotta dell'Unione presentano alla Commissione i progetti di tali codici, unitamente alle relative modifiche (…)». Cfr.F. DONATI, *La tutela dei minori nella direttiva 2018/1808*, in *Medialaws*, 1/2019, p. 60 ss., reperibile *online*.

[53] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.

[54] Nuovi artt. 9, cc. 3 e 4, e 28-*ter*, c. 2 e 4, della Direttiva SMAV.

o a livello dell'Unione, concepiti in modo da essere ampiamente accettati dai principali soggetti interessati a livello nazionale ovvero a livello europeo[55]. La Commissione europea invita i fornitori di piattaforme per la condivisione di video a scambiare le migliori prassi relative ai suddetti codici di condotta di co-regolamentazione[56]. Per accrescere la sua efficacia, la direttiva introduce un codice di co-regolamentazione che collega l'autoregolamentazione con la legislazione nazionale[57]. Il ruolo delle autorità nazionali comprende il riconoscimento del regime, l'audit dei suoi processi e il suo finanziamento. A differenza delle trasmissioni televisive è evidente che i servizi digitali beneficeranno della co-regolamentazione a livello dell'Unione[58].

11. Le indicazioni della Commissione per il nuovo Codice.

Per quanto riguarda il contributo alla co-regolazione da parte della Commissione europea, il Codice dovrà evitarne il posizionamento dalla pubblicità online accanto a contenuti o a siti di disinformazione che ne traggono profitti e sostegno indiretto[59].

In relazione agli annunci pubblicitari politici o sociali[60], il Codice dovrebbe includere impegni rafforzati, tenuto conto delle disposizioni del DSA[61] per garantire la

[55] Nuovo art. 4-*bis* della Direttiva SMAV. Tali codici: a) sono concepiti in modo da essere ampiamente accettati dai principali soggetti interessati negli Stati membri; b) stabiliscono chiaramente e senza ambiguità i loro obiettivi, c) forniscono un monitoraggio e una valutazione regolari, trasparenti e indipendenti degli obiettivi fissati; ed) prevedono un'applicazione effettiva, comprensiva altresì di sanzioni effettive e proporzionate.

[56] Art. 28-*ter*, c. 9, della Direttiva SMAV.

[57] Rilevanti appaiono le considerazioni del considerando 12: «Numerosi codici di condotta esistenti nei settori coordinati dalla direttiva 2010/13/UE hanno dimostrato di essere ben concepiti, in linea con i principi per legiferare e colegiferare meglio. L'esistenza di un meccanismo di sostegno legislativo è stato considerato un fattore di successo importante nel promuovere il rispetto di un codice di autoregolamentazione o di coregolamentazione (…)».; nonché del considerando 13: «(…) Le misure dirette a conseguire gli obiettivi di interesse pubblico generale nel settore dei servizi di media audiovisivi emergenti sono più efficaci se adottate con il sostegno attivo dei fornitori dei servizi stessi».

[57] COM (2020) 825 final, cit., p. 12.

[58] Considerando (54) della proposta.

[59] I ricavi dalle pubblicità online, inclusa quella di grandi marchi, collocata involontariamente accanto ai contenuti di disinformazione contribuiscono ancora in modo significativo alla monetizzazione dei siti Web di disinformazione.

[60] Sebbene non esista una definizione comune di annunci sociali su questioni nel Codice, si tratta di annunci che includono contenuti sponsorizzati su questioni sociali o relativi a un dibattito di interesse generale che potrebbe avere un impatto sul discorso pubblico, quali ad es. il cambiamento climatico, le questioni ambientali in generale, l'immigrazione o la pandemia da COVID-19.

[61] Si tratta dell'attuazione tramite co-regolazione dell'art. 24 DSA sulla trasparenza della pubblicità *online*: «Le piattaforme online che visualizzano pubblicità sulle loro interfacce online provvedono affinché i destinatari del servizio siano in grado di identificare in modo chiaro e non ambiguo e in tempo reale, per ogni singolo messaggio pubblicitario mostrato a ogni singolo destinatario: a) la natura pubblicitaria delle informazioni visualizzate; b) la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità; c) informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità».

trasparenza, la riconoscibilità ed evitare i rischi del *microtargeting* degli utenti[62]. In argomento, il GEPD ha individuato rischi e danni derivanti dai modelli di business in cui i dati personali vengono utilizzati, contribuendo ad una maggiore polarizzazione, disinformazione e manipolazione politica e ideologica[63]. Rischi simili sono stati evidenziati anche dal Comitato europeo per la protezione dei dati (EDPB) nelle sue linee guida sul *targeting* degli utenti dei social media[64].

Per i sistemi di raccomandazione, i soggetti firmatari del Codice riveduto e rafforzato devono impegnarsi alla trasparenza dei criteri utilizzati per dare priorità o retrocedere i contenuti. Inoltre, è necessario assegnare priorità alle fonti autorevoli su argomenti di particolare interesse pubblico e sociale (come le informazioni fornite dalle autorità sanitarie relative alle misure di prevenzione della malattia o alla sicurezza dei vaccini). Al contrario, per i contenuti identificati come falso o fuorviante, gli impegni dovranno applicare sistemi di etichettatura coerente a seguito del "controllo dei fatti".

In relazione ai dati delle piattaforme, l'accesso dovrebbe essere protetto da distinti regimi di dati resi anonimi e non personali e dati che richiedono un controllo aggiuntivo, quali i dati personali. Tale quadro dovrebbe consentire l'accesso ai ricercatori accademici per comprendere fonti, vettori, metodi e modelli di propagazione della disinformazione. La condivisione dei dati personali da parte delle piattaforme con i ricercatori potrebbe avvenire sulla base di un codice di condotta ex art. 40 del GDPR[65] che ridurrebbe le incertezze giuridiche e i rischi per le piattaforme.

Il ruolo dei "verificatori dei fatti" *(fact-checker)* deve essere valorizzato e sostenuto. Tramite la valutazione dei contenuti in base a fatti, prove e informazioni contestuali, tali esperti aumentano la consapevolezza degli utenti sulla disinformazione *online*. Accordi multilaterali tra piattaforme e organizzazioni indipendenti dovrebbero garantirne l'indipendenza e una remunerazione equa.

Un solido sistema di monitoraggio dovrebbe consentire una valutazione regolare dell'attuazione degli impegni da parte dei soggetti firmatari, stimolando miglioramenti nelle loro politiche e azioni per contrastare la disinformazione.

12. Conclusioni.

[62] La Commissione europea ha manifestato l'intenzione di presentare una proposta legislativa sulla trasparenza dei contenuti politici sponsorizzati, v. COM(2020) 790 final, cit., p.5. Non è evidente se questo intento si debba ritenere assorbito dalla adozione di un Codice rivisto e rafforzato sulla disinformazione.

[63] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users*, adottate il 13 aprile 2021, reperibili *online*.

[64] European Data Protection Supervisor, *Opinion 3/2018 on online manipulation and personal data*, 19 March 2018, reperibile *online*.

[65] Il Regolamento generale sulla protezione dei dati (GDPR) incoraggia, all'art. 40, l'utilizzo dei codici di condotta destinati a contribuire alla corretta applicazione, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

In conclusione, la Commissione europea è fortemente impegnata contro la disinformazione *online* e, sulla base dei risultati ottenuti, intende promuovere diverse azioni complementari.

Mediante accordi di autoregolamentazione e di co-regolamentazione, i codici di condotta dovranno riguardare ambiti in cui una piattaforma *online* di dimensioni molto grandi può intervenire efficacemente per l'attenuazione dei rischi di disinformazione o di manipolazione e abuso per la società e la democrazia. L'obiettivo più significativo dovrebbe riguardare il contrasto a "operazioni coordinate" volte ad amplificare informazioni o determinare disinformazione, tramite l'utilizzo di *bot* o *account* falsi. La creazione di informazioni false o fuorvianti è particolarmente dannosa per i destinatari vulnerabili dei servizi digitali, quali i minori.

È evidente che la nuova versione del Codice contro la disinformazione assumerà un valore accresciuto, paragonabile con gli altri due codici vigenti nel settore digitale (codici nei confronti l'odio e per la condivisione di video) perché la co-regolamentazione in materia è ora prevista delle disposizioni legislative dal DSA e ne costituisce integrazione e completamento. Nell'ambito dell'armonizzazione legislativa per il mercato ex art. 115 TFUE, il "Codice rivisto e rafforzato" trova la sua legittimazione mentre, sinora, il Codice in vigore rappresenta uno strumento alternativo al mancato riconoscimento di una competenza legislativa dell'Unione in materia di servizi digitali (salvo che per le materie coordinate dalla direttiva *e-commerce*). In sostanza, l'armonizzazione legislativa trova un articolato sviluppo nel testo del DSA ma rinvia per alcuni aspetti di dettaglio, alle co-regolamentazione tramite codici di condotta da condividere e applicare da parte dalle piattaforme e dagli altri soggetti coinvolti (quali ad es. le società di pubblicità *online*).

La collaborazione dell'Unione europea con le piattaforme sarà certamente incrementata tramite il processo di co-regolazione ma è il quadro giuridico del DSA che contribuirà a garantire certezza e coerenza giuridica agli impegni dei soggetti firmatari. Per questa via, dovrebbero cadere la riluttanza di alcuni Stati membri ad un ampliamento, nel contesto dei servizi digitali, delle competenze dell'Unione in materia di diritti fondamentali e (dell'ambito di applicazione) della Carta dei diritti. Tale posizione poggiava sinora sull'assenza di competenze orizzontali dell'Unione europea in materia di contenuti digitali (competenza limitata dall'entrata in vigore della direttiva e-commerce a limitati aspetti "coordinati", quali ad es. la questione della responsabilità del *service provider*), salvo per alcuni contenuti illegali oggetto di misure verticali o tematiche (odio/terrorismo, pedo-pornografia).

Con la adozione del DSA, il legislatore dell'Unione europea stabilisce che nell'armonizzazione Mercato unico digitale rientra il contrasto alla disinformazione *online*, esercitando la relativa competenza per tale specifico aspetto (*pre-emtion*). In questa fase, la scelta del coinvolgimento delle piattaforme tramite codici di concotta non sarà più dovuta alla mancanza di competenza dell'Unione ma a considerazioni legate

esclusivamente alla maggiore efficacia della formulazione e gestione diretta, in ragione della vastità e urgenza degli interventi necessari al contrasto della disinformazione.

Una spinta irreversibile verso l'integrazione giuridica europea anche in questo delicato settore del Mercato unico digitale, sembra essere stata prodotta dalla prassi sempre più frequente di soggetti interni ed esterni all'Unione europea, intenzionati a produrre tramite disinformazione sui servizi digitali, danni materiali e violazioni dei diritti fondamentali (spesso di soggetti vulnerabili) e alla società nel suo insieme.

ABSTRACT: La proposta di regolamento del *Digital Service Act* (DSA) intende stabilire un'architettura normativa e istituzionale per l'attività dei *service provider* e delle piattaforme di hosting per i contenuti illegali (generati dagli utenti). Tuttavia, un aspetto particolarmente complesso è quello dei contenuti "legali ma dannosi", che caratterizzano la disinformazione online. L'adesione a un determinato codice di condotta (art. 35 DSA) e il suo rispetto da parte di una "piattaforma online di dimensioni molto grandi" possono essere ritenuti una misura adeguata di attenuazione dei rischi (considerando 68 DSA). Regolamentazione e co-regolamentazione devono integrarsi per contrastare la diffusione della disinformazione e delle "notizie false e fuorvianti". Non sarebbe possibile intervenire efficacemente se non con la collaborazione delle piattaforme digitali e degli altri *stakehoder*. Questo articolo esamina anche la recente Comunicazione della Commissione del 25 maggio 2021 di revisione del Codice di buone pratiche sulla disinformazione (2018). La questione appare di grande importanza nel più vasto quadro della "guerra ibrida" che alcuni soggetti statali pongono sempre più in essere soprattutto in occasione delle elezioni nazionali ed europee.

PAROLE CHIAVE: Digital Service Act, piattaforme online, notizie false, disinformazione, codice di buone pratiche

Combating misinformation between new obligations upon online platforms and the protection of fundamental rights in the framework of the Digital Service Act and co-regulation

ABSTRACT: The draft regulation of the Digital Service Act (DSA) intends to establish a regulatory and institutional architecture for the activity of service providers and hosting platforms for illegal content (generated by their users). However, a specific legal issue concerns the disinformation online ("legal but harmful" content) and other manipulative activities which produce systemic risks on society and democracy. This includes the use of bots or fake accounts for the creation of fake or misleading information. The adherence to and compliance with a given code of conduct (art. 35 DSA) by a very large online platform may be considered as an appropriate risk mitigating measure (recital 68 DSA). Regulation and co-regulation must be integrated to counter the spread of disinformation and "fake news". It would not be possible to effectively to react without the collaboration of digital platforms and other stakeholders (publishers, advertisers, etc.). This article also examines the recent Communication from the Commission of 25 May 2021 revising the Code of good practices on disinformation (2018). The question appears to be of great

importance in the broader policy of the "hybrid war" that some foreigner State are increasingly adopting, especially on the occasion of national and European elections.

KEYWORDS: Digital Service Act, online platforms, fake news, misinformation, code of good practices

La proposta della Commissione europea di adozione del "*Digital Markets Act*"

Gianluca Contaldi*

SOMMARIO: 1. Le caratteristiche dei mercati digitali. – 2. Le difficoltà di applicazione delle norme antitrust ai mercati digitali. – 3. La proposta della Commissione europea sul *Digital Markets Act* (DMA). – 4. Il rapporto intercorrente tra il *Digital Markets Act* e la normativa sulla concorrenza.

1. Le caratteristiche dei mercati digitali.

La *digital economy* costituisce il comparto produttivo più dinamico negli ultimi anni. Tale settore commerciale ha, infatti, registrato elevatissimi tassi di crescita a livello mondiale. Le multinazionali operanti in questo ambito (abitualmente identificate con l'acronimo GAFA[1]) hanno, d'altro canto, dimostrato di possedere una capacità di capitalizzazione eccezionalmente ampia, tanto è vero che i bilanci delle società operanti nel settore ammontano, ormai, a svariati miliardi di euro e possono equipararsi al PIL di paesi di media grandezza. I proventi complessivi del comparto non sono arretrati neppure negli anni della crisi finanziaria internazionale[2] e sono addirittura cresciuti, a seguito dell'aumento della domanda di impiego di piattaforme online, durante la pandemia da COVID-19[3].

Il principio di base dell'economia digitale è apparentemente semplice e consiste nello sfruttamento dei dati degli utenti al fine di profilare con la maggiore precisione possibile le offerte di servizi e di prodotti commerciali[4]. Più esattamente, esso consiste nell'elaborazione dei dati forniti dagli utenti attraverso sistemi algoritmici e di intelligenza artificiale. Tale processo presuppone, innanzitutto, l'anonimizzazione e, successivamente, l'elaborazione dell'insieme dei dati ricavati dalla navigazione su

* Professore ordinario di Diritto dell'Unione europea, Università degli Studi di Macerata.

[1] L'acronimo sta per Google, Amazon, Facebook, Apple (appunto: GAFA). In realtà, dal punto di vista concorrenziale, queste quattro piattaforme (alle quali, alle volte, si aggiunge anche Microsoft, nel qual caso, l'acronimo diviene GAFAM) presentano modelli di *business* fortemente differenziati (v., in generale, S. GALLOWAY, *The Four. The Hidden DNA of Amazon, Apple, Facebook and Google*, USA, 2018), che possono essere accomunati solo per il fatto di sfruttare commercialmente i dati degli utenti.

[2] V. lo *Special Report: the Data Economy*, in *The Economist*, February 22-28th 2020, p. 40 ss.

[3] I profitti delle cinque maggiori società operanti nel settore sarebbero aumentati del 43% nel corso dell'ultimo trimestre del 2020 ed i ricavi complessivi nel corso dell'anno supererebbero i mille miliardi di euro (così E. LIVINI, *I cinque giganti dell'hi-tech sono la terza potenza mondiale*, in *La Repubblica*, del 4 febbraio 2021, p. 24).

[4] H. THOMÉ, *Data: the Fuel of the Third Industrial Revolution*, in Fondation Robert Schuman, *European Issues*, 25th Februrary 2020, reperibile online.

internet degli utenti attraverso sistemi algoritmici e di intelligenza artificiale. Ciò che rileva dal punto di vista economico, pertanto, sono non tanto i dati personali singolarmente individuati, quanto piuttosto l'accumulazione e la loro successiva elaborazione attraverso strumenti algoritmici. Una volta compiuto questo processo, le masse di dati vengono normalmente cedute a produttori, società di marketing, partiti politici, gruppi di influenza, i quali vi fanno ricorso per indirizzare proposte mirate in funzione ai profili degli utenti. D'altro canto, i sistemi di intelligenza artificiale sono ormai divenuti così sofisticati che consentono non solo di individuare le preferenze dei consumatori, ma finanche di anticiparle e, in qualche modo, di indirizzarle[5]: così come, alla stessa stregua, si riesce alle volte a prevedere l'esito di determinate tornate elettorali, l'evoluzione dei flussi migratori, l'espansione territoriale delle pandemie[6].

I mercati digitali presentano abitualmente taluni caratteri peculiari, che li distinguono marcatamente da quelli tradizionali[7]. Il primo di questi è l'esistenza di un accentuato carattere di *network* ed un conseguente effetto di *lock-in*. Questi consistono nel fatto che più persone usano una determinata piattaforma, più aumenta l'attrattiva per coloro che, su detta piattaforma, offrono determinati servizi commerciali. Al contempo, l'incremento del numero degli iscritti determina, a propria volta, un aumento del "costo" per gli utenti di spostarsi su una piattaforma diversa. In altri termini, se tutti i miei "contatti" si trovano su *Facebook*, io non sono indotto a spostarmi sulla piattaforma di un concorrente, se non posso al contempo portare con me tutti i miei contatti.

Il secondo carattere è il rilievo assunto dalle economie di scala. La costruzione delle piattaforme online presuppone, infatti, ingenti investimenti in potenti elaboratori, dotati di un'estesa capacità di calcolo e un ampio spazio di archiviazione. Tuttavia, i costi fissi tendono ad assorbirsi, man mano che aumenta il numero degli utenti di una data piattaforma: quest'ultimo può, infatti, aumentare potenzialmente all'infinito, senza

[5] In concreto gli spazi pubblicitari vengono venduti all'asta, tramite sistemi informatici con effetto immediato (c.d. *Real Time Bidding*, RTB) tra i potenziali inserzionisti, in funzione dell'interesse suscitato dalle caratteristiche del singolo utente. V. G. PROIETTI, *La pubblicità nell'era delle nuove tecnologie*, in G. ALPA (a cura di), *diritto e intelligenza artificiale*, Pisa, 2020, p. 161 ss.

[6] V., in generale, S. QUINTARELLI, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Torino, 2019; A. VESPIGNANI, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Milano, 2019.

[7] Le caratteristiche dei mercati digitali sono accuratamente descritte in vari rapporti e indagini da parte delle autorità antitrust e delle commissioni legislative competenti: per l'Unione europea, v. J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era, Final Report*, Luxembourg, Publications Office of the European Union, 2019, reperibile *online*; per la Francia e la Germania, v. AUTORITÉ DE LA CONCURRENCE, BUNDESKARTELLAMT, *Competition Law and Data*, 2016, reperibile *online*; per l'Italia, v. AGCM, AGCOM, GARANTE PROTEZIONE DATI PERSONALI, *Indagine conoscitiva sui Big Data*, Roma, 2019, reperibile *online*; per il Regno Unito, v. J. FURMAN e a., *Unlocking Digital Competition - Report of the Digital Competition Expert Panel*, London, 2019, reperibile *online*; negli Stati Uniti, v. F. FUKUYAMA, B. RICHMAN, A. GOEL, R. R. KATZ, A. DOUGLAS MELAMED, M. SCHAAKE, *Report of The Working Group On Platform Scale*, Stanford University, 2020, reperibile *online*; v., sempre con riferimento al sistema statunitense, il rapporto della SUBCOMMITTEE ON ANTITRUST, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of Competition in Digital Markets*, reperibile *online*.

determinare incrementi rilevanti dei costi variabili. Sotto questo profilo, l'entità dell'investimento iniziale induce una sorta di barriera naturale all'ingresso dei concorrenti, perché occorrono ingenti spese per creare l'infrastruttura e per consentire alla stessa di arrivare ad un livello di utenti sufficientemente ampio da disporre di una massa di dati abbastanza estesa da rendere il loro sfruttamento economicamente vantaggioso.

Gli effetti di network congiuntamente con il rilievo delle economie di scala ha contribuito a determinare un assetto oligopolistico del mercato. Talune piattaforme sono, infatti, talmente sviluppate che finiscono per stabilire, esse stesse, le condizioni per accedere a quel particolare mercato. Detta situazione tende a verificarsi con maggiore frequenza per le piattaforme c.d. "ecosistema"[8], le quali consentono, da un lato, agli utenti di effettuare ricerche e di svolgere altre attività online; ma dall'altro operano, a propria volta, come operatori commerciali. Queste piattaforme funzionano, in altri termini, sia come piazze di mercato per operatori terzi, sia come negozi virtuali per offrire, al contempo, taluni prodotti autonomamente sviluppati.

Si ritiene sovente che tale peculiare struttura del mercato, caratterizzata di fatto dall'esistenza di pochi operatori in posizione dominante e dalla tendenza delle piattaforme presenti ad estendere le proprie attività commerciali anche in settori economicamente molto distanti, abbia determinato diverse conseguenze nefaste. Innanzitutto, esso ha indotto con una certa frequenza chi occupa le posizioni apicali (in termini di quote di mercato) ad abusarne, praticando, di fatto, condizioni poco trasparenti, nei rapporti con gli operatori commerciali che offrono i propri prodotti su una data piattaforma; oppure, utilizzando lo stesso mezzo per promuovere i prodotti confezionati dal gestore del sistema sfruttando, al contempo, i dati generati anche dall'attività degli altri operatori[9].

In secondo luogo, esso ha determinato una minore innovazione tecnologica: vi è, infatti, la diffusa sensazione che non convenga spendere somme per sostenere una nuova impresa che propone un modello di business alternativo rispetto ad un operatore che possiede una rilevante quota di mercato in uno specifico sistema digitale, perché l'investimento rischia di essere troppo impegnativo prima che lo stesso produca qualche frutto[10]. D'altro canto, nel momento in cui viene creata un'impresa che, per la tipologia di *software* utilizzato o perché ha inventato un sistema di intelligenza artificiale particolarmente efficiente, rischia di porsi come concorrente di una determinata piattaforma, accade sovente che la *start-up* venga rilevata dalla piattaforma dominante,

[8] V. A. CANEPA, *I mercanti dell'era digitale. Un contributo allo studio delle piattaforme*, Torino, 2020, p. 39 ss.

[9] V. G. MUSCOLO, A. MASSOLO, *Data Driven Economy. Trade-off Between Competition and Cybersecurity*, in *Analisi Giuridica dell'Economia*, 2019, p. 189 ss., 195.

[10] V. il rapporto della SUBCOMMITTEE ON ANTITRUST, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of Competition in Digital Markets*, cit., pp. 46-48.

sia per eliminarla (c.d. *killer acquisitions*), sia per acquisirne la tecnologia ed integrarla all'interno del proprio sistema digitale: in tal modo la piattaforma dominante riesce ad aumentare il numero e la tipologia dei servizi offerti e, corrispondentemente, ad incrementare la quantità di dati disponibili[11]. Queste acquisizioni sfuggono, in genere, al controllo delle autorità preposte, perché, di fatto, la quota di mercato ed il valore economico della società oggetto di incorporazione non è, in genere, tale da determinare il superamento della soglia di attenzione da parte delle autorità antitrust[12].

Sotto altro profilo, poi, la stessa presenza di piattaforme dominanti, che possiedono quote rilevanti del mercato, finisce per determinare un declino dei settori produttivi tradizionali, quali, ad esempio, quelli della piccola distribuzione o della pubblicità sui media tradizionali (giornali, radio, televisione), la quale risulta evidentemente meno efficace, non potendo raggiungere in tempo reale gli utenti potenzialmente interessati. In questo contesto, non solo l'esistenza delle piattaforme ecosistema ha determinato una minore innovazione nel settore digitale, ma ha anche indotto gli operatori economici a rivedere le proprie strategie di mercato e a ridurre gli investimenti nei settori tradizionali[13].

2. Le difficoltà di applicazione delle norme antitrust ai mercati digitali.

Le autorità antitrust dei vari paesi constatano diverse difficoltà ad applicare le norme sulla concorrenza ai mercati digitali. Ciò si verifica per una pluralità di circostanze.

Innanzitutto, per il fatto che le disposizioni antitrust, essendo state concepite in passato, non sono generalmente strutturate per affrontare il funzionamento della *digital economy*. Un primo evidente ostacolo discende dalla circostanza che i servizi, nell'economia digitale, sono offerti con modalità gratuite. Gli utenti delle piattaforme, per accedere ad un determinato social network o per potere effettuare determinate ricerche sui motori appositi, usano, quale moneta di scambio, i propri dati personali. La concorrenza tra le imprese operanti nel settore non avviene pertanto sui prezzi, come si verifica generalmente nei mercati tradizionali, nei quali le imprese cercano di offrire i medesimi beni ad un prezzo inferiore, quanto piuttosto sui servizi offerti all'utente, in modo da acquisire il maggior numero di dati ed elaborare in maniera più precisa le loro

[11] V. J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era, Final Report*, cit., p. 110 ss.; AUTORITÉ DE LA CONCURRENCE, BUNDESKARTELLAMT, *Competition Law and Data*, cit., p. 16 s.

[12] Secondo il rapporto predisposto dalla società di consulenza Lear per l'Autorità garante della concorrenza italiana (*Ex-post Assessment of Merger Control Decisions in Digital Markets, Final report, Document prepared by Lear for the Competition and Market Authority*, Rome, 9 May 2019) circa il 60% delle acquisizioni nel settore digitale hanno riguardato società particolarmente giovani, entro i quattro anni di vita.

[13] V. il rapporto della SUBCOMMITTEE ON ANTITRUST, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of Competition in Digital Markets*, cit., p. 57 ss.

preferenze commerciali (c.d. profilazione)[14]. In questo contesto, viene necessariamente meno uno degli abituali strumenti di misurazione della concorrenza, quale è il prezzo del prodotto o del servizio[15].

D'altro canto, neppure nelle ipotesi nelle quali il prezzo diventa un elemento del rapporto contrattuale, le autorità garanti della concorrenza possono fare su di esso affidamento per valutare l'esistenza di illeciti. La concertazione sul prezzo non dimostra necessariamente l'esistenza di un'intesa restrittiva della concorrenza, dal momento che la stessa determinazione del prezzo di offerta è sovente frutto di un'operazione algoritmica, priva, in quanto tale, dell'elemento di concertazione che necessariamente contraddistingue gli accordi restrittivi della concorrenza[16].

Sotto altro profilo, poi, pure la determinazione del mercato rilevante appare un'operazione problematica. Infatti, il mercato geografico, proprio per l'assenza di confini che caratterizza il *world wide web*, risulta di difficile individuazione: il mercato rilevante, rispetto alle piattaforme più diffuse, finisce, di fatto, per coincidere con il mondo intero[17]. Tale difficoltà definitoria è poi ulteriormente incrementata per la circostanza che, sovente, le piattaforme dominanti sono spesso imprese che operano su più mercati ovvero come gestori di una pluralità di attività commerciali (c.d. piattaforme "multiversante")[18]. In questo contesto, anche la definizione del mercato del prodotto finisce per essere un'operazione altamente problematica[19].

Da ultimo, la stessa determinazione di una posizione dominante solleva interrogativi di difficile soluzione. Dal momento che i mercati digitali sono fortemente dinamici, una determinata quota di mercato potrebbe non essere effettivamente rappresentativa di un'effettiva posizione di dominio, nel caso in cui un'altra impresa sia in grado di inventare un algoritmo che sia in condizione di svolgere le stesse operazioni in maniera più efficiente o nel caso in cui un'altra impresa offra un servizio nuovo, capace

---

[14] V. P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, p. 31, reperibile *online*.

[15] V. M.E. STUCKE, A.P. GRUNES, *Big Data and Competition Policy*, Oxford, 2016, p. 122 s.; nonchè S. MANNONI, G. STAZI, *Is Competition a click away? Sfida al monopolio nell'era digitale*, Napoli, 2018, p. 32 s.

[16] J. B. BAKER, *The Antitrust Paradigm. Restoring a Competitive Economy*, Cambridge, 2019, p. 101 ss.

[17] V. F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giurisprudenza commerciale*, 2018, p. 1064 ss.

[18] In via esemplificativa, Amazon opera come intermediario tra consumatori e commercianti per la vendita dei prodotti, come produttore e venditore della propria linea di prodotti, come venditore di pubblicità, come piattaforma per la diffusione di film e serie tv, come gestore di un ampio repertorio musicale, come piattaforma alla quale si può ricorrere come spazio di archiviazione di dati. Sulla base di un'indagine, sembra che il mercato dei prodotti offerti sulla piattaforma, da *core business* dell'azienda di Bezos, rappresenti ormai solo un'attività marginale rispetto al volume di affari ricavabile dagli altri settori commerciali.

[19] V., in questo senso, V. BAGNOLI, *The Big Data Relevant Market*, in *Concorrenza e mercato*, 2016, p. 73 ss.

di incontrare un maggiore riscontro da parte degli utenti[20]. In altri termini, le posizioni dominanti potrebbero essere prive di quel carattere di stabilità che, invece, rappresenta un elemento determinante della definizione.

In questo contesto i tradizionali rimedi del diritto antitrust, della nullità delle intese o della sanzione dell'abuso di posizione dominante, che normalmente intervengono solo *ex post*, allorché l'illecito si è già verificato, appaiono spesso insufficienti. Sia perché essi non consentono di risolvere il problema dell'esistenza di posizioni oligopolistiche in un determinato momento, sia perché i rimedi intervengono in maniera tardiva: solo una volta che l'algoritmo ha già determinato il prezzo o nel momento in cui una determinata piattaforma dominante ha già utilizzato i dati degli utenti per promuovere i propri prodotti a scapito di quelli dei concorrenti. Tanto più che le stesse sanzioni che vengono erogate nel diritto antitrust, difficilmente producono gli effetti auspicati, perché non possono certo determinare una modifica dei gusti degli utenti. È, d'altro canto, azzardato ipotizzare che si possano mutare le preferenze dei consumatori, una volta che questi siano abituati all'uso di una determinata piattaforma o di un dato *social network*.

Neppure i rimedi più innovativi, quali quelli correntemente utilizzati nei mercati caratterizzati da alta innovazione tecnologica, risultano funzionali. Da parte di taluni autori, si è infatti pensato che, per facilitare l'accesso al mercato dei nuovi operatori, si potrebbero costringere le piattaforme dominanti a condividere i dati in proprio possesso, attraverso il ricorso alla nota dottrina delle *essential facilities*[21]. Sembra tuttavia difficile configurare i dati alla stregua di *asset* insostituibili, perché è sempre possibile produrne all'infinito, semplicemente tracciando l'ulteriore attività degli utenti del web ovvero ricorrendo a fonti alternative di informazione. D'altro canto, i dati stessi sono facilmente spostabili, sia da parte della piattaforma, sia da parte dello stesso utente che li ha prodotti, che ha sempre il diritto di accedervi, di chiedere delle modifiche ovvero di portarli con sé su una diversa piattaforma[22].

E comunque un siffatto rimedio strutturale si rivelerebbe nella maggior parte dei casi scarsamente efficiente perché, nel momento in cui dovesse intervenire l'ordine dell'autorità, i dati stessi sarebbero ormai inattuali, in quanto superati dall'attività online

[20] Nota è l'affermazione, che viene correntemente addebitata al Ceo di Google, Eric Schmidt: "Competition is just one click away", in audizione davanti al Senato statunitense, Subcommittee on antitrust, competition and consumer rights, riferendosi al fatto che Google non era l'unico motore di ricerca disponibile (la notizia è tuttora riportata *online*).

[21] V., in questo senso, N. DESSARD, *EU Competition Policy in the Big Data Industry. Merger Review and Application of the essential Facility Doctrine*, Beau Bassin, 2018, p. 35 ss.

[22] V. art. 20 del 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), e art. 6 del Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

sopravvenuta[23]. In altri termini, i *big data* sono caratterizzati da un determinato valore che muta in maniera considerevole in rapporto alla loro istantaneità e alla loro quantità. Qualunque sanzione che intervenga in un momento successivo e che abbia lo scopo di diffondere la conoscenza che discende dal loro possesso pregresso (riferito, cioè, ad un momento trascorso nel tempo) risulta di norma inefficace rispetto all'obiettivo di consentire l'accesso al mercato a nuovi operatori.

3. La proposta della Commissione europea sul *Digital Markets Act* (DMA).

Proprio muovendo dalla constatazione della difficoltà di applicazione delle norme antitrust ai mercati digitali che la Commissione europea, in data 15 dicembre 2020, ha presentato una proposta normativa di regolamentazione delle piattaforme online (c.d. DMA, *Digital Markets Act*[24]), al fine di ridurre l'impatto anticoncorrenziale determinato dalla presenza di diffusi monopoli nel settore[25].

Con questa proposta normativa, la Commissione si propone di intervenire nel funzionamento dei mercati digitali, stabilendo una serie di obblighi in capo alle imprese che si pongono come punti di riferimento centrali nel disciplinare l'accesso al mercato. Lo scopo del DMA è, infatti, di contenere la posizione dominante delle grandi piattaforme *online* e favorire un sistema economico nel quale anche le imprese europee, di minori dimensioni e di ridotto potere di mercato, possono partecipare al mercato dei dati. La finalità di questa proposta, in altri termini, è identificabile in quello di creare un sistema nel quale possa prosperare una sorta di sovranità digitale europea[26].

Il legislatore europeo mira, infatti, ad anticipare l'effetto delle misure restrittive, predisponendo un'apposita regolamentazione applicabile *ex-ante*[27]. L'idea di fondo

[23] V. F. VESSIA, *Big data: dai vantaggi competitivi alle pratiche abusive*, cit., note 61-62 e testo relativo.

[24] Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), COM(2020) 842 final del 15 dicembre 2020.

[25] Dette proposte appaiono, per la verità, riduttive rispetto ai progetti inizialmente diffusi. Secondo l'idea originaria, infatti, la Commissione mirava ad articolare una proposta normativa strutturata in tre pilastri. Gli altri due atti concernevano, rispettivamente, la regolamentazione dei servizi digitali (v. la Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM(2020) 825 final del 15 dicembre 2020, c.d. DSA, *Digital Services Act*); e l'introduzione di uno strumento di azione rapida, maggiormente rispondente alle caratteristiche dei mercati digitali (il c.d. *New Competition Tool*; v. la consultazione pubblica lanciata in data 2 luglio 2020: *Impact Assessment for a possible New Competition Tool*, reperibile *online*). Di fatto, mentre il DSA ed il DMA, menzionato nel teso, sono stati effettivamente introdotti, il nuovo strumento concorrenziale è stato abbandonato.

[26] G.M. RUOTOLO, *Le proposte di disciplina di* digital services *e* digital markets *della Commissione del 15 dicembre 2020*, in *DPCE on line*, 2020/4, reperibile *online*.

[27] Già in una lettera datata 4 febbraio 2020, i Governi tedesco, francese, italiano e polacco chiedevano alla Commissaria europea alla concorrenza di predisporre una regolamentazione specifica per le piattaforme di grandi dimensioni: «We believe that the Commission should identify systemic actors against objective criteria taking into account specifities of digital markete, such as emergence of digital

sembra quindi individuabile nella *ratio* di porre taluni obblighi aggiuntivi, in modo di anticipare, per quanto possibile, l'effetto di garantire un mercato aperto e concorrenziale, che l'applicazione *a posteriori* della normativa antitrust, per le peculiari caratteristiche di questo settore economico, non era in grado di garantire.

Le disposizioni principali del DMA sono, infatti, gli articoli 5 e 6, che impongono talune obbligazioni supplementari a quelle piattaforme particolarmente rilevanti nel rispettivo settore economico, denominate, appunto, "*gatekeepers*". Esse vengono individuate – per effetto di una decisione della Commissione, a seguito di autodichiarazione ovvero di indagini – sulla base di taluni elementi oggettivi, astrattamente idonei a stabilire l'esistenza di una quota rilevante di mercato, in termini di fatturato e di utenti attivi su una data piattaforma[28].

Le previsioni principali stabiliscono una serie alquanto eterogenea di obblighi (ben diciotto), rispetto ai quali non è agevole individuare un filo conduttore. La distinzione principale concerne gli obblighi autonomamente applicabili (art. 5), da quelli applicabili a seguito di eventuale specificazione, da disporsi caso per caso, a cura della Commissione (art. 6)[29].

I principali tra gli obblighi del primo tipo riguardano gli abusi abitualmente commessi in questo settore economico dalle piattaforme digitali di grandi dimensioni. Al riguardo, tali obblighi possono suddividersi in due gruppi distinti[30]. Nel primo di questi, si possono includere tutti gli abusi di *sfruttamento*, sia degli utenti, sia degli operatori commerciali. In tale ambito, gli obblighi più rilevanti appaiono quello di astenersi dal combinare i dati ricavati dai principali servizi della piattaforma con quelli desumibili da

platforms with paramount importante for competition, that should be subject to specific scrutiny and, in relevant, to a specific regulatory framework» (la lettera è tuttora consultabile *online*).

[28] L'art. 3, DMA, stabilisce che il fornitore dei servizi di una piattaforma è considerato un gatekeeper se gestisce un servizio essenziale e se occupa una posizione consolidata e durata. Si presume che sussistano tali presupposti se l'impresa raggiunge un fatturato di sei miliardi e mezzo (negli ultimi tre bilanci) o se la capitalizzazione è almeno di sessantacinque miliardi di euro e se ha attivi almeno quarantacinque milioni di utenti al mese.

[29] In realtà, nonostante il titolo della previsione, che per l'appunto sembra affermare che occorra, ai fini della loro applicazione, una specificazione ulteriore ("*Obblighi dei gatekeeper che potranno essere oggetto di ulteriori specifiche*"), talune previsioni sembrano autonomamente applicabili, senza necessità di ulteriori interventi. Tra questi, un certo rilievo presenta l'obbligo del *gatekeeper* di astenersi dall'utilizzare, in concorrenza con gli operatori commerciali che fanno accesso alla medesima piattaforma, dati non accessibili al pubblico generati attraverso le attività dei predetti utenti commerciali: sembra ovvio che un particolare abuso di una piattaforma multiversante possa consistere, per l'appunto, nell'utilizzare i dati generati dall'attività di coloro che fanno ad essa ricorso per offrire in vendita i propri prodotti, quale strumento per fare concorrenza ai medesimi operatori (prassi abitualmente denominata del *data grabbing*: art. 6, lett. *a*). Del pari, non sembra richiedere ulteriore specificazione l'obbligo incombente al *gatekeeper* di consentire agli utenti finali di disinstallare qualsiasi applicazione software preinstallata sul proprio servizio di piattaforma di base (art. 6, lett. *b*); ovvero di astenersi dal garantire un trattamento più favorevole in termini di posizionamento ai servizi e prodotti offerti dal gatekeeper stesso o da terzi che appartengono alla stessa impresa rispetto a servizi o prodotti analoghi di terzi e applica condizioni eque e non discriminatorie a tale posizionamento (c.d. *self preferencing*: art. 6, lett. *d*); o, infine, di garantire la portabilità dei dati generati mediante l'attività di un utente commerciale o utente finale (art. 6, lett. *f*).

[30] V. P. MANZINI, *Equità e contendibilità nei mercati digitali*, cit., p. 40.

altri servizi offerti dalla medesima impresa; precludere la possibilità agli utilizzatori commerciali di offrire gli stessi prodotti e servizi ai consumatori finali a prezzi e condizioni diversi da quelli ottenibili sulla piattaforma; restringere il potere degli operatori commerciali, che fanno ricorso alla piattaforma, di rivolgersi all'autorità giudiziaria; escludere l'obbligo per gli operatori commerciali di registrarsi alla piattaforma e di obbligarli ad offrire i propri beni e servizi in via esclusiva tramite quella piattaforma.

Nella seconda tipologia rientrano, invece, le pratiche c.d. *leganti*, tra le quali si possono ricomprendere, le clausole di cui all'art. 5, lett. *e*), *f*), concernenti, rispettivamente, il divieto per il *gatekeeper* di costringere gli operatori commerciali ad utilizzare un servizio o un identificativo della piattaforma di base (non si possono, pertanto, discriminare tali operatori, in base alla circostanza che essi facciano o meno uso della logistica del medesimo *gatekeeper* per consegnare i beni agli utenti finali) ovvero di costringere gli operatori commerciali o gli utenti finali a registrarsi o a fare uso di un altro servizio del *gatekeeper*, come presupposto per essere presenti sulla piattaforma di base.

L'art. 6, del DMA, stabilisce, inoltre, taluni obblighi supplementari. Tale seconda disposizione precisa che questi obblighi sono suscettibili di essere ulteriormente specificati da parte della Commissione ovvero dell'autorità antitrust competente. A differenza delle ipotesi previste dalla prima disposizione, l'art. 6 contempla solo condotte *escludenti*.

Le disposizioni ora menzionate appaiono, per la verità, assai singolari. Ad un'analisi più attenta, talune delle ipotesi si configurano verosimilmente come specificazioni di obblighi incombenti alle imprese che risultano già desumibili da altre normative europee di carattere generale. Da questo punto di vista, si ha, infatti, l'impressione che il legislatore europeo abbia solo indicato quali obblighi *preventivi* quelle che, in realtà, rappresentano abituali violazioni della concorrenza ovvero del regolamento sulla tutela dei dati personali.

Tale connessione è particolarmente evidente allorché si tratta di obblighi evidentemente desunti da precedenti desumibili dalla giurisprudenza ovvero dalla prassi della Commissione europea. In tale ambito possono verosimilmente ricomprendersi: *i*) l'obbligo incombente al *Gatekeeper* di non confondere i dati propri con quelli ricavati da altre attività offerte dal medesimo soggetto (art. 5, lett. *a*, del *Digital Markets Act*)[31]; *ii*)

[31] Questo caso presenta evidenti analogie con il caso *Facebook – Whatsapp*. Nella specie, secondo i termini di utilizzo, Facebook poteva combinare i dati degli utenti ricavabili da altri servizi, oggetto di precedenti operazioni di concentrazioni, quali Instagram e WhatsApp. Secondo l'autorità della concorrenza tedesca, tale prassi costituiva sia una violazione della privacy, sia, al contempo, una violazione delle norme sulla concorrenza. Ovvero, detto in altri termini, una violazione delle norme antitrust che si concretizzava, di fatto, in un abuso delle norme sulla tutela dei dati personali (decisione n. B6-22/16, del 6 febbraio 2019, la decisione è consultabile *online*). Il ricorso in primo grado venne respinto e la decisione del Bundeskartellamt confermata (OLG Düsseldorf - Beschluss vom 26. August 2019 – VI-Kart 1/19 (V),

l'obbligo di consentire ai terzi di offrire gli stessi prodotti a condizioni diverse da quelle previste dal *gatekeeper* (art. 5, lett. *b*, della proposta DMA)[32]; *iii*) il divieto di creare dei legami tra i vari servizi offerti dall'operatore (art. 5, lett. *f*, della proposta: c.d. *tying clauses*)[33]; *iv*) l'obbligo del *gatekeeper* di permettere agli utenti finali di disinstallare il software preinstallato per accedere alla piattaforma (art. 6, lett. *b*, della proposta)[34]; *v*) il divieto di introdurre meccanismi che determinano una preferenza degli utenti finali per i prodotti sviluppati autonomamente dal *gatekeeper*, nel caso in cui sulla medesima piattaforma siano rinvenibili prodotti di terzi potenzialmente concorrenti (art. 6, lett. *d*, della proposta)[35].

Più limitate appaiono, invece, le analogie tra la proposta in esame ed il regolamento sulla protezione dei dati personali. In questo caso, l'aspetto che presenta maggiori analogie è rappresentato dall'obbligo imposto al *gatekeeper* di garantire la portabilità dei dati personali (art. 6, lett. *h*, della proposta). In concreto, si tratta di un obbligo già desumibile dall'analoga previsione di cui agli artt. 20, del regolamento 2016/679 sulla tutela dei dati personali, e 6 del regolamento 2018/1807, sulla circolazione dei dati non personali[36]: si tratta, pertanto, di una previsione già vigente nell'ordinamento europeo ed

Wettbewerb in Recht und Praxis, 2019, 1333). Il Bundesgerichtshof ha, del pari, respinto l'impugnazione e confermato la decisione dell'Autorità garante, ma ne ha modificato la motivazione. Secondo la Corte federale, infatti, il problema era rappresentato dalla restrizione della possibilità di scelta degli utenti (v. il comunicato stampa Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook, del 23.6.2020, reperibile *online*).

[32] Questa a previsione è tratta dal caso *Expedia* e *Booking*. A seguito della denuncia di un'associazione di albergatori, l'autorità garante della concorrenza francese ha sanzionato il comportamento di taluni portali di soggiorni alberghieri, per la prassi di imporre agli albergatori che offrivano le proprie stanze sulla piattaforma l'obbligo di non praticare prezzi e condizioni diverse (c.d. clausole di parità o *MFN-Most favoured Nation Clause*): v. la *Décision n° 19-D-23 du 10 décembre 2019 relative à des pratiques mises en œuvre dans le secteur de la réservation hôtelière en ligne*, reperibile *online*. Sul tema, v. P. MANZINI, *Le restrizioni verticali al tempo di internet*, in *Diritto del commercio internazionale*, 2018, p. 289 ss., par. 7; S. MAKRIS, *Antitrust Governance in an Era of Rapid Change*, in B. LUNDQVIST, M.S. GAL (eds.), *Competition Law for the Digital Economy*, Cheltenham, UK, 2019, p. 325 ss., p. 353 ss.

[33] Tale divieto è evidentemente ricavabile dagli articoli dall'art. 101, lett. *e*) e 102, lett. *d*, TFUE.

[34] La disposizione di cui all'art. 6, lett. *b*), DMA, è chiaramente desunta dalla decisione della Commissione europea nel caso *Google-Android* (18 luglio 2018, caso COMP/AT.40099), nella quale la Commissione europea ha qualificato come abusiva l'imposizione di Google ai produttori di dispositivi che usavano Android come sistema operativo di preinstallare Google Search e Google Chrome, come prerequisito per ottenere, al contempo, anche la licenza di uso di Play Sore, che costituisce il portale attraverso il quale gli utenti di tale sistema operativo possono acquisire le app necessarie a garantire un'efficiente utilizzazione dei propri dispositivi mobili. Sul caso v. P. MANZINI, *Prime riflessioni sulla decisione Google Android*, in *Eurojus.it*, 11 settembre 2018, reperibile *online*.

[35] Si tratta di una previsione che trae evidentemente spunto dal caso *Google Search (Shopping)*, nel quale la Commissione europea ha sanzionato Google perché il motore di ricerca collocava i prodotti offerti dal proprio servizio di vendita in cima alla lista, mentre i prodotti dei concorrenti si trovavano solo in terza e quarta pagina. La decisione della Commissione è stata impugnata davanti al Tribunale e la causa è ancora pendente (causa T-612/17, *Google e Alphabet* c. *Commissione*).

[36] La distinzione tra le due previsioni menzionate nel testo è determinata dalla natura dei dati dei quali viene garantita la portabilità. I dati oggetto del regolamento 2016/679 sono i dati personali, che consentono di individuare l'utente che li ha generati. L'oggetto del regolamento 2019/1807 sono, invece, i dati anonimi: ovvero proprio quelli normalmente impiegati nell'ambito dei c.d. *big data* e che sono

autonomamente applicabile nel caso in cui la piattaforma in posizione dominante sia, al contempo, qualificabile come responsabile del trattamento (come avverrà nella maggior parte delle ipotesi).

L'impressione di una sorta di sovrapposizione tra i vari settori normativi dell'ordinamento dell'Unione europea, risulta d'altro canto ulteriormente rafforzata, laddove si prenda in considerazione il fatto che tutti e tre gli strumenti normativi che stabiliscono specifici rimedi procedurali in ognuno dei settori in esame (rispettivamente, il DMA, da un lato ed i regolamenti 1/03 e 2016/679, dall'altro[37]) prevedono, nella sostanza, analoghi poteri di indagine e simili poteri sanzionatori.

Più dettagliatamente: l'autorità di controllo, in tutti e tre i sistemi normativi considerati, può richiedere informazioni nell'ambito di un'analisi del settore[38], richiedere informazioni all'impresa sottoposta alle indagini[39] ovvero effettuare accertamenti *in loco*[40].

Del pari, profonde somiglianze sussistono tra il potere sanzionatorio riconosciuto alle autorità competenti nei medesimi tre sistemi normativi. In tutti i casi le autorità di controllo dispongono del potere di imporre misure provvisorie[41]; possono accettare ovvero imporre impegni[42]; erogare sanzioni[43], di importo variabile dall'1% (in ipotesi di violazione dei soli obblighi di carattere procedurale), al 4% (irrogabile per gravi violazioni della privacy: es.: mancata richiesta del consenso), fino ad arrivare al 10% del fatturato complessivo di una determinata impresa (in caso di gravi violazioni della concorrenza, ovvero di mancato rispetto degli impegni o di mancata ottemperanza alle misure provvisorie). In altri termini, il dubbio che si pone legittimamente all'interprete è che vi sia una duplicazione di poteri di indagine e di quelli sanzionatori in capo a diverse autorità competenti, anche in presenza di illeciti a carattere unitario, laddove questi, per la loro particolare natura, rientrino nel campo di applicazione sia della normativa antitrust, sia di quella posta a tutela della privacy, sia del *Digital Markets Act*.

4. Il rapporto intercorrente tra il *Digital Markets Act* e la normativa sulla concorrenza.

suscettibili di sfruttamento commerciale (v. G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, pp. 160-162).

[37] Oltre alla proposta denominata *Digital Markets Act*, gli altri testi normativi ai quali facciamo riferimento nel testo sono il Regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del trattato, ed il citato reg. 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[38] V. art. 17 reg. 1/03; art. 15 DMA.

[39] V. art. 18 reg. 1/03; art. 58, par. 1, lett. *a*, reg. 2016/679; art. 19 DMA.

[40] Art. 20 reg. 1/03; art. 58, par. 1, lett. *e-f*, reg. 2016/679; art. 21 DMA.

[41] Art. 8 reg. 1/03; art. 58, par. 2, lett. *a-c*, reg. 2016/679; art. 22 DMA.

[42] Art. 9 reg. 1/03; art. 23 DMA.

[43] Art. 23 reg. 1/03; art. 83, reg. 2016/679; art. 26 DMA.

Date le sovrapposizioni rilevate tra i vari settori normativi dell'ordinamento europeo sopra rilevati, risulta fondamentale accertare quali siano i rapporti tra i tre sistemi normativi. Perché è evidente che se sussiste una sovrapposizione tra i vari sistemi, potrebbe accadere che le sanzioni irrogate nell'ambito di un sistema escludano un analogo potere da parte delle autorità competenti in un altro ambito[44].

Il DMA è abbastanza laconico sul punto. Esso si limita, infatti, a precisare che il regolamento si applica senza pregiudizio delle norme sulla concorrenza[45]; ovvero che lo stesso è complementare rispetto alle norme sulla tutela dei dati personali[46].

È bene chiarire che le ipotesi nelle quali, in relazione ad una medesima fattispecie, si possano applicare tutti e tre i sistemi normativi sopra indicati appare, invero, alquanto remota. Si potrebbe in astratto ipotizzare, che talune violazioni della normativa antitrust determinino, a propria volta, una lesione dei dati personali, come potrebbe avvenire nel caso in cui taluni problemi anticoncorrenziali discendano proprio dall'acquisizione di un concorrente che, nel proprio "patrimonio", possiede un'estesa massa di dati. In questo caso, se la piattaforma incorporante procede ad incrociare i dati presenti su entrambi i *network*, senza avere previamente avvisato gli utenti dell'una e dell'altra piattaforma, potrebbe verosimilmente porre in essere sia un comportamento anticoncorrenziale, sia una violazione della normativa posta a protezione della *privacy*, sia, infine, una violazione del disposto dell'art. 6, par. 1, lett. *a*), DMA[47]. In questo caso, cosa dovrebbero fare le autorità competenti per l'applicazione dell'uno e dell'altro strumento normativo (che, nell'ipotesi ora formulata, sarebbero la Commissione – o l'autorità garante della concorrenza nazionale –, per quanto riguarda l'applicazione della normativa antitrust; la Commissione, nel cado del DMA; e l'autorità garante della protezione dei dati all'interno dell'ordinamento nazionale coinvolto)?

In via preliminare vale la pena di precisare che i rapporti tra le diverse fonti regolatorie non appaiono risolvibili con i consueti criteri ermeneutici, i quali, d'altro canto, forniscono elementi contraddittori. Se da un lato, infatti, nella prospettiva della Commissione, il DMA è destinato a divenire una fonte regolamentare – pertanto subordinata agli artt. 101 e 102 TFUE – dall'altro è agevole osservare che lo stesso rappresenta una fonte speciale, quindi ipoteticamente destinata a prevalere sui

[44] Non è per la verità certo che il principio del *ne bis in idem* si estenda anche alle sanzioni amministrative. Esso è, infatti, espressamente previsto dall'art. 50, della Carta dei diritti fondamentali dell'Unione europea, come un solo in riferimento alla materia penale. Secondo le *Spiegazioni relative alla Carta dei diritti fondamentali*, il principio farebbe già autonomamente parte del diritto dell'Unione europea.

[45] Considerando n. 9; art. 1, par. 6, DMA.

[46] Considerando 11, DMA.

[47] Come potrebbe accadere nel caso *Facebook-WhatsApp*, laddove si seguisse l'impostazione del *Bundeskartellamt* (*supra*, nt. 39). In generale, le autorità competenti tendono a distinguere i profili di lesione della concorrenza da quelli di tutela dei dati personali, senza che si determini un assorbimento dei due diversi aspetti, i quali, appunto attengono alla protezione di beni giuridici diversi (V. L. CALZOLARI, *International and EU Enforcement in the Age of Big Data*, in *Diritto del commercio internazionale*, 2017, p. 855, par. IV).

regolamenti 1/03, relativo all'applicazione delle norme antitrust e 2016/679, sulla tutela dei dati personali.

Per la verità, il principio di specialità non appare – in questa specifica ipotesi – risolutivo. Secondo la nostra opinione, la soluzione del problema dipende, infatti, dalla visione che riteniamo più confacente della regolamentazione europea sui mercati digitali.

Al riguardo, è opportuno avvertire che, nonostante una formulazione sostanzialmente similare delle norme antitrust nell'Unione europea e negli Stati Uniti d'America, un analogo problema tenderebbe a non porsi oltreoceano[48]. Innanzitutto perché in quel sistema è la stessa autorità che regola la concorrenza che, al contempo, tutela i consumatori e, in parte, i dati personali degli utenti[49]. In questo ordinamento, pertanto, la stessa autorità può modulare il proprio potere sanzionatorio a seconda della gravità della violazione dei dati, della mancanza di innovazione in un determinato settore indotta da quel particolare comportamento abusivo, nonché della posizione dominante occupata dalla piattaforma che ha posto in essere l'illecito sullo specifico mercato di riferimento. In questo caso, infatti, l'autorità garante della concorrenza statunitense, verosimilmente, adotterà sanzioni lievi nell'ipotesi in cui la violazione della privacy sia di scarso rilievo e se la percentuale di mercato detenuta dalla piattaforma sia di dimensioni contenute. Viceversa, essa irrogherà sanzioni pesanti, fino ad arrivare a veri e propri rimedi strutturali (quali potrebbero essere la separazione delle società che gestiscono i diversi programmi software o tra i diversi rami operativi di una medesima piattaforma), nell'ipotesi in cui il danno arrecato allo sviluppo del mercato sia profondo e tendenzialmente irreversibile[50].

Diversamente dall'approccio statunitense, quello europeo si configura, piuttosto, come di carattere "sistemico", dal momento che esso è articolato in una pluralità di regolamentazioni, ognuna caratterizzata da una propria finalità specifica.

Questo aspetto è evidente per quanto concerne la normativa antitrust. L'ordinamento statunitense è, infatti, ispirato ad un maggiore liberismo, nel senso che tutto ciò che non è espressamente regolamentato, è rimesso al mercato e allo spirito imprenditoriale dei singoli. Nell'ordinamento dell'Unione europea, al contrario, la

[48] Non si intende qui prendere posizione sulla questione della validità della tesi, mai del tutto sconfitta, propugnata dai c.d. *Hipster Antitrust*, secondo la quale l'antitrust non dovrebbe occuparsi solo del benessere del consumatore, ma dovrebbe porsi anche altri obiettivi (quali, in particolare, il potere di mercato). Sul tema v. J.D. WRIGHT, E. DORSEY, J. RYBNICEK, J. KLICK, *Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust*, in *Arizona State Law Journal*, 2019, p. 293 ss.; H.J. HOVENKAMP, *Is Antitrust's Consumer welfare Principle Imperiled?*, University of Pennsylvania Law School, Research paper No. 18-15, 2019, p. 3 ss.

[49] Si tratta, nella specie, della *Federal Trade Commission*. Sul tema della tutela della privacy da parte dell'autorità normalmente competente per l'applicazione delle norme anticoncorrenziali, v. C.J. HOOFNAGLE, *Federal Trade Commission Privacy Law and Policy*, Cambridge, 2016, secondo il quale il ruolo della FTC si sarebbe evoluto, nel corso degli anni, da guardiano del potere di mercato, a controllore del rispetto della privacy.

[50] Come i procuratori dei vari Stati federati coinvolti sembrerebbero ora intenzionati a fare nel *complaint* contro Google (v. *State of Colorado et al. vs. Google*, 17 dicembre 2020, consultabile *online*).

funzione delle regole antitrust, un tempo concepita in funzione essenzialmente integrazionista, ora assolve essenzialmente allo scopo di contenere il potere di mercato, al fine di evitare che determinate aziende acquistino un ruolo eccessivamente preponderante e, in un certo senso, finiscano per sostituirsi al legislatore, stabilendo in via autonoma le regole di accesso ad un determinato mercato[51].

Al contrario, la tutela della *privacy* serve per tutelare gli individui e i loro dati personali. Ovviamente non perché si possa loro riconoscere un diritto di proprietà del singolo utente sui dati prodotti attraverso la navigazione sul *web*[52], ma nel senso che ogni individuo può sempre opporsi al trattamento e alla profilazione ovvero chiedere la cancellazione dei dati personali che lo riguardano[53].

Il DMA, dal canto suo, serve per intervenire con una regolazione *ex ante*, di modo che il commercio online non sia dominato solo da talune piattaforme, che di fatto restringono, con la loro stessa esistenza, la competizione e deprimono l'innovazione. In questo modo, il legislatore dell'Unione europeo, con l'adozione di detto atto normativo, intende passare dall'*enforcement* della normativa antitrust, alla regolamentazione del settore.

Se queste riflessioni sono corrette, è necessario affermare che i tre gruppi normativi individuati (antitrust, privacy, DMA) rispondono a logiche divergenti.

In questo contesto, sembra logico affermare che non intercorre alcun rapporto di sovrapposizione tra i diversi settori normativi. Questo ci porta innanzitutto a dire che non sussiste alcun rapporto di *bis in idem* tra le varie procedure. Le indagini devono essere condotte per uno scopo specifico; gli elementi acquisiti nel corso dell'una non possono essere utilizzati anche per un'indagine di tipo diverso, perché altrimenti si incorrerebbe in violazioni di principi cardine del diritto dell'Unione europea, quali i diritti nella difesa ed il rispetto del principio del contraddittorio.

---

[51] Il punto di svolta si può verosimilmente individuare nella relazione della Commissione sulla politica della concorrenza nel 2013 (*Relazione sulla politica di concorrenza 2013*, COM(2014) 249 final del 6 maggio 2014, p. 2). Si può infatti leggere nella relazione della Commissione sulla politica di concorrenza per il 2013 che: «la concorrenza svolge un ruolo cruciale nella promozione di fattori di crescita economica quali la produttività e l'innovazione. Ciò significa che la politica di concorrenza, che intensifica la concorrenza, stimola la crescita. Ciò vale per tutti gli strumenti della politica di concorrenza: l'applicazione della normativa antitrust può *contrastare i tentativi delle imprese dominanti di tenere nuovi operatori lontani dal mercato, impedendo loro di competere efficacemente* e può creare le condizioni per una riduzione dei prezzi dei fattori produttivi per l'industria UE; il controllo delle concentrazioni può mantenere i mercati aperti ed efficienti (…). Inoltre, la concorrenza e la politica di concorrenza sono parte integrante delle condizioni generali necessarie affinché *prosperi l'innovazione*. Esse incentivano le imprese innovative e quelle di nuova costituzione, incoraggiano le aziende a diventare più efficienti e promuovono la concessione di sovvenzioni destinate a *stimolare la R&S e l'innovazione*» (corsivi aggiunti).

[52] Per la disamina critica della tesi che tende a ravvisare un diritto di proprietà del singolo utente sui propri dati personali v. J. CIANI, *Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?*, in *Diritto del commercio internazionale*, 2017, p. 831, spec. parr. 7 e 8.

[53] V., rispettivamente, M. FRAIOLI, *Il diritto di opposizione e la revoca del consenso*, e A. BERTI SUMAN, *Il diritto alla cancellazione*, entrambi pubblicati in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, pp. 239 ss. e 199 ss.

Ne consegue, inoltre, che non vi è alcuna sovrapposizione nell'applicazione delle sanzioni. Se così è, nella rara ipotesi in cui una determinata impresa (che sia, al contempo, una piattaforma dominante) ponga in essere, con un unico comportamento, una violazione di tutti e tre i settori normativi, dovremmo giungere alla conclusione che ogni autorità possa, nei limiti dei rispettivi regolamenti attributivi del potere, irrogare le proprie sanzioni.

L'assenza di sovrapposizioni logiche e normative determina quindi l'ulteriore conseguenza che, nella rara ipotesi in cui con un unico comportamento la piattaforma dominante sia incorsa in violazione di tutti e tre i settori normativi, le sanzioni applicabili per effetto della normativa antitrust si possono – in punto di fatto – sommare a quelle applicabili per violazione del regolamento sulla protezione dei dati, che, a propria volta si possono aggiungere agli obblighi supplementari imposti ai colossi del *web* dal legislatore. Con la conseguenza che potremmo arrivare a comminare ad una determinata piattaforma sanzioni che, nel loro complesso, ammontano addirittura il 24% del fatturato globale dell'impresa: quindi, una cifra di assoluto rilievo, che risulta di entità tale da scoraggiare effettivamente finanche un'impresa di grandi dimensioni, quali sono oggi i giganti del mondo digitale, a porre in essere comportamenti abusivi e che, verosimilmente, consente di porre un freno allo strapotere di queste multinazionali.

Se così stanno le cose, si dovrebbe concludere che l'introduzione di una regolamentazione applicabile *ex ante*, quale quella contenuta nel DMA, avrebbe finanche una finalità intimidatoria, in modo tale da prevenire concretamente gli illeciti e favorire effettivamente lo sviluppo dell'innovazione e la nascita di un effettivo mercato digitale europeo.

ABSTRACT: I mercati digitali presentano caratteristiche molto peculiari, che ne hanno determinato una struttura fortemente oligopolistica. Questo assetto ha, fino a questo momento, prodotto diverse conseguenze dannose, sia sul funzionamento del mercato che sullo sviluppo di nuove imprese e nuovi prodotti. In questo contesto, diversi Stati hanno cercato di contrastare il fenomeno attraverso l'intervento delle autorità antitrust. Tuttavia, al momento, i tentativi sembrano non aver prodotto gli effetti sperati. L'approccio ora tentato dalla Commissione europea, che sta cercando di introdurre una specifica regolamentazione *ex ante* delle piattaforme online, fa sperare in una parziale soluzione del problema. La proposta non appare, tuttavia, molto chiara su una questione cruciale, che è il rapporto della stessa con la normativa antitrust. A parere dell'Autore, il *Digital Markets Act* deve essere considerato come una fonte di diritto complementare, il che significa che gli obblighi previsti al suo interno devono sommarsi agli obblighi previsti dagli artt. 101 e 102 TFUE.

PAROLE CHIAVE: concorrenza nei mercati digitali; piattaforme digitali; tutela dei dati personali; *Digital Markets Act*.

The European Commission's Proposal for a Digital Markets Act

ABSTRACT: Digital markets present very peculiar characteristics, which have determined a strongly oligopolistic structure of the market. This structure has produced several harmful consequences, both on the functioning of the market and on the development of new businesses and new products. In this context, several States have tried to tackle the phenomenon through the intervention of the antitrust authorities. However, at the moment, the attempts do not seem to have produced the desired effects. In this context, the approach now attempted by the European Commission, which is trying to introduce specific ex ante *regulation of online platforms, gives hope for a partial solution to the problem. The proposal is not very clear on a crucial matter, which is the relationship between the proposal itself and the antitrust rules. According to the opinion of the Author, the Digital Markets Act must be regarded as a complementary source of law, which means that the obligations provided within should add up to the obligations provided for by Articles 101 and 102 TFEU.*

KEYWORDS: Antitrust Law in Digital Markets; Digital Platforms; Privacy; Digital Markets Act.

Minori 4.0 e tutela dei diritti fondamentali nell'era della digitalizzazione: quali sfide per l'Unione europea?

Greta Bonini*

SOMMARIO: 1. La tutela del minore nell'Unione europea. – 2. I diritti dei minori nell'era della digitalizzazione. – 3. Alcune riflessioni conclusive: la pandemia da Covid-19 e la nuova Strategia europea sui diritti dei minori.

1. La tutela del minore nell'Unione europea.

L'Unione europea non fornisce una base giuridica specifica per l'adozione di normative poste a tutela dei diritti dell'infanzia. Con l'entrata in vigore del Trattato di Lisbona, tuttavia, in forza dell'art. 3, par. 3 e 5 TUE, che annovera tra gli obiettivi dell'Unione la promozione dei diritti umani, in particolare quelli dei minori, nello spazio giuridico europeo si è assistito ad un rilevante processo di promozione degli interessi dei soggetti in età evolutiva e di valorizzazione dei principi derivanti dalle convenzioni internazionali poste a tutela dei loro diritti fondamentali. Fra queste, assume un ruolo centrale la Convenzione sui diritti dell'infanzia e dell'adolescenza, adottata a New York il 20 novembre 1989[1] e successivamente completata da tre Protocolli facoltativi[2]. Nello

* Dottoranda di ricerca in Scienze giuridiche europee ed internazionali, Università degli Studi di Verona.

[1] Cfr. Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza; in dottrina v., su tutti, M. DISTEFANO, *Convenzione delle Nazioni Unite 20 novembre 1989 sui diritti del fanciullo*, in A. ZACCARIA (diretto da), *Commentario breve al diritto della famiglia*, 4ª ed., Padova, 2020, pp. 3323-3336; AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza: conquiste e prospettive a 30 anni dall'adozione*, 2019; U. KILKELLY, T. LIEFAARD (editors), *International Human Rights of Children*, Singapore, 2019; W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Children's Rights. A Commentary on the Convention on the Rights of the Child and its Protocols*, Cheltenham-Northampton, 2019; T. LIEFAARD, J. SLOTH-NIELSEN (edited by), *The United Nations Convention on the Rights of the Child. Taking Stock after 25 Years and Looking Ahead*, Leiden-Boston, 2017; E. VERHELLEN, *The Convention on the Rights of the Child. Reflections from a historical, social policy and educational perspective*, in W. VANDENHOLE, E. DESMET, D. REYNAERT, S. LEMBRECHTS (edited by), *Routledge International Handbook of Children's Rights Studies*, New York, 2015, pp. 43-59.

[2] V. Protocollo facoltativo alla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza relativo alla vendita dei minori, alla prostituzione infantile e alla pornografia rappresentante minori, adottato dall'Assemblea generale con risoluzione A/RES/54/263 del 25 maggio 2000 ed entrato in vigore il 18 gennaio 2002; Protocollo facoltativo alla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza relativo al coinvolgimento dei minori nei conflitti armati, adottato dall'Assembla generale con risoluzione A/RES/54/263 del 25 maggio 2000 ed entrato in vigore il 12 febbraio 2002; Protocollo facoltativo alla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza che stabilisce una procedura di presentazione delle comunicazioni, adottato

specifico, la sua importanza deriva soprattutto dal fatto che all'art. 3, par. 1 essa ha sancito per la prima volta il principio dei *best interests of the child*[3], stabilendo che in tutte le decisioni che riguardano i minori, qualunque sia l'organo o l'istituzione che le adotta, sia necessario rispettare il loro superiore interesse[4]. Benché tale principio rappresenti uno dei quattro pilastri su cui si fonda la Convenzione in parola[5], quest'ultima non ne detta una vera definizione, lasciando il compito al Comitato dei diritti del fanciullo, che nel suo *General Comment No 14 on the right of the child to have his or her interests taken as a primary consideration*[6] ne indica i tre aspetti essenziali. In primo luogo, esso rappresenta il diritto sostanziale del bambino ad ottenere una valutazione dei propri interessi, soprattutto nelle ipotesi in cui questi debbano essere contrapposti con altri diritti ugualmente rilevanti. In secondo luogo, i *best interests of the child* costituiscono una fonte interpretativa, cui è necessario ricorrere in caso di lacune presenti in altri strumenti normativi. Infine, il principio del superiore interesse del minore assurge a regola procedurale, che obbliga il giudice a motivare ogni decisione riguardante i minori, così che sia possibile valutare gli eventuali impatti concreti prodotti su di essi[7].

Nonostante l'Unione europea non sia parte della Convenzione delle Nazioni Unite[8],

dall'Assemblea generale con risoluzione A/RES/66/138 del 19 dicembre 2011 ed entrato in vigore il 27 gennaio 2012.

[3] E. LAMARQUE, *I* best interests of the child, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 140-161 chiarisce quale sia il corretto uso terminologico dell'espressione *best interests of the child* contenuta nella Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. A differenza della traduzione italiana «interesse superiore del minore», essa è declinata al plurale dal legislatore onusiano, lasciando intendere che non esiste un unico interesse del minore, ma, piuttosto, un insieme di interessi preminenti da tutelare. Sul punto cfr. anche A. GAUDIERI, *Il principio dei "best interests of the child" e la tutela della vittima minorenne nello spazio giuridico europeo*, in *Freedom, Security and Justice: Eur. Legal Studies*, 2019, pp. 106-138, spec. p. 109, reperibile *online*.

[4] L'espressa previsione all'interno della Convenzione ONU del principio dei *best interests of the child* ha mutato radicalmente la considerazione dei diritti dei minori, soprattutto con riguardo alla loro definizione e alla loro titolarità. Cfr., sulla questione, F. POCAR, *La CRC nel sistema delle Nazioni Unite*, in *La Convenzione delle Nazioni Unite*, cit., pp. 12-19, spec. p. 13.

[5] Oltre al superiore interesse del minore, la Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza si regge su altri tre pilastri fondamentali: il principio di non discriminazione (art. 2); il diritto alla vita, alla sopravvivenza e allo sviluppo (art. 6); il diritto all'ascolto (art. 12). Cfr. M.C. BARUFFI, *Il principio dei* best interests of the child *negli strumenti di cooperazione giudiziaria civile europea*, in A. DI STASI, L.S. ROSSI (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020, pp. 233-253, spec. p. 234; F. POCAR, *La CRC*, cit., p. 14; H. STALFORD, *Children and the European Union*, Portland, 2012, p. 32.

[6] Committee on the Rights of the Children, *General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para 1)*, 2013, UN Doc. CRC/C/GC/14.

[7] V. M.C. BARUFFI *Il principio dei* best interests of the child, cit., p. 234 s.; A. GAUDIERI, *Il principio dei "best interests of the child"*, cit., p. 109 s.

[8] Pur non esistendo, per le organizzazioni internazionali, un meccanismo di adesione alla Convenzione delle Nazioni Unite, nel novembre 2018 il Parlamento europeo ha invitato la Commissione a «esplorare soluzioni e mezzi che consentano all'UE di aderire unilateralmente alla Convenzione delle Nazioni Unite sui diritti del fanciullo (…) dato che tutti gli Stati membri dell'Unione l'hanno ratificata e che il diritto primario e derivato dell'UE reca disposizioni sostanziali sulla tutela dei diritti del fanciullo»; cfr. risoluzione del Parlamento europeo del 12 dicembre 2018 sulla relazione annuale sui diritti umani e la

anche l'ordinamento giuridico eurounitario, sia tra le sue fonti primarie che negli strumenti legislativi di diritto derivato, riserva al principio dei *best interests of the child* una posizione privilegiata. A tal proposito, occorre fare riferimento all'art. 24 della Carta dei diritti fondamentali dell'Unione europea, che, avente la stessa efficacia vincolante dei Trattati in forza dell'art. 6, par. 1 TUE[9], introduce per la prima volta nello spazio giuridico europeo norme *ad hoc* poste a salvaguardia dei diritti dei minori[10]. In particolare tale disposizione, basandosi espressamente sulla Convenzione delle Nazioni Unite[11], riassume in sé le principali tutele cui sono soggetti i minori d'età, ovverosia il diritto alla protezione e alle cure necessarie per il loro benessere ed il diritto ad esprimere liberamente la loro opinione, tenuta in considerazione l'età e il grado di maturità raggiunto (par. 1), il rispetto dei loro *best interests* in tutte le questioni che li riguardano (par. 2) ed il diritto a mantenere una relazione con entrambi i genitori, sempre che ciò sia conforme, ancora una volta, ai loro interessi (par. 3).

Anche negli strumenti normativi di diritto derivato si registra una crescente rilevanza del principio dei *best interests of the child*, in particolare nell'ambito della cooperazione giudiziaria in materia civile e, soprattutto, del regolamento (CE) n. 2201/2003[12]. In esso, ad esempio, in materia di responsabilità genitoriale, i titoli di competenza giurisdizionale individuati mirano a soddisfare proprio il superiore interesse dei minori, come nel caso della regola generale prevista dall'art. 8, che individua quale unico foro quello della residenza abituale, in considerazione del fatto che il giudice più

democrazia nel mondo nel 2017 e sulla politica dell'Unione europea in materia (2018/2098/INI). Anche i giudici di Lussemburgo hanno sottolineato l'importanza della Convenzione ONU per l'ordinamento giuridico europeo, ritenendo che essa si può annoverare «tra gli strumenti internazionali relativi alla tutela dei diritti dell'uomo di cui la Corte tiene conto per l'applicazione dei principi generali del diritto comunitario». Cfr. Corte di giustizia (Grande Sezione), sentenza del 27 giugno 2006, causa C-540/03, *Parlamento* c. *Consiglio*, EU:C:2006:429, punto 37; in dottrina v. G. BIAGIONI, *The Convention on the Rights of the Child and the EU Judicial Cooperation in Civil Matters*, in *Diritti umani e diritto internazionale*, 2020, pp. 365-386, spec. p. 367 e, in generale, A. ADINOLFI, *La rilevanza della CRC nell'ordinamento dell'Unione europea*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 63-86; H. STALFORD, *Children*, cit., pp. 32-36.

[9] Pur avendo la stessa efficacia vincolante dei Trattati, la Carta UE dei diritti fondamentali, ai sensi dell'art. 51, parr. 1-2, stabilisce che essa si applica «esclusivamente nell'attuazione del diritto dell'Unione europea» e «nel rispetto dei limiti delle competenze conferite dall'Unione nei trattati», non estendendo in alcun modo l'ambito di applicazione del diritto europeo. Per un commento all'art. 51 della Carta v., *ex multis*, P. MENGOZZI, C. MORVIDUCCI, *Istituzioni di Diritto dell'Unione europea*, 2ª ed., Milano, 2018, pp. 319-320; N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Milano, 2018, pp. 133-148; R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione europea*, 2ª ed., Torino, 2017, p. 148; J. ZILLER, *Art. 51. Ambito di applicazione*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, pp. 1044-1061.

[10] V. L. RATTI, *Art. 24. Diritti del minore*, *ivi*, pp. 476-484; F. CASOLARI, *Art. 24 della Carta dei diritti fondamentali dell'Unione europea*, in F. POCAR, M.C. BARUFFI (diretto da), *Commentario breve ai Trattati dell'Unione europea*, 2ª ed., Padova, 2014, pp. 1734-1739.

[11] Cfr. Spiegazioni relative alla Carta dei diritti fondamentali, pp. 17-35.

[12] Regolamento (CE) n. 2201/2003 del Consiglio, del 27 novembre 2003, relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e in materia di responsabilità genitoriale, che abroga il regolamento (CE) n. 1347/2000 (c.d. regolamento «Bruxelles II *bis*»).

vicino all'ambiente sociale e familiare del minore risulta essere quello più adatto a garantirne gli interessi[13], salvo applicare il principio in parola in maniera dinamica e flessibile a seconda della fattispecie concreta considerata[14]. A conferma che la ricerca dei *best interests of the child* rappresenta il filo conduttore della disciplina posta a tutela dei diritti dell'infanzia, nel 2019 il legislatore europeo ha adottato il regolamento di rifusione (UE) 2019/1111[15], ove il superiore interesse è stato elevato a «canone ermeneutico»[16] delle regole relative alla competenza in materia di responsabilità genitoriale[17], in virtù del richiamo espresso contenuto nel suo considerando 19. Tale atto legislativo risulta particolarmente importante, in quanto garantisce anche negli strumenti di diritto internazionale privato dell'Unione europea un livello minimo di protezione dei diritti fondamentali dei minori, grazie all'adozione sia dell'art. 21 relativo al diritto all'ascolto, sia di una specifica causa di sospensione dell'esecuzione di una decisione giudiziaria in caso di esposizione del minore a grave rischio di pericoli fisici o psichici, così come previsto dall'art. 56, par. 4[18]. Oltre alla disciplina contenuta nei regolamenti citati, fra gli

[13] M.C. BARUFFI, *Il principio dei* best interests of the child, cit., p. 242; C.E. TUO, *Superiore interesse del minore e regolamenti UE di diritto internazionale privato della famiglia*, in *Nuova giurisprudenza civile commentata*, 2020, pp. 676-686, spec. p. 678 s.

[14] Secondo A. GAUDIERI, *Il principio dei "best interests of the child"*, cit., p. 110, il principio dei *best interests of the child*, in quanto «dinamico, complesso, flessibile e adattabile» deve adeguarsi alle peculiarità e alle circostanze della fattispecie concreta che il giudice è chiamato ad esaminare. Cfr. anche O. LOPES PEGNA, *Tecniche internazionalprivatistiche a tutela del superiore interesse del minore: flessibilità alla ricerca del miglior risultato nel caso concreto*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 368-385.

[15] Regolamento di rifusione (UE) 2019/1111 del Consiglio, del 25 giugno 2019, relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e in materia di responsabilità genitoriale, e alla sottrazione internazionale di minori (c.d. «Bruxelles II *ter*»).

[16] Ricorre a tale espressione M.A. LUPOI, *Il regolamento (Ue) n. 1111 del 2019: novità in materia matrimoniale e di responsabilità genitoriale*, in *Rivista trimestrale di diritto e procedura civile*, 2020, pp. 575-610, spec. p. 577.

[17] Sulla ricerca del *best interests of the child* quale obiettivo perseguito dal regolamento di rifusione (UE) 2019/1111 si vedano, in particolare, L. CARPANETO, *Impact of the best interests of the child on the Brussels II ter Regulation*, in E. BERGAMINI, C. RAGNI (eds.), *Fundamental Rights and Best Interests of the Child in Transnational Families*, Cambridge-Antwerp-Chicago, 2019, pp. 265-285, EAD., *La ricerca di una (nuova) sintesi tra interesse superiore del minore «in astratto» e «in concreto» nella riforma del Regolamento Bruxelles II-bis*, in *Rivista di diritto internazionale privato e processuale*, 2018, pp. 944-977; M.C. BARUFFI, *La riforma del regolamento Bruxelles II* bis *e la tutela dell'interesse superiore del minore*, in E. *Triggiani, F. Cherubini, I. Ingravallo, E. Nalin, R. Virzo* (a cura di), *Dialoghi con Ugo Villani*, II, Bari, 2017, pp. 1087-1092; C. HONORATI, *La proposta di revisione del regolamento Bruxelles II-bis: più tutela per i minori e più efficacia nell'esecuzione delle decisioni*, in *Rivista di diritto internazionale privato e processuale*, 2017, pp. 247-282.

[18] G. BIAGIONI, *Il nuovo regolamento (UE) n. 2019/1111 relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e di responsabilità genitoriale, e alla sottrazione internazionale*, in *Rivista di diritto internazionale*, 2019, pp. 1169-1178, spec. p. 1173 ss. sottolinea i vantaggi di un riferimento più esplicito alla tutela dei diritti fondamentali del minore all'interno del regolamento di rifusione, sia nell'ambito del diritto all'ascolto che in quello dell'esecuzione delle decisioni giurisdizionali. Secondo l'autore, infatti, nel primo caso, l'art. 21, da un lato, permetterà di rendere direttamente applicabili dinnanzi ai giudici nazionali le disposizioni relative al diritto del minore di esprimere la propria opinione, dall'altro faciliterà il lavoro interpretativo della Corte di giustizia relativo alle condizioni e ai limiti di tale diritto; nel secondo caso, l'art. 56, par. 4 consentirà una maggiore considerazione del diritto del minore alla vita privata e familiare, tutelato sia dalla Carta UE dei diritti

atti adottati dall'Unione europea a tutela dei minori nel contesto della cooperazione giudiziaria in materia civile, rileva anche il regolamento (CE) n. 4/2009[19], il quale, pur non prevedendo espressamente la promozione dei *best interests of the child*, non esclude la rilevanza di tale principio nella sua interpretazione e applicazione[20].

Sebbene non contenga specifiche disposizioni a protezione dell'infanzia, anche la Convenzione europea per la salvaguardia dei diritti e delle libertà fondamentali dell'uomo (CEDU) promuove gli interessi dei minori nello spazio europeo[21], soprattutto in virtù dell'art. 6 TUE, che rafforza il ruolo dei diritti umani all'interno dell'ordinamento giuridico eurounitario. In particolare, nonostante la mancata formale adesione da parte dell'Unione alla CEDU, pur prevista dall'art. 6, par. 2 TUE, i diritti in essa contenuti rilevano quali principi fondamentali ai sensi del paragrafo 3 della stessa disposizione[22], rappresentando, in questo modo, un'importante fonte di interpretazione per i giudici della Corte di giustizia[23], in particolare nell'ambito dell'art. 8 posto a tutela della vita privata e familiare dei minori[24].

---

fondamentali che dalla CEDU.

[19] Regolamento (CE) n. 4/2009 del Consiglio, del 18 dicembre 2008, relativo alla competenza, alla legge applicabile, al riconoscimento e all'esecuzione delle decisioni e alla cooperazione in materia di obbligazioni alimentari.

[20] È quanto si evince, ad esempio, da Corte di giustizia, sentenza del16 luglio 2015, causa C-184/14, *A* c. *B*, EU:C:2015:479; secondo C.E. TUO, *Superiore interesse del minore*, cit., p. 677 la Corte di giustizia si è trovata ad affrontare questioni interpretative aventi ad oggetto sia il regolamento «Bruxelles II *bis*» che il reg. (CE) n. 4/2009 in quanto la realtà dei rapporti familiari evidenzia una «stretta correlazione tra gli aspetti inerenti all'affidamento dei figli minori e quelli riguardanti il loro mantenimento».

[21] Sulla rilevanza della CEDU nell'ambito della protezione del minore, cfr., per tutti, U. KILKELLY, *The Child and the European Convention of Human Rights*, Londra-New York, 2016.

[22] M. PARODI, *L'adesione dell'Unione Europea alla CEDU: dinamiche sostanziali e prospettive formali*, Napoli, 2020, p. 61 ss. contrappone la mancata «adesione formale» dell'Unione europea alla CEDU all'«adesione sostanziale» alla stessa, che avviene in virtù della rilevanza attribuitale dall'art. 6, par. 3 TUE. Sulla mancata adesione dell'Unione europea alla CEDU si vedano, in generale, I. ANRÒ, *Carta dei diritti fondamentali dell'Unione europea e CEDU: dieci anni di convivenza*, in *Federalismi.it*, 2020, pp. 109-146, spec. p. 140 ss., reperibile *online*; M.C. CARTA, *I "livelli" di tutela dei diritti fondamentali nello spazio giuridico europeo: i limiti del "dialogo" tra le Corti*, in *Studi sull'integrazione europea*, 2019, p. 161-186, spec. p. 181 ss.; F. CHERUBINI, *Qualche riflessione in merito alle prospettive di adesione dell'Unione europea alla Convenzione europea dei diritti dell'uomo alla luce del parere 2/13 della Corte di giustizia*, *ivi*, 2015, pp. 243-272; C. ZANGHÌ, *La mancata adesione dell'Unione europea alla CEDU nel parere negativo della Corte di giustizia UE*, *ivi*, 2015, pp. 33-62; P. GIANNITI, *L'adesione dell'Unione europea alla CEDU*, in P. GIANNITI (a cura di), *La CEDU e il ruolo delle Corti*, Bologna, 2015, p. 549 ss.; M. PEDRAZZI, *Art. 6 TUE*, in F. POCAR, M.C. BARUFFI (diretto da), *Commentario breve*, cit., p. 39 s.; C. SANNA, *Art. 6 TUE,* in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, 2ª ed., Milano, 2014, pp. 54-70, spec. p. 65 ss. Nonostante nel 2014 l'accordo di adesione alla CEDU sia stato bocciato dalla Corte di giustizia perché considerato incompatibile con i Trattati (Seduta Plenaria, parere 2/13 del 18 dicembre 2014, EU:C:2014:2454), a seguito di un incontro informale svoltosi il 22 giugno 2020, nel settembre 2020 ha preso avvio un nuovo negoziato formale di adesione alla Convenzione. La relazione relativa all'ultimo incontro dei negoziatori, svoltosi in data 25 marzo 2021, è reperibile *online*.

[23] Sulla CEDU quale fonte di interpretazione per il diritto dell'Unione europea, anche per il tramite della Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, v. A. ANNONI, *La CRC e la Convenzione europea dei diritti dell'uomo*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 20-43; H. STALFORD, *Children*, cit., pp. 36-39.

[24] Sull'art. 8 CEDU, v., *ex plurimis*, V. COLUCCI, *Il diritto di visita del minore nella giurisprudenza della Corte europea dei diritti dell'uomo (art. 8 Cedu)*, in A. DI STASI (a cura di), *Cedu e ordinamento*

Nel rispetto di siffatto quadro normativo, l'Unione europea tutela la minore età anche attraverso atti atipici, quali programmi e strategie d'azione[25], dedicando, così, massima attenzione alla protezione dei diritti fondamentali dei soggetti in età evolutiva. In tal senso, un primo documento d'impulso è rappresentato dalla comunicazione «Verso una strategia dell'Unione europea sui diritti dei minori»[26], adottata nel 2006 dalla Commissione europea e successivamente sviluppata nel «Programma UE per i diritti del minore»[27] del 2011, strumento che, pur non essendo giuridicamente vincolante, è tuttavia significativo nella misura in cui definisce il modello di riferimento per la normativa e l'approccio metodologico adottati dall'Unione nei confronti dei minori[28]. Nello specifico, essa si propone obiettivi quali una giustizia civile e penale a misura di minore e la lotta alla violenza in ogni sua forma, oltre ad interventi nell'ambito del diritto di famiglia e l'impegno di verificare che le misure e le proposte legislative aventi ad oggetto i minori siano compatibili con la Carta UE dei diritti fondamentali[29] e, in particolare, con il principio dei *best interests of the child*. Per il raggiungimento di siffatti scopi, il Programma si prefigge di raccogliere dati ufficiali affidabili e comparabili, ottenuti con l'aiuto degli Stati membri e delle parti interessate, le cui rilevazioni confluiscono regolarmente nel Forum europeo per i diritti dei minori[30]. Nel 2014, a distanza di tre anni dall'avvio del Programma, il Consiglio ha considerato raggiunti undici fra gli obiettivi

italiano, 2ª ed., Milano, 2020, pp. 591-616; V. PICCONE, *Tutela familiare e interesse alla conservazione dei rapporti di affettività (art. 8 Cedu)*, *ivi*, pp. 561-590; E. BERGAMINI, *Human Rights of Children in the EU Context*, in E. BERGAMINI, C. RAGNI (eds.), *Fundamental Rights*, cit., pp. 3-20; C. FENTON-GLYNN, *Children, Parents and the European Court of Human Rights*, in *European Human Rights Law Review*, 2019, pp. 643-652; G. HOHLOCH, *La protezione della vita familiare nella CEDU e nella Carta UE*, in *Familia*, 2019, pp. 115-124; L. TOMASI, *La famiglia nella Convenzione europea dei diritti dell'uomo: gli artt. 8 e 14 CEDU*, in *Questione giustizia*, 2019, reperibile *online*.

[25] Cfr. risoluzione del Consiglio dell'Unione europea e dei rappresentanti dei governi degli Stati membri, riuniti in sede di Consiglio, su un quadro di cooperazione europea in materia di gioventù, Strategia dell'Unione europea per la gioventù 2019-2027 (ST/14944/2018/INIT); risoluzione del Parlamento europeo del 18 aprile 2016, Salvaguardia dell'interesse superiore del minore in tutta l'UE sulla base delle petizioni presentate al Parlamento europeo (2016/2575(RSP)); comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Programma UE per i diritti dei minori, COM(2011) 60 def. del 15 febbraio 2011; conclusioni del Consiglio, del 9 novembre 2010, sulle agende politiche europee e internazionali sui bambini, i giovani e i diritti dei bambini; comunicazione della Commissione, Verso una strategia dell'Unione europea sui diritti dei minori, COM(2006) 367 def. del 4 luglio 2006.

[26] Comunicazione della Commissione, Verso una strategia dell'Unione europea, cit.

[27] Comunicazione della Commissione, Programma UE per i diritti dei minori, cit. Per un commento, cfr. A. RIETI, *Il Programma dell'Unione europea per i diritti dei minori*, in *Sud in Europa*, 2011, reperibile *online*; M.C. LANZA, *Unione Europea: le strategie di protezione e promozione dei diritti del bambino nell'azione interna ed esterna*, in *Dossier del Centro Diritti Umani (2009-2018)*, in *La giustizia a misura di bambino*, reperibile *online*.

[28] Così AGENZIA EUROPEA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA, *Manuale di diritto europeo in materia di diritti dell'infanzia dell'adolescenza*, 2016, p. 23, reperibile *online*.

[29] Comunicazione della Commissione, Programma UE per i diritti dei minori, cit., p. 4.

[30] Il Forum europeo per i diritti dei minori, istituito nella comunicazione della Commissione «Verso una strategia dell'Unione europea sui diritti dei minori» del 2006, si svolge con scadenza annuale ed è giunto nel 2020 alla sua 13ª edizione.

indicati dalla Commissione[31], grazie, in particolar modo, ai progressi realizzati dagli Stati membri e dalle istituzioni europee nell'attuazione delle politiche e delle strategie proposte. I riscontri concreti alle azioni intraprese con il Programma del 2011 sono rinvenibili nelle fonti secondarie del diritto dell'Unione, tra cui si possono ricordare, soprattutto con riguardo alla tutela processuale del minore, la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile[32], la direttiva 2012/13/UE sull'informazione nei procedimenti penali[33], la direttiva 2012/29/UE in materia di diritti, assistenza e protezione delle vittime di reato[34], la direttiva 2013/33/UE relativa all'accoglienza dei richiedenti la protezione internazionale[35], la direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, nonché al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari[36]. Tra le misure non legislative si possono annoverare la raccomandazione della Commissione «Investire nell'infanzia per spezzare il circolo vizioso dello svantaggio sociale»[37] del 2013, che si propone di attuare una serie di interventi contro la povertà e l'esclusione sociale nella prima infanzia, e il documento strategico del 2015 sul coinvolgimento dei minori in procedimenti giudiziari civili, amministrativi e penali nei ventotto Stati membri dell'Unione[38], nonché gli studi redatti dall'Agenzia europea dei diritti fondamentali dell'Unione europea del 2015[39] e del

[31] Si tratta, in particolare, del diritto di asilo, delle politiche migratorie, della salute, della sicurezza e del *welfare*, della povertà e dell'esclusione sociale, del lavoro minorile, della partecipazione, della giustizia civile e penale, dell'istruzione, dell'ambiente, dei media e di Internet, della non discriminazione e della violenza sui minori; cfr. L. RATTI, *Art. 24*, cit., p. 480.

[32] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio; v. *amplius* par. 2

[33] Direttiva 2012/13/UE del Parlamento europeo e del Consiglio, del 22 maggio 2012, sul diritto all'informazione nei procedimenti penali.

[34] Direttiva 2012/29/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2012, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI.

[35] Direttiva 2013/33/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante norme relative all'accoglienza dei richiedenti protezione internazionale (rifusione).

[36] Direttiva 2013/48/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari.

[37] Raccomandazione della Commissione, del 20 febbraio 2013, Investire nell'infanzia per spezzare il circolo vizioso dello svantaggio sociale (2013/112/UE).

[38] DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS (EUROPEAN COMMISSION), UNIVERSITY COLLEGE CORK. CHILD LAW CLINIC, *Children's involvement in criminal, civil and administrative judicial proceedings in the 28 Member States of the EU. Policy Brief*, June 2015, reperibile *online*.

[39] Cfr. AGENZIA EUROPEA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA, *Giustizia a misura di minore: prospettive ed esperienze di professionisti*, 2015, reperibile *online*, la quale esamina la situazione dei minori di diciotto anni nei procedimenti giudiziari civili e penali in dieci Stati membri, tra cui Regno Unito, Spagna, Francia, Germania, Finlandia, Romania, Polonia, Estonia, Croazia e Bulgaria, selezionati

2017[40], i quali esaminano l'effettiva fruizione da parte dei minori dei diritti loro spettanti, partendo dalle esperienze concrete di professionisti e operatori del diritto, oltre che dal punto di vista dei più piccoli. Nell'ambito delle politiche europee a tutela dei diritti dei minori, infine, nel 2018 la Commissione ha adottato la «Strategia dell'Unione europea per la gioventù 2019-2027»[41] e nel 2020 la «Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea»[42], nella quale, in particolare, viene sottolineato l'impegno dell'Unione nel proteggere i minori da gravi pregiudizi allo sviluppo fisico ed emotivo, soprattutto alla luce dell'attuale contesto sociale, costantemente in evoluzione[43]. A livello nazionale, sempre in conformità agli obiettivi fissati nel Programma, è stata istituita con legge 12 luglio 2011, n. 112[44] l'Autorità garante per l'infanzia e l'adolescenza, col fine di assicurare l'attuazione e la tutela dei diritti e degli interessi dei minori d'età, come previsto anche dall'art. 18 della Convenzione delle Nazioni Unite.

2. I diritti dei minori nell' era della digitalizzazione.

Le nuove tecnologie digitali rappresentano un'importante risorsa per lo sviluppo e la crescita dei minori, poiché l'abbattimento delle barriere spaziali e temporali che caratterizza la Rete offre ad essi numerose opportunità di scambio e socializzazione[45]. L'uso di Internet, tuttavia, evidenzia anche la condizione di oggettiva debolezza dei minori d'età, in quanto essi, a causa del loro incompiuto processo di maturazione[46], sono soggetti particolarmente vulnerabili nel *cyberspace*. Per questo, è necessario predisporre

in quanto presentano un ampio ventaglio dei diversi sistemi giudiziari europei nonché per la presenza o l'assenza di buone prassi; cfr. anche M. CASTELLANETA, *La giustizia a misura di minore in uno studio dell'Agenzia UE sui diritti fondamentali*, in *Minori giustizia*, 2015, pp. 169-180.

[40] Cfr. AGENZIA EUROPEA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA, *Giustizia a misura di minore: prospettive ed esperienze di minori e professionisti*, 2017, reperibile *online*.

[41] Risoluzione del Consiglio dell'Unione europea, Strategia dell'Unione europea per la gioventù 2019-2027, cit.

[42] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea, COM(2020) 711 final del 2 dicembre 2020.

[43] *Ibidem*, p. 2.

[44] Cfr. legge 12 luglio 2011, n. 112, Istituzione dell'Autorità garante per l'infanzia e l'adolescenza, entrata in vigore il 3 agosto 2011.

[45] G. VOTANO, *Protezione e tutela dei minori in internet*, in G. CASSANO, S. PREVITI (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, pp. 117-137, spec. p. 118.

[46] Così A. ASTONE, *I dati personali dei minori in rete, Dall'internet delle persone all'internet delle cose*, Milano, 2019, p. 7, la quale sottolinea la necessità di garantire il principio dei *best interests of the child* anche nel mondo digitale. Sulla tutela dei minori d'età quali soggetti particolarmente vulnerabili nel contesto di Internet e delle nuove tecnologie digitali v. anche D. DE FELICE, *The right to Security of Online Childhood*, in *The International Journal of Children's Rights*, 2017, pp. 573-598; B. CAROTTI, *La tutela dei minori*, in E. APA, O. POLLICINO (a cura di), *La regolamentazione dei contenuti digitali*, Ariccia, 2014, pp. 407-432; L. MUSSELLI, *La tutela dei minori nei nuovi media*, in AA.VV., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Santarcangelo di Romagna, 2013; A. THIENE, *L'inconsistente tutela dei minori nel mondo digitale*, in *Studium iuris*, 2012, pp. 528-535.

misure efficaci di tutela, capaci di garantire loro sicurezza e protezione anche nel mondo del *web*. Per far fronte a tale esigenza, l'Unione europea ha adottato numerosi atti di *soft law*[47] che, pur non avendo efficacia vincolante, hanno evidenziato l'impegno delle istituzioni europee nello sviluppo di linee guida a prevenzione e contrasto dei pericoli derivanti da un uso incontrollato delle moderne tecnologie multimediali da parte dei soggetti in età evolutiva[48]. Tra gli strumenti più significativi in materia, assume rilevanza la «Strategia per un internet migliore per i ragazzi»[49], adottata nel 2012 dalla Commissione, a cui è seguita, pochi mesi dopo, la risoluzione del Parlamento europeo sulla tutela dei minori nel mondo digitale[50]. Nella sua Strategia, in particolare, la Commissione invita gli Stati membri a fornire ai minori le competenze e gli strumenti digitali necessari affinché essi possano utilizzare in modo completo e sicuro la rete Internet, oltre a sbloccare, sempre a loro beneficio, il potenziale del mercato dei contenuti *online* di tipo interattivo, creativo ed educativo. Nel fare ciò, essa ha individuato una serie di azioni programmatiche che le istituzioni e gli Stati sono tenuti ad adottare e a sviluppare in modo sinergico, che possono ricondursi a quattro pilastri fondamentali, individuabili in: contenuti *online* di qualità; svolgimento di attività di sensibilizzazione e responsabilizzazione; creazione di un ambiente in linea sicuro; contrasto degli abusi e dello sfruttamento sessuale minorile. Gli obiettivi perseguiti dalla Strategia hanno trovato un riscontro concreto nella creazione del portale *Better Internet for Kids*[51], nato allo scopo di fornire informazioni e studi aggiornati relativi ai problemi derivanti dall'uso di Internet da parte dei minori. Esso ha influenzato numerose politiche degli Stati membri[52],

[47] Comunicazione congiunta al Parlamento europeo e al Consiglio, Strategia dell'UE in materia di cibersicurezza per il decennio digitale (JOIN/2020/18 final del 16 dicembre 2020); relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Valutazione finale del programma pluriennale dell'UE per la protezione dei bambini che usano internet e altre tecnologie di comunicazione (programma Safer Internet), COM(2016) 364 final del 6 giugno 2016; risoluzione del Parlamento europeo del 20 novembre 2012 sulla tutela dei minori nel mondo digitale (2012/2068(INI)); comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia europea per un internet migliore per i ragazzi, COM(2012) 196 final del 2 maggio 2012; decisione n. 1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 1998, relativa a un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione; Raccomandazione del Consiglio del 24 settembre 1998 concernente lo sviluppo della competitività dell'industria dei servizi audiovisivi e d'informazione europei attraverso la promozione di strutture nazionali volte a raggiungere un livello comparabile e efficace di tutela dei minori e della dignità umana (98/560/CE); libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione, COM(96) 483 def. del 16 ottobre 1996.

[48] G. VOTANO, *Protezione e tutela*, cit., p. 118 sottolinea tuttavia come, a causa della velocità del progresso tecnologico, il legislatore europeo si sia spesso trovato in difficoltà a predisporre in anticipo idonei strumenti di regolazione e protezione dei minori.

[49] Cfr. Comunicazione della Commissione, Strategia europea per un internet migliore per i ragazzi, cit.

[50] Risoluzione del Parlamento europeo sulla tutela dei minori nel mondo digitale, cit.

[51] Per conoscere le iniziative e leggere gli studi promossi sul portale *Better Internet for Kids* è possibile consultare il sito della piattaforma.

[52] Nell'ambito della «Strategia per un internet migliore per i ragazzi» e di *Better Internet for Kids* gli Stati membri sono stati invitati ad adeguare le loro politiche in tema di tutela dei diritti dell'infanzia nel

incentivando l'organizzazione di azioni e campagne, soprattutto nel contesto delle scuole. Tra il 2019 e il 2020, in particolare, si sono svolti numerosi eventi rivolti ai più giovani, durante i quali sono stati affrontati temi come le *fake news*, il cyberbullismo, la riservatezza e il *grooming*, oltre ad altre problematiche legate all'esposizione dei minori ai contenuti dannosi rinvenibili nel *web*[53].

Fra i diritti dei minori maggiormente esposti a pregiudizio nel contesto di Internet, è necessario considerare innanzitutto quello alla riservatezza, rilevante sia a livello sovranazionale *ex* art. 16 della Convenzione delle Nazioni Unite[54], sia a livello europeo nell'ambito dell'art. 8 della Carta UE dei diritti fondamentali e, soprattutto, del regolamento (UE) 2016/679 sulla protezione dei dati personali[55]. Sorto con l'obiettivo di contemperare il diritto alla *privacy* con gli eventuali altri interessi fondamentali coinvolti[56], tale regolamento è significativo anche nell'ambito della protezione del minore[57], la cui riservatezza deve essere considerata nell'ottica del rispetto dei *best interests of the child*[58]. Alla luce di tale principio, infatti, la disciplina contenuta nel *General Data Protection Regulation* deve tenere conto di due aspetti: da un lato, la

mondo digitale. Al fine di monitorare i progressi compiuti a livello nazionale in termine di raggiungimento degli obiettivi fissati dalla Commissione europea nella sua Strategia, negli anni sono state predisposte tre relazioni (nel 2015, nel 2018 e, infine, nel 2020) i cui risultati sono organizzati attorno a tre argomenti principali, ovverosia *policy framework*, *policy making* e *policy implementation*. Con riguardo ai risultati ottenuti nel 2020, la Commissione ha riportato, relativamente al *policy framework*, che tutti gli Stati coinvolti nell'indagine hanno incorporato nelle loro politiche nazionali elementi derivanti dalla Strategia, relativamente alla *policy making*, che tali Stati hanno adottato modelli di cooperazione interministeriale e raccolto dati circa l'uso di Internet da parte dei minori, i quali vengono sistematicamente e direttamente consultati e informati sulle politiche relative all'uso di Internet, relativamente alla *policy implementation*, che tutti gli Stati coinvolti hanno organizzato iniziative volte a stimolare la produzione e la visibilità di contenuti *online* di alta qualità nonché a supportare l'insegnamento della sicurezza *online* nelle scuole, con un aumento superiore al 60% rispetto a quanto riportato nella relazione del 2018.

[53] Il calendario degli eventi organizzati nel contesto della «Strategia per un internet migliore per i ragazzi», reperibili sul portale *Better Internet for Kids*, è disponibile *online*.

[54] Per un commento all'art. 16 della Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, cfr. F. DI PORTO, *La libertà di espressione del minore e il diritto all'accesso ai mezzi di comunicazione e alla riservatezza*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 224-240; W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Article 16. The right to privacy*, in ID., *Children's Rights*, cit., pp. 184-193, spec. p. 192 s.

[55] 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, noto anche come *General Data Protection Regulation* o, più semplicemente, *GDPR*.

[56] G. SPOTO, *Disciplina del consenso e tutela del minore*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, p. 111 s.

[57] In base al considerando 38 del regolamento (UE) 2016/679, i minori meritano «una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali».

[58] Cfr. A. ASTONE, *I dati personali dei minori in rete*, cit., p. 32 ss.; V. MONTARULI, *dei dati personali e il minore*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 275-325, spec. p. 277; J.C. BUITELAAR, *Child's best interest and informational self-determination: what the GDPR can learn from children's rights*, in *La protezione International Data Privacy Law*, 2018, pp. 293-308.

vulnerabilità e l'immaturità del minore; dall'altro, la sua soggettività, soprattutto nei casi in cui egli abbia raggiunto un livello di maturità psicofisica tale da poter esprimere la propria opinione in relazione al trattamento dei suoi dati, come previsto anche nell'ambito dell'ascolto, tutelato in generale dall'art. 12 della Convenzione delle Nazioni Unite[59]. Nello specifico, è espressione di tale bilanciamento la disciplina contenuta all'art. 8 del *GDPR*, che, in relazione al consenso del minore, da una parte valorizza la sua posizione giuridica, in quanto esso è chiamato a partecipare in modo diretto al trattamento dei propri interessi, dall'altra ne tutela la vulnerabilità, dettando un preciso limite anagrafico per l'esercizio dei diritti a lui riservati[60]. In particolare, al primo comma l'art. 8 stabilisce che il consenso del minore è legittimamente prestato al compimento del sedicesimo anno d'età[61], salvo indicare, al capoverso successivo, che i legislatori nazionali sono liberi di dettare per legge un'età inferiore, purché essa non sia al di sotto dei tredici anni[62]. Tale flessibilità sembra costituire un'intrinseca contraddizione all'interno del regolamento, in quanto concedere agli Stati membri la possibilità di indicare età diverse ai fini del consenso da parte del minore al trattamento dei suoi dati personali significherebbe vanificare il generale intento di armonizzazione delle discipline nazionali perseguito dallo stesso *GDPR*[63]. A ciò si aggiungono altre criticità, quali la facilità con cui i «nativi

[59] L'ascolto del minore, strumento attraverso il quale egli può partecipare alle decisioni che lo riguardano, rappresenta un diritto unanimemente condiviso non solo a livello internazionale ed europeo, ma anche nel diritto interno. Per un'analisi dell'istituto v., per tutti, R. CLERICI, *Il diritto all'ascolto e i diritti di partecipazione*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 203-223.

[60] Cfr. V. MONTARULI, *La protezione*, cit., p. 288.

[61] Secondo L. BOLOGNINI, C. BISTOLFI, *L'età del consenso digitale. Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679 (UE*), 7 marzo 2017, reperibile *online*, il limite d'età fissato dal legislatore europeo affinché i minori possano prestare un valido consenso digitale non fornisce una risposta adeguata alle esigenze di tutela perseguite dal regolamento, in quanto impedire astrattamente loro di accedere a Internet e alla società dell'informazione «non farebbe che generare un maggiore senso di curiosità nei giovani». A parere degli autori, piuttosto, sarebbe più utile cercare soluzioni differenti, quali programmi di formazione all'interno delle scuole, così che i minori possano acquisire competenze digitali a prescindere dalla loro età.

[62] In Italia, il legislatore ha fissato il limite a quattordici anni; cfr. art. 2-*quinquies*, d.lgs. 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).

[63] Così D. AMRAM, *La tutela dei dati personali degli utenti vulnerabili nell'IOT*, in *Il diritto di internet*, cit., pp. 401-409, spec. p. 406 s.; F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Il diritto dell'informazione e dell'informatica*, 2018, pp. 27-64, spec. p. 36. Critica la possibilità concessa agli Stati membri di derogare al limite d'età indicato dal regolamento (UE) n. 2016/679 anche G. PEDRAZZI, *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, in *Informatica e diritto*, 2017, pp. 437-451, spec. p. 443, reperibile *online*, il quale sottolinea come tale libertà rappresenta «una delle principali situazioni in grado di generare potenziale incertezza». L'intento di armonizzazione perseguito dal *General Data Protection Regulation* è indicato al considerando 3, il quale ricorda come anche la direttiva 95/46/CE, abrogata proprio dal regolamento (UE) 2016/679, si proponesse il medesimo scopo. Cfr. direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

digitali»[64] aggirano la regola del consenso[65] e la scarsa accessibilità alle informative relative alla *privacy* [66], spesso non adatte agli utenti più giovani, nonostante l'esplicita richiesta contenuta nell'art. 12, par. 1 del medesimo regolamento[67]. Nel contesto della tutela della riservatezza, inoltre, un ulteriore rischio è rappresentato dall'uso scorretto dei *social networks*, ove, senza un preventivo controllo da parte degli adulti, il comportamento del minore può sfociare in fenomeni pericolosi, come ad esempio il cyberbullismo[68], che l'art. 17 lett. *f* del regolamento (UE) 2016/679 ha scoraggiato tramite l'istituto della cancellazione (o «diritto all'oblio»), il quale prevede la possibilità per il minore di ottenere, senza ingiustificato ritardo da parte del titolare del trattamento, l'eliminazione dalla Rete dei dati che lo riguardano[69]. Come esplicitato dal considerando 65, tale richiesta può essere formulata anche dopo il raggiungimento della maggiore età, se il minore aveva prestato il proprio consenso prima di aver sviluppato la maturità necessaria a comprendere i pericoli presenti nel cyberspazio. Lo stesso art. 17, par. 3,

[64] L'espressione «nativi digitali» descrive la condizione di coloro che, nati e cresciuti nell'era di Internet, hanno imparato a utilizzare sin dalla tenera età le tecnologie digitali, che fanno parte della loro quotidianità; cfr., su tutti, M. MARTONI, *Datificazione dei nativi digitali e società della classificazione. Prime riflessioni sull'educazione alla cittadinanza digitale*, in *Federalismi.it.*, reperibile *online*, 2020, pp. 119-136; A. PELLAI, *Costruzione di identità e nuovi processi di socializzazione: le sfide evolutive dei nativi digitali*, in *Minori giustizia*, 2018, pp. 68-76; A. DINGLI, D. SEYCHELL, *The New Digital Natives*, Berlin-Heidelberg, 2015, pp. 9-22.; P. FERRI, *Nativi digitali*, Milano, 2011.

[65] Per ovviare alle problematiche legate alla verifica dell'età dei minori fruitori dei servizi della società dell'informazione G. BIANCHEDI, *Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico*, in *Ciberspazio e Diritto*, 2019, pp. 389-413, spec. p. 406 ss. propone di ricorrere a strumenti quali, ad esempio, l'invio di un documento d'identità del genitore o dell'esercente la responsabilità genitoriale, l'esecuzione di una minima transazione economica tramite carta di credito, la c.d. verifica dei pari (o *peer based verification*), l'analisi semantica e la verifica *offline*.

[66] Sul punto cfr. A. ASTONE, *L'accesso dei minori d'età ai servizi della c.d. Società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul Codice per la protezione dei dati personali*, in *Contratto e impresa*, 2019, pp. 614-648, spec. pp. 622 e 643; I.A. CAGGIANO, Privacy *e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, pp. 3-23, spec. p. 5.

[67] L'art. 12, par. 1 della direttiva (UE) 2016/679 prevede che le informative relative alla *privacy* presentino «forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori».

[68] Allo scopo di adeguarsi alla disciplina europea relativa al trattamento e alla protezione dei dati personali dei minori, l'Italia ha adottato la l. 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo. In dottrina, per un commento alla l. n. 71/2017 V. PICCININI, *La tutela dei minori contro il cyberbullismo*, in *Il diritto di* internet, cit., pp. 139-159; G. GINI, *Il cyberbullismo*, in *Minori giustizia*, 2019, pp. 142-149; R. BOCCHINI, M. MONTANARI, *Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*, in *Nuove leggi civili commentate*, 2018, pp. 340-384; R.M. COLANGELO, *La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche*, in *Informatica e diritto*, 2017, pp. 397-418, reperibile *online*; A. GATTO, *Social network, skype, nuovi media nelle relazioni familiari*, Milano, 2017, pp. 112-126; P. PITTARO, *La legge sul cyberbullismo*, in *Famiglia e diritto*, 2017, pp. 819-823; M. ROSPI, *Social media, minori e cyberbullismo: lo* status quo *della legislazione nazionale ed eurounitaria*, in *Informatica e diritto*, 2017, pp. 453-482, reperibile *online*.

[69] A. ASTONE, *I dati personali dei minori in rete*, cit., p. 66, sottolinea come il legislatore italiano, inserendo all'art. 2 l. n. 71/2017 la regola secondo cui il minore che ha compiuto i quattordici anni possa ottenere «l'oscuramento, la rimozione o il blocco» di qualsiasi dato personale diffuso in Rete, abbia voluto coordinare la normativa relativa al cyberbullismo con le disposizioni in tema di *privacy* contenute nella l. n. 101/2018 e nel regolamento (UE) n. 2016/679.

tuttavia, introduce significative eccezioni all'obbligo di cancellazione, ad esempio laddove dovessero sussistere motivi di interesse pubblico tali per cui risulti necessario conservare i dati dell'interessato. In simili ipotesi, sempre a tutela del principio dei *best interests of the child*, è necessario procedere con un rigoroso esame della fattispecie concreta, al fine di evitare che la potenzialità particolarmente lesiva della Rete, ove la possibilità di divulgazione delle notizie è elevata, comporti gravi ripercussioni sulla formazione del minore[70].

La rivoluzione digitale ha prodotto effetti pure sul diritto alle comunicazioni e all'accesso alle informazioni, garantito nell'ambito dell'art. 17 della Convenzione delle Nazioni Unite[71]. In particolare, tale diritto rileva in quanto, grazie alla fruibilità dei supporti informatici quali *personal computers*, telefoni cellulari e televisioni *on demand* presenti ormai in ogni ambiente familiare, i minori possono accedere al *web* con maggiore facilità, anche se privi del senso critico necessario per comprendere i messaggi rinvenibili in Rete, col rischio di incorrere in situazioni pericolose o inadatte alla loro età. Da ciò, deriva la necessità di predisporre adeguate politiche legislative volte a incentivare nei minori un uso consapevole dei nuovi media, impegno che si è tradotto, a livello europeo, nell'adozione della direttiva (UE) 2018/1808 sui servizi media audiovisivi[72], che ha aggiornato la precedente disciplina[73] e introdotto nuove forme di tutela per i soggetti in età evolutiva, con riguardo, soprattutto, ai servizi di video a richiesta e alle piattaforme per la condivisione di contenuti audiovisivi, compresi quelli *on demand*, come *YouTube*, *Netflix*, *iTunes* o *Amazon Video*[74]. Nello specifico, la direttiva rimette agli Stati membri il compito di adottare misure volte a vietare la sponsorizzazione *online* di prodotti dannosi per la salute dei minori, nonché la diffusione sulle piattaforme digitali di contenuti pedopornografici, violenti e di incitamento all'odio o al terrorismo, considerati

[70] Evidenziano la necessità di applicare l'istituto della cancellazione alla luce del superiore interesse del minore V. MONTARULI, *La protezione*, cit., p. 310 e G. PEDRAZZI, *Minori*, cit., p. 449.

[71] V. F. DI PORTO, *La libertà di espressione*, cit.; W. VANDENHOLE, G. ERDEM TÜRKELLI e S. LEMBRECHTS, *Article 17. Access to appropriate information through media*, in in IID., *Children's Rights*, cit., pp. 194-202.

[72] Cfr. direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, 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), in considerazione dell'evoluzione delle realtà del mercato.

[73] Fino al 2018, la tutela dei minori nel contesto dei servizi audiovisivi era contenuta nella 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, c.d. direttiva «SMAV»). In particolare, essa tutelava i minori all'art. 27, imponendo agli Stati membri l'obbligo di adottare misure atte a impedire la trasmissione sulle emittenti televisive di programmi che possono «nuocere gravemente allo sviluppo fisico, mentale o morale dei minori»; cfr., sul punto, S. MICONI, *Servizi di media audiovisivi e tutela dell'utente vulnerabile: il caso del minore*, in *Contratto e impresa*, 2015, pp. 1472-1496, spec. p. 1473.

[74] F. DONATI, *La tutela dei minori nella direttiva 2018/1808*, in *Medialaws*, 2019, pp. 60-72, spec. p. 70, reperibile *online*.

particolarmente dannosi per il loro sviluppo fisico, mentale e morale[75]. Essa, inoltre, pone rigorosi divieti in materia di pubblicità, al fine di impedire lo sfruttamento dell'inesperienza, della credulità e della fiducia dei più piccoli[76], incoraggiando gli Stati membri a ricorrere a strumenti di autoregolamentazione e co-regolamentazione, mediante l'adozione di codici di condotta sia a livello nazionale[77] che a livello europeo. Sotto quest'ultimo profilo, in particolare, l'art. 4 *bis*, c. 2 della direttiva prevede la possibilità per la Commissione, nel rispetto dei principi di sussidiarietà e proporzionalità, di promuovere in cooperazione con gli Stati membri la predisposizione di codici di condotta dell'Unione, elaborati dai fornitori di servizi di media e di piattaforme per la condivisione di video, ovvero da organizzazioni che li rappresentano. A questo proposito, il legislatore europeo ha sottolineato la necessità, da un lato, che tali codici lascino impregiudicati quelli addottati a livello nazionale, dall'altro che essi si sviluppino grazie allo scambio e alla condivisione delle migliori prassi fra i fornitori stessi, così che i codici possano essere accettati dai principali soggetti interessati operanti sul territorio europeo. In Italia, in attesa del recepimento della direttiva (UE) 2018/1808[78], la disciplina relativa ai diritti dei minori e alle nuove tecnologie media e digitali è contenuta nel d.lgs. 31 luglio 2005, n. 177 («Testo Unico sui servizi di media audiovisivi»)[79], in particolare all'art. 34.

Nello spazio virtuale pure alle libertà di pensiero ed espressione, tutelate sia dalla Convenzione delle Nazioni Unite e dalla CEDU che dalla Carta UE dei diritti fondamentali[80], deve essere prestata particolare attenzione, soprattutto nel contesto delle

[75] Cfr. l'art. 6-*bis*, comma 1 della direttiva «SMAV», introdotto dall'art. 10 della direttiva (UE) 2018/1808; in dottrina, v. T. CIMMINO, *Direttiva sui servizi di media audiovisivi e misure nazionali di ordine pubblico*, in *DPCE Online*, 2019, pp. 3005-3010, spec. p. 3010, reperibile *online*.

[76] S. MICONI, *Servizi di media audiovisivi*, cit., p. 1495 ha criticato la struttura stessa degli *spot* pubblicitari destinati ai minori, in quanto essi sono caratterizzati da «una particolare repentinità delle immagini e del messaggio sonoro, fonte di potenziale pregiudizio di carattere psichico (in termini di stress ed equilibrio), fisico (per la vista o l'udito) o anche solo economico (potendo causare condizionamenti)».

[77] Con riguardo al ricorso all'autoregolamentazione e alla co-regolamentazione negli ordinamenti giuridici degli Stati membri, F. DONATI, *La tutela dei minori*, cit., p. 71 s. osserva, da un lato, che il bilanciamento fra libertà d'impresa e di informazione e gli interessi dei minori, perseguito dalla disciplina relativa ai servizi media audiovisivi, dovrebbe essere affidato al potere legislativo, in quanto su di essa opera riserva di legge, dall'altro, che il ricorso a tali strumenti, oltre a permettere l'adozione di discipline differenziate nei diversi Stati membri, può comportare numerosi problemi applicativi.

[78] Gli Stati membri sono tenuti a recepire nei loro ordinamenti interni la direttiva (UE) 2018/1808 entro il 19 settembre 2020, così come previsto dall'art. 2 della stessa; in Italia, la l. 22 aprile 2021, n. 53, Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020, ha conferito al Governo le deleghe necessarie per la predisposizione del decreto legislativo di attuazione della nuova direttiva «SMAV».

[79] D.lgs. 31 luglio 2005, n. 177, Testo unico della radiotelevisione, entrato in vigore l'8 settembre 2005.

[80] Le libertà di espressione e pensiero del minore sono tutelate, rispettivamente, agli artt. 13 e 14 della Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Per un commento alla prima libertà cfr. W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Article 13. Freedom of expression*, in ID., *Children's Rights*, cit., pp. 160-166; per la seconda v., invece, ID., *Article 14. Freedom of thought, conscience and religion*, *ivi*, pp. 167-173; per entrambe cfr. F. DI PORTO, *La libertà di espressione*, cit. Nella CEDU e nella Carta UE dei diritti fondamentali le libertà di pensiero e di espressione sono garantite, rispettivamente, agli artt. 9 e 10 e agli artt. 10 e 11.

piattaforme di comunicazione e dei *social networks*, ove il loro esercizio deve essere bilanciato con quello di altri diritti[81], ad esempio la vita privata e familiare o la salute, grazie anche all'educazione del minore ad un uso più corretto e responsabile della Rete. Ciò dovrebbe avvenire, soprattutto, nelle ipotesi riconducibili al c.d. *conduct risk*, che si verificano quando il bambino diviene vittima di contesti relazionali spiacevoli, che possono sfociare in comportamenti aggressivi a danno della sua salute fisica ed emotiva[82]. Tali maltrattamenti sono dovuti spesso al fatto che i più piccoli, credendosi «protetti» dallo schermo del *computer*, oltre che ad essere spinti da naturale immaturità e curiosità, sono portati a sentirsi più sicuri rispetto ad una situazione reale e, dunque, ad abbassare la guardia nei confronti di contatti e richieste pure da parte di sconosciuti[83]. Per questo è fondamentale che anche nello spazio digitale venga loro garantita protezione contro ogni forma di violenza[84], compresa quella a sfondo sessuale, così come stabilito dagli artt. 19 e 34 della Convenzione delle Nazioni Unite[85]. Nell'ambito della cooperazione giudiziaria in materia penale, con particolare riguardo all'abuso e allo sfruttamento minorile, l'Unione europea ha adottato la direttiva 2011/93/CE[86] con l'intento, da un lato, di introdurre nuove e più incisive misure di contrasto alle principali fattispecie penali aventi carattere sessuale, dall'altro di fornire una risposta significativa al fenomeno dello sfruttamento minorile, favorito ed, anzi, aumentato a causa delle nuove tecnologie, che

---

[81] Cfr. G. MANCOSU, *Le droit à la liberté d'expression de l'enfant à l'heure des plateformes de socialisation en ligne et les chantiers ouverts en Italie*, in *Federalismi.it.*, 2020, pp. 62-75, spec. p. 69 ss., reperibile *online*.

[82] Per riprendere la classificazione effettuata dal progetto *EU Kids Online Network*, nell'ambito del *Safer Internet Programme* istituito dalla Commissione europea con Decisione 1351/2008/CE è possibile distinguere tra *content risk*, ove l'attenzione è posta sull'esposizione del minore a contenuti lesivi *online*, *contact risk*, ove è rilevante la partecipazione di un minore, anche non volontaria, ad un'iniziativa di un adulto, e *conduct risk*, ove il minore d'età, coinvolto in un contesto relazionale tra pari, diviene «vittima» dei comportamenti dei suoi coetanei; cfr. decisione 1351/2008/CE, cit.

[83] Cfr. I. SALVADORI, *L'adescamento di minori. Il contrasto al* child-grooming *tra incriminazione di atti preparatori ed esigenze di garanzia*, Torino, 2018, p. XVI.

[84] Una vita libera dalla violenza rientra anche fra le cinque aree di priorità chiave della Strategia del Consiglio d'Europa sui diritti dei minori (2016-2021), ove la tutela delle persone di minore età è ritenuta «a legal, ethical and economic imperative». Cfr. S. DE VIDO, *La CRC e le convenzioni del Consiglio d'Europa a tutela dell'infanzia e dell'adolescenza*, in *La Convenzione delle Nazioni Unite*, cit., pp. 43-62, spec. p. 43.

[85] Relativamente agli artt. 19 e 34 della Convenzione ONU, cfr. W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Article 19. Protection from all forms of violence*, in ID., *Children's Rights*, cit., pp. 209-221; ID., *Art. 34. Protection from sexual exploitation and abuse*, *ivi*, pp. 334-342. Per entrambi v. A. LEANDRO, C. ZONILE, *La tutela da ogni forma di violenza*, in AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *La Convenzione delle Nazioni Unite*, cit., pp. 258-272.

[86] Cfr. direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, cit. Nel luglio 2020 la Commissione europea si è impegnata a proporre, entro il secondo trimestre del 2021, la legislazione necessaria per contrastare più efficacemente gli abusi sessuali su minori *online*; cfr. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori, COM(2020) 607 final del 24 luglio 20. In Italia, la direttiva 2011/93/UE è stata recepita con il d.lgs. 4 marzo 2014, n. 39, Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI, entrato in vigore il 06.04.14.

hanno reso più agevole l'accesso e la diffusione di materiale pedopornografico[87]. Nel fare ciò, Parlamento europeo e Consiglio, ispirandosi espressamente alla Convenzione del Consiglio d'Europa adottata a Lanzarote nel 2007[88], hanno sviluppato un catalogo più ampio e preciso di reati perpetuati contro i minori, tra i quali emergono, soprattutto, la pedopornografia, l'abuso sessuale e l'adescamento di soggetti minorenni per scopi sessuali, conosciuto anche come *child-grooming*. Tale ultima fattispecie delittuosa, in particolare, è introdotta all'art. 6, par. 1 della direttiva 2011/93/UE, il quale impone ai legislatori nazionali di punire la condotta posta in essere dall'adulto che, tramite le nuove tecnologie dell'informazione e della comunicazione, propone al minore di incontrarlo con l'intento di compiere atti sessuali o di produrre materiale pedopornografico. L'esplicito riferimento all'uso di Internet per la realizzazione dell'adescamento minorile, oltre a rendere il reato a forma vincolata, ha sollevato alcune perplessità, dal momento che non vengono prese in considerazione le condotte altrettanto pericolose poste in essere da chi ha un contatto fisico con il minore[89]. Ciononostante, l'indicazione contenuta all'interno dell'art. 6, par. 1 della direttiva dimostra come il legislatore europeo abbia voluto evidenziare la natura allarmante dell'*online-grooming*, che costituisce sempre più spesso una grave minaccia per i minori a causa dall'anonimato garantito ai soggetti attivi, che, così facendo, possono nascondere con facilità la loro età e le loro reali intenzioni[90]. Oltre a condannare il reato di adescamento per scopi sessuali, la direttiva obbliga gli Stati membri a punire le condotte di accesso a materiale pedopornografico realizzate tramite tecnologie digitali, tra le quali rientra anche la c.d. «pornografia virtuale», consistente nella detenzione o riproduzione di immagini che, pur non coinvolgendo una persona davvero esistente, ritraggono realisticamente un minore in atteggiamenti sessualmente espliciti[91]. Con riguardo a tali condotte di reato, il legislatore ha previsto l'obbligo per gli Stati membri di bloccare il materiale presente *online*, eliminandolo sia dalle pagine *web*

[87] M. TROGLIA, *Lotta contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile: alcune riflessioni sulla direttiva 2011/93/UE del Parlamento e del Consiglio del 13 dicembre 2011*, in *Cassazione penale*, 2012, pp. 1906-1918, spec. p. 1907.

[88] V. Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali, firmata a Lanzarote il 25 ottobre 2007. La direttiva 2011/93/UE si riferisce espressamente ad essa nel considerando 5, ove tale Convenzione viene definita una «tappa fondamentale verso il miglioramento della cooperazione internazionale in questo settore»; cfr. G. MAGNO, *La condizione della persona di minore età nelle principali convenzioni internazionali e nei regolamenti europei*, in *Minori giustizia*, 2013, pp. 160-196, spec. p. 184.

[89] Sul punto v. I. SALVADORI, *L'adescamento di minori*, cit., p. 20 s.

[90] M. TROGLIA, *Lotta contro l'abuso*, cit., p. 1910.

[91] La rilevanza penale delle c.d. pornografia virtuale è dibattuta in sede extraeuropea, in quanto le condotte riconducibile alla fattispecie in esame non offenderebbero un vero e proprio soggetto passivo, ma solamente una simulazione di esso. Sulla questione è rilevante la conclusione cui è giunta la *Supreme Court of Canada* (26 January 2001, case number 27376), in quanto sembra essere la più simile a quella prevista dall'art. 5, comma 8 della direttiva 2011/93/UE, che prevede la punibilità di tale reato soltanto a patto che esso non sia commesso ad esclusivo uso privato; cfr., sul punto, B. GIORS, *L'impegno dell'Unione europea contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia*, in *Minori giustizia*, 2012, pp. 217-223, spec. p. 219; M. TROGLIA, *Lotta contro l'abuso*, cit., p. 1912.

che dai *server*. Particolarmente significativa, infine, è la previsione di cui all'art. 20 della direttiva 2011/93/CE relativa all'audizione del minore, che dovrebbe svolgersi soltanto se strettamente necessaria ai fini dell'indagine e del procedimento penale, preferibilmente ricorrendo all'uso di appropriate tecnologie di comunicazione, come ad esempio l'esame a distanza tramite collegamento audiovisivo, così come previsto anche dalla direttiva 2012/29/UE[92] in materia di diritti, assistenza e protezione delle vittime di reato[93].

Per concludere l'analisi sino a qui svolta, infine, è importante ricordare l'istruzione quale diritto fondamentale atto a garantire inclusione, partecipazione e socializzazione ai soggetti in età evolutiva, tutti aspetti essenziali per lo sviluppo della loro personalità. Proprio in virtù del ruolo riservato all'educazione nella vita dei minorenni, essa è tutelata in tutti gli strumenti internazionali ed europei posti a salvaguardia dei diritti umani[94], nonché negli atti adottati dall'Unione[95], tra i quali è rilevante il «Piano d'azione per l'istruzione digitale 2021-2027»[96], che propone il ricorso a soluzioni d'insegnamento innovative in un'ottica di promozione dello sviluppo tecnologico, senza dimenticare i diritti fondamentali dei soggetti più vulnerabili. Nel fare ciò, il Piano prevede lo sviluppo di tre priorità, che possono riassumersi nel miglioramento dell'utilizzo delle tecnologie digitali nel campo dell'insegnamento e dell'apprendimento, nel potenziamento delle competenze e delle capacità tecnologiche di alunni e docenti, nell'analisi dei dati e, infine, nella raccolta di buone pratiche da condividere tra gli insegnanti. Nel rispetto di tali obiettivi, l'Unione europea intende adottare specifiche misure, tra le quali emerge

[92] Direttiva 2012/29/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2012, cit.

[93] Il ricorso a forme di audizione del minore diverse dalla normale presenza fisica in udienza risponde alla necessità di bilanciare il principio dei *best interests of the child* della vittima minorenne, che in caso di normali interrogatori potrebbe essere soggetto a gravi danni emotivi, con gli altri interessi contrapposti, fra tutti quello dell'imputato ad un equo processo, da svolgersi secondo i principi e le garanzie proprie del diritto processuale penale. Il legislatore nazionale non sembra aver recepito in maniera chiara e precisa la regola prevista nella direttiva 2012/29/UE circa l'esame a distanza del testimone minore d'età, tanto che il ricorso a tale possibilità non sembra essere presente nell'ordinamento italiano; cfr., per entrambe le questioni, A. GAUDIERI, *Il principio dei "best interests of the child"*, cit., p. 124 ss.

[94] Il diritto all'istruzione è tutelato, sul piano internazionale, dall'art 2 CEDU e dall'art. 2 Protocollo 1 CEDU, nonché dagli artt. 28 e 29 della Convenzione ONU; a livello europeo, dall'art. 14 della Carta UE dei diritti fondamentali; per un commento in dottrina cfr. A. DI STEFANO, *Il diritto all'educazione*, in *La Convenzione delle Nazioni Unite*, cit., pp. 273-291; W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Article 28. Right to education*, in ID., *Children's Rights*, cit., pp. 288-298; ID., *Article 29. Aims of education*, *ivi*, pp. 299-302.

[95] Cfr. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sulla realizzazione dello spazio europeo dell'istruzione entro il 2025, COM(2020) 625 final del 30 settembre 2020; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Piano d'azione per l'istruzione digitale 2021-2027. Ripensare l'istruzione e la formazione per l'era digitale, COM(2020) 624 final del 30 settembre 2020; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sul piano d'azione per l'istruzione digitale, COM(2018) 22 final del 17 gennaio 2018. Nel contesto della transizione digitale, il Consiglio europeo si è proposto di disporre almeno il 20% dei fondi previsti dal dispositivo per la ripresa e la resilienza per «migliorare le capacità digitali nei sistemi di istruzione»; cfr. conclusioni della riunione straordinaria del Consiglio europeo del 1° e 2 ottobre 2020.

[96] Cfr. comunicazione della Commissione, Piano d'azione per l'istruzione digitale 2021-2027, cit.

l'acquisto di attrezzature digitali capaci di garantire equità e qualità nell'accesso ai contenuti didattici da parte dei minori, allo scopo sia di fronteggiare il divario di connettività nel campo dell'apprendimento che di promuovere l'alfabetizzazione digitale. Si tratta di azioni che la Commissione si è impegnata ad attuare in quanto, nel settore dell'istruzione, i vantaggi apportati dall'uso di Internet in termini di semplicità, prossimità, rapidità e diffusione[97] devono spesso fronteggiare altrettanti profili negativi, che possono tradursi in rischi per i diritti fondamentali dei minori, come ad esempio il *digital divide*[98], conseguenza derivante della scarsa o mancata connettività che caratterizza alcuni territori degli Stati membri. Le nuove modalità di apprendimento offerte dallo sviluppo tecnologico, inoltre, hanno svelato la presenza anche di altre insidie, che possono sfociare in condotte di cyberbullismo[99] o in violazioni della *privacy* del minore[100]. La scuola «digitale», infine, può rappresentare una barriera per i soggetti più vulnerabili, come ad esempio i minori portatori di disabilità o con difficoltà di apprendimento, i quali necessitano di piani educativi individuali, che mal si adattano all'impiego del *web* e delle tecnologie informatiche.

3. Alcune riflessioni conclusive: la pandemia da Covid-19 e la nuova Strategia europea sui diritti dei minori.

L'evoluzione digitale ha posto l'Unione europea di fronte a nuove e molteplici sfide in termini di tutela dei diritti dei minori, obbligando Stati membri e istituzioni a rimodulare i propri obiettivi al fine di adeguarli al fenomeno di Internet e al ricorso senza precedenti alle tecnologie multimediali. Anche l'emergenza sanitaria internazionale dovuta alla pandemia da Covid-19 ha rivoluzionato significativamente la società attuale, imponendo un ripensamento in chiave digitale dei diritti fondamentali dei minori, che sono stati costretti ad adattarsi a situazioni originali ed inaspettate di godimento delle loro

[97] M.N. CAMPAGNOLI, *Diritto all'educazione e nuove tecnologie. Sulla necessità di un approccio consapevole*, in *dirittifondamentali.it*, 2019, pp. 1-14, spec. p. 11, reperibile online; L. LODEVOLE, *L'uso delle tecnologie digitali nel contesto della scuola: attività didattiche, comunicazioni scuola-famiglia e rilievi penalistici*, in *Informatica e diritto*, 2017, pp. 419-435, spec. p. 423, reperibile online.

[98] L'espressione «*digital divide*» descrive la differenza che può intercorrere tra diversi Paesi nell'accesso alle Rete, inclusa la diversa distribuzione delle tecnologie digitali e la disomogenea diffusione delle competenze necessarie per utilizzare le potenzialità degli strumenti informatici; per un'analisi più approfondita v. G. SARACENI, *Digital divide e Povertà*, in *dirittifondamentali.it*, 2019, pp. 1-19, spec. p. 6, reperibile online. Una scarsa o assente connettività potrebbe violare anche il divieto di discriminazione, posto a tutela dei minori dagli artt. 21 della Carta UE, 14 CEDU e 2 Convenzione ONU, con gravi ripercussioni sul loro sviluppo armonioso ed equilibrato; sulla violazione del divieto di discriminazione quale conseguenza dell'uso delle nuove tecnologie digitali cfr. F. MODUGNO, *Breve discorso intorno all'uguaglianza. Studio di una casistica: i minori e i nuovi* media, in *Osservatorio AIC. Bimestrale di attualità costituzionale*, 2014, pp. 1-7, reperibile online.

[99] V. L. LODEVOLE, op. cit., p. 423.

[100] Cfr. R.M. COLANGELO, *Istituzioni scolastiche e trattamento online dei dati personali di studenti minorenni*, in *Annali Online della Didattica e della Formazione Docente*, 2017, pp. 72-89, reperibile online.

libertà[101]. Ad esempio, nell'ambito del rispetto della vita privata e familiare, soprattutto durante le prime fasi della pandemia, il ricorso alla tecnologia ha rappresentato un'utile alternativa al regolare godimento del diritto di visita dei genitori non affidatari, quale aspetto essenziale del diritto alla bigenitorialità, garantito ai minori dagli artt. 8 CEDU e 24, par. 3 della Carta UE dei diritti fondamentali[102]. In Italia, al fine di permettere il mantenimento del rapporto con la prole, il giudice ha spesso incentivato il genitore a ricorrere a strumenti informatici, come videochiamate *Skype*, *chat* o altre applicazioni di messaggistica, quale *Whatsapp*[103], previo bilanciamento con il contrapposto interesse alla salute e sempre che ciò avvenga per un tempo limitato, ritenendo dunque più opportuno individuare modalità telematiche di frequentazione che possano assicurare il costante contatto con i figli senza mettere a rischio la loro integrità psico-fisica[104]. A tale orientamento, tuttavia, si è affiancata una seconda interpretazione giurisprudenziale, che ha invece privilegiato il diritto-dovere dei genitori e dei figli di incontrarsi personalmente, in quanto, a parere dei giudici, le limitazioni alla circolazione dovute alla crisi sanitaria non devono incidere sulla frequentazione della prole, fatta salva, naturalmente, la valutazione concreta della situazione familiare e del rischio per il minore di pregiudicare la propria salute[105]. Con riguardo al diritto di informazione e partecipazione, invece, è

[101] Pur consapevole di dover imporre rigide restrizioni allo scopo di fronteggiare la pandemia da Covid-19 e, dunque, di tutelare la salute privata e collettiva dei suoi cittadini, l'Unione europea ha incoraggiato e invitato gli Stati membri al continuo rispetto dei diritti umani, compresi quelli dei minori d'età, anche adottando soluzioni coraggiose ed innovative. Cfr. risoluzione del Parlamento europeo del 13 novembre 2020 sull'impatto delle misure connesse alla COVID-19 sulla democrazia, sullo Stato di diritto e sui diritti fondamentali (2020/2790(RSP)).

[102] Il diritto alla bigenitorialità, rilevante soprattutto nelle ipotesi di dissoluzione del vincolo matrimoniale, viene spesso garantito alla luce del principio dei *best interests of the child* tramite l'istituto dell'affidamento condiviso del minore e il diritto di visita. Proprio il rispetto dell'interesse superiore del minore rappresenta, tuttavia, un limite per l'adozione di misure standardizzate o per l'esecuzione di provvedimenti giudiziali in contrasto con i diritti del bambino; cfr. V. COLUCCI, op. cit.; V. PICCONE, op. cit.; M. RENNA, *Affidamento del minore, bigenitorialità e alienazione parentale*, in *Familia*, 2020, pp. 439-456; E. BARONI, *Principio di bi genitorialità e giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *Minori giustizia*, 2018, pp. 229-237.

[103] Così Trib. Terni, ord. 30 marzo 2020, reperibile alla banca dati *Pluris*; per un'analisi della sentenza, v. E. TROTTA, *Esercizio della responsabilità genitoriale e diritto alla bigenitorialità in pendenza delle misure di contrasto al Covid-19*, in *Famiglia e diritto*, 2020, pp. 442-450. Durante la prima fase dell'emergenza pandemica si sono pronunciati allo stesso modo anche Trib. Napoli, sez. I, ord. 26 marzo 2020; App. Bari, sez. min., ord. 26 marzo 2020, entrambe reperibili alla banca dati *DeJure*; in dottrina, a commento delle sentenze citate, cfr. A. ABBRUZZESE, *Diritto di visita e Covid-19: tra interesse del minore, responsabilità genitoriale e diritto alla salute*, in *Giustiziacivile.com*, in *Speciale Emergenza Covid-19*, 5 agosto 2020, pp. 1-15, spec. p. 4 ss., reperibile *online*; G.O. CESARO, *Covid-19 e diritti fondamentali nell'ambito della famiglia e dei minori: tra limitazioni ordinarie e straordinarie*, in *D&G*, 12 maggio 2020; C. IRTI, *Relazioni familiari e Covid-19: la difficile ricerca di un equilibrio tra la salvaguardia del diritto alla salute pubblica e gli altri diritti fondamentali*, in *Familia*, 2020, pp. 683-697, spec. p. 685; D. PIAZZONI, *Diritto alla bigenitorialità, diritto di visita e frequentazione e coronavirus: un mosaico in composizione*, in *Giustiziacivile.com*, in *Speciale Emergenza Covid-19*, 4 maggio 2020, pp. 1-22, spec. p 4 ss., reperibile *online*.

[104] V. G. FREZZA, *Abitazione e "confinamento". Covid-19, diritto di visita del genitore non affidatario e successione* mortis causa *nel diritto abitativo*, in *Diritto della famiglia e delle persone*, 2020, pp. 1140-1154, spec. p. 1143.

[105] Cfr. Trib. Lecce, sez. II, ord. 9 aprile 2020; Trib. Roma, sez. I, decr. 7 aprile 2020; Trib. Brescia,

rilevante segnalare le indicazioni fornite dalla Rete Europea dei Garanti per l'Infanzia e l'Adolescenza (ENOC), che ha evidenziato l'importanza, in tempo di pandemia, di diffondere notizie accurate e corrispondenti alla realtà, affinché nel corso delle loro ricerche sul *web* i minori possano comprendere chiaramente la pericolosità del virus e le limitazioni alle loro libertà personali, evitando *fake news* e informazioni non consone alla loro età[106]. Nel corso della crisi emergenziale dovuta al Covid-19, invero, le sfide maggiori sono emerse nel campo dell'istruzione, ove le amministrazioni sono state obbligate a valutare metodi di didattica innovativi e del tutto dipendenti dalle tecnologie digitali. L'esempio più significativo si rinviene nella c.d. didattica a distanza (o «DAD»), quale unico strumento capace di assicurare la continuità del diritto allo studio dei minori in seguito al confinamento domestico e alle limitazioni agli spostamenti personali. In particolare, essa si è distinta per due diverse modalità educative, che prevedono, da un lato, la didattica online asincrona («DOA»), caratterizzata da lezioni preparate e registrate anticipatamente, messe a disposizione su piattaforme di gestione quali *Moodle* o *BlackBoard* e supportate da *e-mail*, materiali *online*, forum di discussione e *social media*, dall'altro la didattica online sincrona («DOS»), durante la quale gli studenti, non trovandosi fisicamente nell'ambiente scolastico, sono collegati in videoconferenza o audioconferenza con gli insegnanti, con i quali possono comunicare attraverso *chat* e altri dispositivi di messaggistica istantanea[107]. In tale contesto, è innegabile che la chiusura delle scuole causata dalla crisi pandemica ha costituito un'occasione di ripensamento, anche in un'ottica positiva, dei metodi educativi, ad esempio attraverso la differenziazione delle modalità di apprendimento e la valorizzazione delle capacità inclusive degli strumenti didattici telematici. Tuttavia, in generale sembrano predominare i profili di criticità, dovuti all'insufficiente disponibilità all'interno dei nuclei familiari degli strumenti tecnologici necessari per accedere all'insegnamento *online* o alla scarsa copertura digitale di alcuni territori degli Stati membri, col rischio, in buona sostanza, di generare nei minori disuguaglianze sociali, evolutive e pedagogiche, che potrebbero causare loro conseguenze dannose ed irreparabili[108].

Gli esempi citati dimostrano come il ricorso alla tecnologia si sia dimostrato indispensabile per reagire all'emergenza pandemica che ha investito la società attuale. In

decr. 31 marzo 2020, tutte reperibili alla banca dati *DeJure*; Trib. Milano, sez. IX, decr. 11 marzo 2020, reperibile alla banca dati *Pluris*.

[106] Cfr. Rete europea dei Garanti per l'infanzia e l'adolescenza (ENOC), *I diritti dei minorenni nel contesto dell'epidemia di COVID-19*, 1 aprile 2020. Sull'importanza di garantire informazioni adeguate nel contesto della pandemia, al fine di evitare il diffondersi di *fake news*, v. F. LAJOLO DI COSSANO, *Il diritto di informazione ai tempi del Coronavirus: un diritto fondamentale*, in *dirittifondamentali.it*, 10 aprile 2020, reperibile *online*.

[107] Si veda S. BARONCELLI, *La didattica online al tempo del coronavirus: questioni giuridiche legate all'inclusione e alla* privacy, in *Osservatorio sulle fonti*, 2020, pp. 437-451, spec. p. 438 s., reperibile *online*.

[108] Cfr., sul punto, G.O. CESARO, *Covid-19 e diritti fondamentali*, cit.; S. DE VIDO, *Diritto all'istruzione e accesso a internet all'epoca del Covid-19*, in *SidiBlog*, 20 aprile 2020, reperibile *online*.

tale contesto, proprio la crisi sanitaria dovuta al diffondersi del Covid-19 sembra aver contribuito ad accelerare l'andamento della rivoluzione digitale, evidenziando, in questo modo, l'inadeguatezza degli strumenti legislativi attualmente in vigore. Al momento della loro adozione, infatti, il legislatore non poteva immaginare che le tecnologie dell'informazione e della comunicazione si sarebbero diffuse sino a permeare la quotidianità degli individui, cambiando radicalmente le loro abitudini sociali e il modo di vivere e relazionarsi delle persone[109], né che gli ordinamenti giuridici internazionali sarebbero stati costretti ad affrontare una crisi sanitaria di tale diffusione. Proprio alla luce di siffatte considerazioni, appare chiara la necessità di procedere con un aggiornamento della normativa esistente posta a tutela dei diritti dell'infanzia, in quanto gli strumenti attualmente in vigore non si sono dimostrati pienamente capaci di contrastare le insidie presenti nel mondo di Internet. In risposta a tali esigenze, l'Unione europea sembra aver già intrapreso un percorso di innovazione, adottando il 24 marzo 2021 una nuova strategia generale sui diritti dei minori[110], nonché una proposta di raccomandazione che istituisce una garanzia europea per l'infanzia[111], le quali, a partire dalle indicazioni fornite dagli Stati membri e dai portatori d'interesse raccolte fra settembre e dicembre 2020 nel corso di una consultazione pubblica[112], si propongono lo scopo di fornire il nuovo quadro programmatico di promozione e salvaguardia degli interessi dei soggetti in età evolutiva. La nuova Strategia, nello specifico, si basa su sei aree tematiche che promuovono azioni mirate in settori quali la partecipazione democratica, la povertà e l'esclusione sociale, la lotta alla violenza, la giustizia e gli aiuti umanitari. Nell'ambito di tale strumento, soprattutto, risulta particolarmente rilevante l'impegno assunto dalla Commissione relativo alla sicurezza informatica e digitale, per la quale l'Istituzione si è proposta, prima, di aggiornare la propria «Strategia per un Internet migliore per i ragazzi» del 2012 e, successivamente, di promuovere l'attuazione negli Stati membri di norme sulla protezione dei minori e sullo sviluppo delle loro competenze digitali di base. Sembra dunque che l'intento dell'Unione sia quello di rendere Internet un luogo sempre più adatto ai minori, ove essi possano sentirsi liberi di giocare, socializzare, sviluppare idee proprie, imparare e crescere, mentre agli studiosi e agli operatori del diritto rimarrà il compito di valutare se, nel concreto, le misure varate sapranno soddisfare le aspettative rimaste, in parte, ancora deluse.

---

[109] Cfr. W. VANDENHOLE, G. ERDEM TÜRKELLI, S. LEMBRECHTS, *Article 17*, cit., p. 201.

[110] Cfr. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Empty, EU Strategy on the Rights of the Child, COM(2021) 142 final of 24 March 2021.

[111] Proposal for a Council Recommendation, Establishing a European Child Guarantee, COM(2021) 137 final of 24 March 2021

[112] Sul sito della Commissione europea è possibile reperire tutta la documentazione e le informazioni riguardanti la consultazione pubblica relativa all'adozione della nuova Strategia dell'UE sui diritti del minore.

ABSTRACT: Il contributo si propone di esaminare i diritti fondamentali dei minori nel contesto delle nuove tecnologie dell'informazione e della comunicazione, analizzando vantaggi e svantaggi della rivoluzione digitale nell'ordinamento giuridico europeo, anche alla luce dell'emergenza sanitaria dovuta al diffondersi del Covid-19.

PAROLE CHIAVE: Minori; diritti fondamentali; best interests of the child; rivoluzione digitale; Covid-19.

Minors 4.0 and protection of fundamental rights in the age of digitalisation: what challenges for the European Union?

ABSTRACT: This contribution aims to examine minors' fundamental rights in the context of new information and communication technologies (ICT), analyzing advantages and disadvantages of the digital revolution within the European legal order, also in the light of the health emergency due to the spread of Covid-19.

KEYWORDS: Minors; fundamental rights; best interests of the child; digital revolution; Covid-19.

La nuova strategia della Commissione europea in tema di finanza digitale: *quid iuris* per i (futuri) servizi finanziari offerti dalle società *Tech*?

Mattia Mengoni*

SOMMARIO: 1. Contesto di riferimento: il caso *Ant Group* e *Amazon-Barclaycard Germany*. – 2. Intelligenza artificiale e sistema finanziario. – 3. Rischi connessi all'innovazione tecnologica. – 3.1. Standardizzazione dei comportamenti. – 3.2. *Bias* e discriminazione. – 3.3. Trasparenza. – 3.4. Lacune normative. – 4. La risposta della Commissione europea: il principio «stessa attività, stesso rischio, stesse norme». – 5. Prime considerazioni. – 5.1. La strategia europea come primo passo necessario. – 5.2. L'opportunità di un c.d. *regulatory sandbox*?

1. Contesto di riferimento: il caso *Ant Group* e *Amazon-Barclaycard Germany*.

In seguito alla c.d. prima ondata del virus Sars-Cov-2, il ricorso alle tecnologie digitali è stato individuato come uno dei mezzi necessari al fine di modernizzare l'economia europea e ristabilire, più in generale, condizioni di benessere per i cittadini europei[1]. L'emergenza sanitaria che stiamo affrontando in questo periodo ha, in effetti, assunto i connotati anche di una crisi economica di natura esogena con notevoli impatti sia sul tasso di disoccupazione dei settori maggiormente colpiti, sia sulla stabilità finanziaria del mercato dei capitali. Con riferimento a quest'ultimo settore, le istituzioni europee hanno, in particolare, affermato che una priorità chiave al fine della ripresa economica è rappresentata dalla transizione digitale, ossia dall'applicazione sistemica di innovazioni tecnologiche nelle fondamentali attività di raccolta, gestione e allocazione del capitale[2].

La dottrina tende a ricomprendere all'interno del concetto di finanza digitale, ovvero con il termine entrato nel gergo comune degli addetti ai lavori «*fintech*», le *start-up* innovative e/o le società tecnologiche che svolgono attività tradizionalmente bancarie mediante l'utilizzazione di strumenti tecnologici (piattaforme *online*, applicazioni per

*Dottorando di ricerca in Scienze giuridiche europee ed internazionali, Università degli Studi di Verona.

[1] Si veda a tal proposito la comunicazione al Parlamento europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final del 19 febbraio 2020.

[2] Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato per le regioni, *Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione*, COM (2020) 456 final del 27 maggio 2020.

smartphone) basati sulla rete Internet[3]. Questa apertura del mondo della finanza a nuovi operatori economici ha consentito, a sua volta, di estendere la platea degli utenti di servizi finanziari anche a quei soggetti, persone fisiche e piccole e medie imprese, che non hanno i requisiti di meritevolezza del credito storicamente chiesti dagli intermediari creditizi come *condicio sine qua non* per la concessione, a vario titolo, di linee di credito[4]. La diffusione capillare di informazioni sui servizi finanziari mediante canali informatici ormai accessibili da parte della stragrande maggioranza della popolazione globale ha già permesso, infatti, a soggetti previamente esclusi dal mercato dei capitali di usufruire di prodotti finanziari a basso costo come, ad esempio, i servizi di pagamento tramite moneta elettronica, il *crowdfunding* e, più in generale, il prestito di somme mediante piattaforme elettroniche[5].

Il successo riscontrato sul mercato finanziario dalle prime realtà *fintech* ha destato, però, fin da subito l'attenzione sia delle pubbliche autorità, sia di altri operatori economici

[3] Per una breve ricostruzione della nozione di *fintech* si veda W. MAGNUSON, *Regulating Fintech*, in *Vanderbilt Law Review*, 2018, n. 4, pp.1167-1226, spec. p. 1174, laddove si sottolinea in particolare l'ambiguità del termine in esame, usato a vario titolo sia per definire, in senso ampio, qualsiasi applicazione della tecnologia all'attività finanziaria, sia in chiave restrittiva per intendere soltanto quelle ipotesi di intermediazione finanziarie offerte direttamente al consumatore finale attraverso soluzioni innovative basate sulla connessione internet. L'utilizzazione di una nozione ampia del termine *fintech* si rinviene, per esempio, nel documento congiunto del *Financial Stability Board* (FSB) e del *Committee on the Global Financial System* (CGFS) della Banca dei Regolamenti Internazionali (BIS), *FinTech credit. Market structure, business models and financial stability implications*, 22 May 2017, p. 2, reperibile *online*, laddove si afferma testualmente che «"FinTech" can be broadly defined as technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets, financial institutions and the provision of financial services»; in senso conforme cfr. anche il lavoro a cura di F. MAIMERI, M. MANCINI, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, in *Quaderni di Ricerca Giuridica della Banca d'Italia*, settembre 2019, n. 87, p. 23, reperibile *online*, in cui si afferma che con il termine *fintech* «ci si riferisce alla Financial Technology, ossia all'offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica, che comportano forti spinte innovative nel mercato dei servizi finanziari». Sul tema è utile richiamare anche la collana dei *Quaderni FinTech* della Consob, in particolare il lavoro di A. SCIARRONE ALIBRANDI, G. BORELLO, R. FERRETTI, F. LENOCI, E. MACCHIAVELLO, F. MATTASSOGLIO, F. PANISI, *Marketplace lending. Verso nuove forme di intermediazione finanziaria?*, in *Quaderni FinTech*, p. 19, reperibile *online*, in cui viene posto l'accento sul concetto di piattaforma per lo sviluppo dell'universo *fintech*.

[4] Cfr. le parole del Governatore della Banca d'Inghilterra, il quale, nell'affrontare la tematica dell'apertura del mondo della finanza alla generalità della popolazione, ha utilizzato il termine «democratizzazione dei servizi finanziari»: M. CARNEY, *The Promise of FinTech – Something New Under the Sun?*, discorso svolto durante la conferenza Bundesbank G20 «*Digitising finance, financial inclusion and financial literacy*», tenutasi a Wiesbaden il 25 gennaio 2017, reperibile *online*.

[5] Cfr. sul punto, tra gli altri, R. SHARMA, *Technology will save emerging markets from sluggish growth*, in *Financial Times*, 11 April 2021, in cui si rileva che in Stati come il Kenya, sebbene soltanto il cinque percento della popolazione disponga di una carta di credito, più del settanta percento dei kenioti hanno comunque accesso a servizi di «digital banking»; D.A. ZETZSCHE, D.W. ARNER, R.P. BUCKLEY, B. TANG, *Artificial Intelligence in Finance: Putting the Human in the Loop*, in CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, no. 1, University of Hong Kong Faculty of Law Research Paper No. 2020/006, reperibile *online*; K. ALEXANDER, *Principles of Banking Regulation*, Cambridge, 2019, p. 330 ss.; D.W., ARNER, J. BARBERIS, R.P. BUCKLEY, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, University of Hong Kong Faculty of Law Research Paper No. 2016/035, 2016, reperibile *online*.

desiderosi di lucrare una parte dei guadagni derivanti dall'applicazione di metodi ad alta intensità tecnologica. Quanto alle prime, l'interesse verso le nuove tecnologie finanziarie è stato mosso principalmente dalla constatazione di politica del diritto che le società *fintech*, benché abbiano come *core business* la fornitura di servizi finanziari, non possono essere definite, da un punto di vista legale, come entità bancarie. Più esattamente, sebbene gli strumenti tecnologici utilizzati nel settore in esame consentano l'offerta di finanziamenti in misura similare alle banche, i c.d. nuovi *players* del mercato finanziario non impiegano risparmi raccolti dal pubblico al fine di fornire prestiti al settore economico e, pertanto, non ricadono all'interno della nozione di banca, o di attività bancaria[6]. Di conseguenza, le società *fintech* svolgono la propria attività finanziaria al di fuori del campo di applicazione della normativa bancaria di matrice prudenziale, beneficiando in concreto di una libertà di impresa non ristretta dai limiti operativi imposti, invece, agli intermediari creditizi tradizionali[7]. In tale contesto, oltre a valutazioni di salvaguardia della concorrenza, le autorità di vigilanza si sono preoccupate precipuamente della tenuta sistemica del mercato finanziario, messo a repentaglio dalla naturale inesperienza delle società tecnologiche nel gestire rischi derivanti dall'attività di intermediazione creditizia, auspicando interventi normativi in grado di eliminare situazioni di arbitraggio regolamentare[8].

Quanto alle dinamiche concorrenziali, è stato, invece, sostenuto che gli esiti positivi del connubio tra nuove tecnologie e mercato finanziario, uniti a fattori dirompenti come la disponibilità di dati, convenzionali e non, sulle abitudini di vita della popolazione e la presenza di algoritmi in grado di processare *big data* per scopi predittivi, hanno stimolato società tecnologiche attive in prevalenza nei settori dell'*e-commerce* o dei *social network* ad affiancare alle rispettive attività costitutive la fornitura di servizi intrinsecamente finanziari (c.d. *TechFins*)[9]. Esempi emblematici di tale *trend* economico sono

[6] Sulla nozione legislativa di banca di matrice euro-unitaria cfr. l'art. 4, par. 1, n. 1, del regolamento (UE) 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) 648/2012 (c.d. CRR) in cui si stabilisce che per ente creditizio si deve intendere qualsiasi impresa ‹‹la cui attività consiste nel raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto››; in dottrina, cfr. E. MACCHIAVELLO, *FinTech. Problematiche e spunti per una regolazione ottimale*, in *Mercato Concorrenza Regole*, n. 3, 2019, pp. 435-473, a p. 461, in cui si cita come esempio paradigmatico di attività fintech non riconducibili al paradigma dell'ente creditizio quello del *marketplace lending*, cioè di un'attività di intermediazione creditizia in cui viene agevolata la connessione tra consumatori, ovvero tra consumatori e imprese, svolgendo all'uopo una funzione similare a quella esercitata da *broker* e/o da mercati regolamentati.

[7] Si v. sul punto il lavoro di H. GENBERG, *Digital Transformation: Some implications for financial and macroeconomic stability*, in ADBI Working Paper Series, Asian Development Bank Institute, No.1139/2020, p. 5, reperibile *online*, in cui si afferma che l'emersione di nuove imprese che svolgono servizi finanziari può essere qualificabile ad una sorta di liberalizzazione del mercato finanziario.

[8] In tal senso, si vedano le riflessioni del FSB, *Artificial intelligence and machine learning in financial services. Market developments and financial stability implications*, 2017, reperibile *online*.

[9] Sulla prestazione telematica di servizi bancari da parte di operatori industriali cfr. R. LENER, *Il paradigma dei settori regolati e la democrazia dell'algoritmo. Note introduttive*, in *Rivista di Diritto Bancario*, pp. 193-207, a p. 196;, reperibile *online*; per quanto concerne, invece, la differenza tra le c.d.

rappresentati, per il mercato asiatico, dal gruppo *Ant* e per quanto concerne il mercato europeo dal recente accordo siglato tra *Amazon* e *Barclayscard Germany*[10].

Quanto al gruppo *Ant*, tale entità rappresenta l'evoluzione del progetto imprenditoriale assunto dal fondatore di *Alibaba*, Jack Ma. Più esattamente, quest'ultimo, sulla base dei dati di *e-commerce* raccolti fin dal 1999 grazie alla vendita online di prodotti tramite la piattaforma *Alibaba*, ha deciso di costituire nel 2014 una società finanziaria, la *Zhejiang Ant Small & Micro Financial Service Group*, allo scopo di offrire servizi di pagamento e di investimento a chiunque fosse titolare di un semplice *smartphone*. Negli ultimi anni, grazie al successo maturato in tale settore, la società in esame, quotata sia ad Hong Kong che a Shanghai, è passata da una capitalizzazione di 50 miliardi di dollari ad una valutazione che si aggira tra i 200 e i 300 miliardi di dollari, mutando la sua ragione sociale in *Ant Group*, togliendo quindi il suffisso «*financial*», al fine di sottolineare la mutazione del suo oggetto sociale: dalla fornitura di meri servizi finanziari alla predisposizione di una sorta di «*digital supermarket*» in cui i consumatori-investitori possono, tra le altre cose, usufruire di credito al consumo, acquistare prodotti assicurativi, ovvero investire in fondi comuni di investimento[11]. I servizi così offerti vengono erogati da intermediari finanziari partner del gruppo *Ant*, tuttavia è quest'ultimo che analizza i *big data*, effettua le decisioni di finanziamento e provvede alla costituzione dei contratti incorporanti i prodotti finanziari offerti; le banche e gli altri intermediari finanziari si limitano a fornire le risorse monetarie necessarie[12]. Il successo più grande del gruppo *Ant*, però, non si è registrato nel settore del microcredito, bensì nel settore della gestione collettiva del risparmio in cui, oltre a vantare *partnership* con società leader come *Invesco* e *Bank of China Investment Management*, il fondo comune monetario *Yu'e Bao* gestito all'interno del gruppo stesso è attualmente il fondo comune monetario più grande a livello globale per ammontare di attività finanziarie gestite[13].

In riferimento al contesto europeo, invece, la situazione del mercato finanziario è diametralmente opposta: nessuna società c.d. *Big-Tech* ha ancora assunto in proprio

società *TechFin* e le preesistenti istituzioni finanziarie, ovvero le più «tradizionali» *Fintech*, cfr. D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, J.N. BARBERIS, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, in *EBI Working Paper Series*, 2017 – no. 6, p. 5 ss., reperibile online.

[10] Per quanto riguarda, invece, l'inziale interesse delle società tecnologiche verso l'offerta di servizi di pagamento cfr. A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fin- Tech, il paradigma Open banking e la minaccia delle Big Tech companies*, in *Mercato Concorrenza Regole*, n. 3, 2018, pp. 441-466, spec. p. 456, laddove si riportano le iniziative europee intraprese inizialmente da *Facebook* che nel 2017 ha ottenuto in Irlanda l'autorizzazione a emettere moneta elettronica e a offrire servizi di pagamento, e in un secondo momento da *Amazon* e *Google* che rispettivamente nel 2018 in Lussemburgo e nel 2019 in Lituania hanno ottenuto delle licenze per l'emissione di monete elettroniche.

[11] Y.YANG, *Jack Ma Rails Against global financial rules ahead of $30 billion Ant Group IPO*, in *Financial Times*, 25 October 2020.

[12] R. MCMORROW, N. LIU, S. FEI JU, *The Transformation of Ant Financial*, *ivi*, 26 August 2020.

[13] Cfr. sul punto le analisi del FSB, *FinTech and market structure in financial services: Markets developments and potential financial stability implications*, 2019, p. 15, reperibile online, in cui vengono citati come altri casi emblematici le operazioni nel mercato finanziario intraprese dalle società *Tencent* e *Baidu*.

l'iniziata di creare una piattaforma digitale simile a quella ideata in Cina da Jack Ma e, in generale, l'andamento del mercato finanziario ha registrato una diminuzione di importanza rispetto allo scenario globale, passando da una quota di attività finanziarie gestite su scala globale del 20 percento durante l'anno 2006 a poco meno del 13 percento attuale[14]. Ciononostante, lo scorso novembre è stato annunciato un accordo tra *Amazon* e *Barclayscard Germany* che sembra, invece, rappresentare un cambio di passo importante. Le due società hanno, infatti, annunciato di aver concluso un contratto di *partnership* in base al quale gli utenti della nota piattaforma digitale potranno acquistare prodotti *online* usufruendo di contratti di credito al consumo ad un tasso annuo percentuale del 7.69%. Dopo aver scelto i beni da acquistare e la durata del finanziamento al consumo, i consumatori tedeschi, sulla base di un'analisi storica dei dati relativi alla quota di acquisti andati a buon fine sulla piattaforma *Amazon*, potranno ricevere *online* una risposta immediata da *Barclayscard Germany* circa la fattibilità economica del prestito[15]. Sebbene tale accordo possa rappresentare ben poca cosa rispetto all'esperienza cinese testé riportata, è indubbio che tale innovazione rappresenti un esempio paradigmatico di come anche nel vecchio Continente le società tecnologiche vogliano sfruttare il potenziale derivante dall'analisi computazionale dei *big data* tramite algoritmi per iniziare a offrire servizi finanziari[16].

Alla luce di quanto precede, appare palese come il futuro prossimo della finanza sia digitale[17]: il ruolo pioneristico svolto sul punto dal mercato cinese rappresenta un barometro sensibile di come l'innovazione tecnologica applicata al mondo finanziario possa comportare notevoli benefici all'economia reale. La crescita registrata dai mercati finanziari che si sono convertiti pressoché integralmente all'innovazione tecnologica suscita, tuttavia, dei quesiti che meritano di essere analizzati. In primo luogo, ci si domanda cosa si intende, in concreto, per ricorso all'innovazione tecnologica e, in particolare, agli algoritmi e al *deep learning* a scopo predittivo nelle attività di raccolta, gestione e allocazione di risorse monetarie. In secondo luogo, la domanda che è stata sollevata dagli studiosi di riferimento attiene ai possibili rischi che sono insiti nella

[14] J. FORD, *Future of the City: How London's reach will shrink after Brexit*, in *Financial Times*, 9 November 2020, in cui si rileva invece che il mercato asiatico attualmente gestisce, a livello globale, una quota di attività finanziarie pari al 40 percento, con un tasso di crescita del breve periodo in salita.

[15] Si veda sul punto il comunicato stampa diffuso sul sito della società tedesca *Barclayscard Germany*, «*Amazon partners with Barclaycard Germany to launch purchase financing through Amazon.de*», reperibile *online*.

[16] G. TETT, *Artificial Intelligence is reshaping finance*, in *Financial Times*, 19 November 2020.

[17] Cfr. Comunicazione della al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE, COM(2020) 591 final del 24 settembre 2020, laddove si legge nell'incipit che «il futuro della finanza è digitale: i consumatori e le imprese hanno sempre più accesso a servizi finanziari in modalità digitale, partecipanti al mercato innovativi mettono in campo nuove tecnologie e i modelli di business già esistenti stanno cambiando».

transizione digitale[18]. Più esattamente, ci si domanda se in un'ottica di analisi costi-benefici, sia possibile contemperare i grandi benefici connessi all'utilizzo dell'intelligenza artificiale nel mondo della finanza con il bisogno di garantire stabilità finanziaria e un utilizzo appropriato (cioè conforme ai noti canoni civilistici di correttezza e buona fede) degli strumenti di analisi e studio dei *big data*. In tale ottica, il secondo paragrafo del presente lavoro sarà dedicato alla definizione di intelligenza artificiale e a una breve rassegna delle possibili applicazioni di tale tecnologia nel mondo finanziario, mentre nel terzo paragrafo l'analisi sarà focalizzata sui rischi connessi alla transizione digitale.

2. Intelligenza artificiale e sistema finanziario.

In via di prima approssimazione, nell'analizzare il fenomeno dell'intelligenza artificiale applicata al settore finanziario, è utile fare una premessa: le reti neurali (c.d. «*neural networks*») alla base del funzionamento degli algoritmi incentrati sul *deep learning* non sono frutto di un'invenzione relativamente recente, in quanto le stesse sono state teorizzate per la prima volta durante gli anni Sessanta[19]. Senonché, l'assenza di computer dotati di una forza di calcolo importante e, soprattutto, la mancanza di dati in grado di sostenere con precisione analisi predittive hanno smorzato allora l'iniziale entusiasmo per tale scoperta, impedendo qualsiasi tipo di applicazione concreta. Negli ultimi anni, invece, il venir meno degli ostacoli in precedenza incontrati ha dato un nuovo slancio alle ricerche sull'intelligenza artificiale, fino al punto che i risultati di questi sforzi sono diventati un terreno fertile di applicazione empirica nel mercato di riferimento. In particolare, la disponibilità di un'enorme quantità di dati su vasta scala, la predisposizione di innovative architetture *cloud computing* per la conservazione delle informazioni e l'incremento delle possibilità di calcolo dei computer hanno costituito le principali cause scatenanti la ‹‹nuova corsa›› allo sfruttamento dell'intelligenza artificiale applicata alla finanza[20]. Ne consegue che, è improprio definire con l'appellativo ‹‹nuove›› delle

[18] Per degli studi sulle dinamiche connesse all'applicazione dell'intelligenza artificiale a problematiche di *corporate governance*, v. L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, in *European Corporate Governance Institute* (ECGI), *Law Working Paper* No. 457/2019, reperibile *online*; F. MOSLEIN, *Robots in the Boardroom: Artificial Intelligence and Corporate Law*, in W. BARFIELD, U. PAGALLO (edited by), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham, 2017, reperibile *online*; in generale, sui rischi alla stabilità finanziaria legati al ricorso agli algoritmi di tipo «deep learning», cfr. T. LIN, *Artificial Intelligence, Finance and the Law*, in *Fordham Law Review*, 2019, issue 2, pp. 531-551, spec. p. 541; W. KNIGHT, *The Financial World Wants to Open AI's Black Boxes*, in *MIT Technology Review*, 13 April 2017, reperibile *online*.

[19] Cfr. T. COVER, P. HART, *Nearest Neighbor Pattern Classification*, in *IEEE transactions on information theory*, 1967, n. 1, pp. 21-27.

[20] Il *World Economic Forum* ha stimato che dal 2011 al 2015 gli investimenti delle società private nel settore dell'intelligenza artificiale sono decuplicati, passando da un ammontare di 282 milioni di dollari a circa 2,4 miliardi di dollari: cfr. SLAUGHTER AND MAY, ASI Data Science, *Superhuman Resources: Responsible deployment of AI in business*, Joint White Paper, 2017, p. 7, reperibile *online*.

tecnologie che in realtà sono state inventate più di cinquant'anni fa; la novità si rinviene, piuttosto, nell'avvento dei c.d. *big data* e nella conseguente possibilità di poterli sfruttare mediante algoritmi di calcolo per finalità di natura prevalentemente predittiva e di massimizzazione dei risultati.

Ciò detto, il termine intelligenza artificiale racchiude al suo interno tecniche computazionali di calcolo e valutazione di complessi problemi del mondo reale che sfruttano algoritmi in grado di imitare le capacità percettive del sistema nervoso e del cervello umano: ferme restando le abissali differenze sussistenti tra il lavoro di una macchina e le capacità di ragionamento umane, la scienza computeristica ritiene in particolare possibile sfruttare alcune analogie di fondo per replicare le modalità di funzionamento del nostro cervello attraverso sistemi di calcolo artificiali[21]. Le reti neurali di natura artificiale possono, infatti, essere definite come sistemi di elaborazione di informazioni che utilizzano logiche di apprendimento e generalizzazione altamente adattabili alla realtà circostante. In virtù delle caratteristiche surriferite, tali algoritmi sono particolarmente indicati per tecniche di elaborazione soggettiva dell'informazione e processi decisionali e previsionali aventi ad oggetto sviluppi futuri di determinate variabili[22].

La dottrina di riferimento ha indicato come l'applicazione di algoritmi basati sulle reti neurali artificiali possano essere utilizzati nel settore finanziario per migliorare da un punto di vista sia quantitativo che qualitativo i risultati di analisi dati raggiunti in passato dai tradizionali metodi statistici. In particolare, è stato indicato che settori di analisi incentrati tipicamente sulle simulazioni finanziarie, sulla previsione dei comportamenti degli investitori, sulla valutazione del merito creditorio dei progetti imprenditoriali, ovvero nel settore della gestione individuale e/o collettiva del risparmio possano beneficiare grandemente delle potenzialità di calcolo derivanti dall'intelligenza artificiale[23].

Nello specifico, quanto alla valutazione creditizia, algoritmi incentrati su sistemi neurali di natura artificiale possono sfruttare i dati finanziari degli utenti di servizi bancari raccolti negli anni dagli intermediari finanziari (il c.d. *input*) al fine di raggiungere conclusioni di natura binaria (SI-NO) sulla fattibilità economica della concessione di un

---

[21] Cfr. I.A. BASHEER, M. HAJMEER, *Artificial neural networks: fundamentals, computing, design, and application*, in *Journal of Microbiological Methods*, 2000, issue 1, pp. 3-31.

[22] Si veda sul punto, tra gli altri, M. LAM, *Neural network techniques for financial performance prediction: integrating fundamental and technical analysis*, in *Decision Support Systems*, 2004, issue 4, pp. 567-581; C. TOUZET, *Neural reinforcement learning for behaviour synthesis*, in *Robotics and Autonomous Systems*, 1997, issue 3-4, pp. 251-281.

[23] A. BAHRAMMIRZAEE, *A comparative survey of artificial intelligence applications in finance: artificial neural networks, expert system and hybrid intelligent systems*, in *Neural Computing & Applications*, 2010, pp. 1165-1195, spec. p. 1166 ss.; si veda anche per quanto riguarda il ricorso all'intelligenza artificiale nel campo della gestione delle attività finanziarie il lavoro di C. HSIEH, *Some Potential Applications of Artificial Neural Systems in Financial Management*, in *Journal of Systems Management*, 1993, issue 4, pp. 12-15, reperibile *online*.

determinato finanziamento (il c.d. *output*). L'obiettivo di tali sistemi è, invero, quello di imitare il lavoro degli uffici bancari addetti alla concessione di credito, migliorando, però, la precisione nello stabilire (i) l'*an* dell'eventuale linea di credito da concedere, e, soprattutto, (ii) il *quantum*, ossia l'ammontare massimo del credito concedibile a fronte dei rischi di *default* che la banca potrebbe subire in caso di inadempimento del mutuatario[24]. Le applicazioni concrete hanno dimostrato che la capacità degli algoritmi in esame di superare il grado di precisione degli uffici prestiti interni agli istituti di credito nel prevedere e stimare le tendenze di *default* dei possibili *non-performing loans* (c.d. NPL) dipende, ovviamente, dalla disponibilità di dati precisi sulla storia finanziaria dei clienti bancari e sullo stato delle finanze personali al momento dell'inoltro della domanda di finanziamento, nonché dalla predisposizione di applicativi in grado di effettuare appropriate analisi e studio dei dati disponibili[25]. Una volta soddisfatte tali condizioni, si è infatti rilevato che la velocità di calcolo e la precisione nei risultati prodotti dagli applicativi basati sull'intelligenza artificiale superano il livello di affidabilità raggiungibile dall'esperienza umana, ovvero dai tradizionali modelli bancari di analisi creditizia[26].

In riferimento alla gestione patrimoniale, si afferma che tale settore del mercato finanziario è particolarmente consono all'applicazione dell'intelligenza artificiale, atteso che gli algoritmi basati sulle reti neurali artificiali producono risultati efficienti in presenza di un ambiente caratterizzato (i) da incertezza sugli sviluppi dei corsi dei titoli[27]; (ii) dalla diversità delle informazioni disponibili. In altri termini, in un settore in cui è fondamentale diversificare il risparmio raccolto in una varietà di attività finanziarie (azioni, obbligazioni, strumenti finanziari ibridi, prodotti del mercato monetario) che coincidano con le esigenze di investimento degli intermediari finanziari e con il profilo di rischio richiesto dai risparmiatori-investitori, le tecnologie in esame, sfruttando la capacità computazionale degli algoritmi nell'analisi dei dati disponibili sul mercato,

[24] D. HALWEY, J. JOHNSON, D. RAINA, *Artificial Neural Systems: A New Tool for Financial Decision-Making*, in *Financial Analysts Journal*, 1990, n. 6, pp. 63-72, spec. p. 66.

[25] A. BAHRAMMIRZAEE, *A comparative survey*, cit., p. 1167.

[26] Si veda sul punto il lavoro di M. STARK, *Authorizer's Assistant: a knowledge-based system for credit authorization*, Wescon/96, 1996, pp. 473-477, reperibile *online*, il quale ha rilevato che il tasso di errore circa il *default* dei possessori di carte di credito *American express* ottenuto tramite l'utilizzazione di metodi di analisi convenzionali era stato del 15%, mentre tale soglia si era ridotta drasticamente al 4 percento in caso di utilizzo di metodi basati sull'intelligenza artificiale; in senso conforme v. anche K. BRYANT, *ALEES: an agricultural loan evaluation expert system*, in *Expert Systems with Applications*, 2001, issue 2, pp. 75-85; A. BAHRAMMIRZAEE, A.R. GHATARI, P. AHMADI, K. MADANI, *Hybrid credit ranking intelligent system using expert system and artificial neural networks*, in *Applied Intelligence*, 2011, pp. 28-46, in cui si è rilevato che la commistione tra algoritmi basati sulle reti neurali artificiali e quelli incentrati su *expert system* riduce le imperfezioni dei singoli modelli, aumentando al contempo la capacità predittiva generale.

[27] Ovvero, in presenza di un andamento del mercato in cui i prezzi dei prodotti finanziari sono caratterizzati da elevata volatilità, potendo il relativo valore cambiare direzione in maniera del tutto imprevedibile e sulla base di fattori sia esogeni al mercato di riferimento, sia endogeni all'attività finanziaria oggetto di un repentino mutamento del proprio valore nominale.

possono condurre all'assunzione di scelte di investimento appropriate e conformi al noto brocardo in voga soprattutto nel mercato dei capitali «non mettere tutte le tue uova in un solo cestino»[28]. Svariati studi specialistici hanno, invero, dimostrato che i metodi di analisi basati sull'intelligenza artificiale sono risultati più incisivi rispetto ai modelli statistici o alle strategie di *trading* convenzionali nell'incrementare il valore dei patrimoni gestiti[29]: le società finanziarie che hanno utilizzato algoritmi di tipo neurale sono riuscite ad allocare efficacemente le proprie risorse monetarie verso progetti imprenditoriali rivelatesi vincenti sotto il profilo di un congruo ritorno economico[30].

Per quanto concerne, invece, la previsione e pianificazione finanziaria, è stato affermato che le caratteristiche insite del mercato finanziario, incentrato come noto su un complesso sistema non-lineare di interconnessioni tra operatori economici non sempre facilmente controllabili dalle possibilità di osservazione umane, ben si confanno all'utilizzo dell'intelligenza artificiale. I sistemi di calcolo basati su quest'ultima tecnologia possono, infatti, essere ideati in guisa da consentire la previsione di variabili del mercato finanziario come la liquidità bancaria, il tasso di inflazione e/o la probabilità di insolvenza di determinate controparti contrattuali[31]. Anche in questo caso sono stati avanzati degli studi che hanno, per esempio, dimostrato come reti neurali artificiali possano prevedere con ragionevole certezza e in un lasso di tempo relativamente breve il rischio di insolvenza degli utilizzatori delle carte di credito, sfruttando a tal proposito come *input* principalmente i dati storici delle transazioni economiche effettuate in passato[32].

In tale quadro, se ci basassimo soltanto sugli effetti positivi che derivano dal ricorso all'intelligenza artificiale nel mercato finanziario, la soluzione più ovvia sarebbe quella

---

[28] L. MOTIWALLA, M. WAHAB, *Predictable variation and profitable trading of US equities: a trading simulation using neural networks*, in *Computers & Operations Research*, 2000, issue 11-12, pp. 1111-1129.

[29] Cfr. sul punto il lavoro di D. KAHNEMAN, *Thinking Fast and Slow*, London, 2012, p. 214, in cui si afferma che l'esperienza empirica ha dimostrato come per la maggior parte dei gestori di patrimoni la selezione dei titoli azionari è similare al lancio dei dati: invero, negli ultimi cinquant'anni almeno due terzi dei fondi comuni di investimento c.d. attivi hanno avuto un rendimento inferiore rispetto agli andamenti registrati dal mercato azionario nel suo complesso.

[30] Sul punto, si vedano tra gli altri gli studi di P. KO, P. LIN, *Resource allocation neural network in portfolio selection*, in *Expert Systems with Applications*, 2008, issue 1-2, pp. 330-337; H.J. ZIMMERMANN, R. NEUNEIER, R. GROTHMANN, *Active Portfolio-Management based on Error Correction Neural Networks*, 2001, reperibile *online*; A. BADIRU, D. SIEGER, *Neural network as a simulation metamodel in economic analysis of risky projects*, in *European Journal of Operational Research*, 1998, issue 1, pp. 130-142.

[31] A. BAHRAMMIRZAEE, *A comparative survey*, cit., p. 1169.

[32] Si veda sul punto, tra gli altri, il modello ideato da I. JAGIELSKA, J. JAWORSKI, *Neural network for predicting the performance of credit card accounts*, in *Computational Economics*, 1996, p. 77-82; altri esempi in tal senso spaziano dall'utilizzo dell'intelligenza artificiale per ideare strategie di marketing adeguate alle necessità di banche commerciali, come il modello studiato da B. CURRY, L. MOUTINHO, *Using Advanced Computing Techniques in Banking*, in *International Journal of Bank Marketing*, 1993, n. 6, p. 39-46; ovvero, il modello teorizzato da F. PETROPOULOS, K. NIKOLOPOULOS, V. ASSIMAKOPOULOS, *An expert system for forecasting mutual funds in Greece*, in *International Journal of Electronic Finance*, 2008, issue 4, pp. 404-418 per prevedere l'andamento del mercato dei fondi comuni di investimento di tipo aperto in Grecia.

di auspicare *sic et simpliciter* una sostituzione dei vecchi modelli statistici in favore di un utilizzo generalizzato degli algoritmi intelligenti sopra richiamati. Questo mutamento, però, non è avvenuto, e gli scenari per il breve periodo non indicano, almeno per quanto concerne il mondo occidentale, una effettiva transizione digitale del mercato finanziario. Le ragioni di questo «conservatorismo» sembrano rinvenirsi sia in ostacoli di natura tecnica, sia in valutazioni connesse al corretto funzionamento del sistema economico.

Quanto all'aspetto prettamente tecnico, la dottrina di riferimento osserva che l'intelligenza artificiale, fondando le proprie valutazioni sullo sfruttamento di dati finanziari di natura storica, potrebbe non rappresentare un adeguato punto di riferimento in presenza di mercati in costante mutamento. Considerato che il settore finanziario degli ultimi decenni rappresenta un tipico esempio di mercato le cui caratteristiche di fondo sono in continua trasformazione, tale situazione potrebbe in alcuni casi minare l'effetto utile connesso all'applicazione dell'intelligenza artificiale nel mercato in esame[33].

In riferimento, invece, a valutazioni di più ampio respiro connesse al buon funzionamento del sistema economico in generale, la letteratura economica e giuridica ha sottolineato, a vario titolo, i rischi connessi all'innovazione tecnologica, sia a livello di singola entità economica, sia da un punto di vista macroeconomico[34]. Nel prossimo paragrafo ci cercherà, quindi, di fare una rassegna delle principali criticità che sono state sollevate nei confronti di un uso sistemico dell'intelligenza artificiale.

3. Rischi connessi all'innovazione tecnologica.

Come testé anticipato, le metodologie di calcolo e analisi basate sull'intelligenza artificiale non sono una panacea per tutti i mali dell'economia. Le potenzialità di sviluppo degli algoritmi intelligenti devono, infatti, fare i conti con le conseguenze per il tessuto economico derivanti da un uso eccessivo degli stessi. In particolare, da un lato, è stato sostenuto che l'adozione di modelli di calcolo basati sulla *deep learning* può rendere il sistema finanziario meno resiliente a scenari di mercato avversi[35]; dall'altro, è stato sottolineato come le caratteristiche proprie dell'intelligenza artificiale possano provocare i seguenti rischi: (i) standardizzazione dei comportamenti («herding behavior»); (ii) discriminazioni avverso determinati soggetti deboli; (iii) mancanza di adeguata

[33] Per una visione critica dei modelli predittivi incentrati sullo studio dell'insolvenza degli operatori economici v. M. NWOGUGU, *Decision-making, risk and corporate governance: A critique of methodological issues in bankruptcy/recovery prediction models*, in *Applied Mathematics and Computation*, 2007, issue 1, pp. 178-196.

[34] Sul rapporto tra rischi e regolamentazione cfr. T. KURAN, C. SUNSTEIN, *Availability Cascades and Risk Regulation*, in *Stanford Law Review*, 1999, pp. 683-768, reperibile *online*.

[35] Sul punto cfr. H. GENBERG, *Digital Transformation*, cit., p. 6.

trasparenza nel funzionamento degli algoritmi; (iv) superamento del quadro normativo attuale[36].

3.1. Standardizzazione dei comportamenti.

Quanto al rischio di standardizzazione dei comportamenti, parte della dottrina ha affermato che l'utilizzazione generalizzata di algoritmi che favoriscono l'assunzione di *best practices* e/o modelli predittivi che si assomigliano tra loro possono dare luogo ad una sorta di «monocultura» tra gli intermediari finanziari: in altri termini, piuttosto che assumere scelte di investimento originali, gli operatori del mercato finanziario potrebbero seguire alla lettera i dettami consigliati dall'intelligenza artificiale, eliminando così quella diversità di agire utile a mantenere appropriati livelli di stabilità finanziaria[37]. Ed invero, quest'ultima potrebbe essere danneggiata dall'assunzione di comportamenti uniformi che aumenterebbero la pro-ciclicità del settore di riferimento, soprattutto in periodi di espansione, riducendo al contempo i naturali controlimiti rappresentati da comportamenti di segno contrario[38].

Un caso di scuola utile a comprendere tale ragionamento può essere rappresentato dalla previsione circa il corso di un titolo obbligazionario che un algoritmo intelligente è solito calcolare sulla base dell'andamento storico del valore nominale del titolo stesso. Se un fattore esogeno, di natura imprevedibile in quanto mai verificatosi in passato, altera il valore del titolo obbligazionario in maniera diametralmente opposta rispetto alle previsioni effettuate dall'algoritmo in precedenza, gli intermediari finanziari che si sono erroneamente fidati di quest'ultimo, investendo parte delle loro risorse finanziarie nel titolo obbligazionario oggetto di una svalutazione repentina, potrebbero incorrere in gravi perdite. Qualora questo algoritmo fosse stato adottato come punto di riferimento per le strategie di investimento da un numero elevato di intermediari finanziari, allora le perdite conseguenti potrebbero tramutarsi in una crisi sistemica difficilmente gestibile con strumenti di natura ordinaria.

Allo stesso tempo, uno scenario analogo si potrebbe verificare in presenza di incentivi economici a costituire dei *mega-database* di archiviazione dei *big data*. Le economie di scala connesse alla conservazione dei dati sulle transazioni concluse ogni giorno dai consumatori spingono, infatti, i fornitori di servizi di *cloud computing* ad aggregare tali dati in singoli collettori. In tale contesto, se gli algoritmi utilizzati a fini predittivi dagli intermediari finanziari vedono limitata la scelta di *database* da cui

[36] Per una recente analisi dei rischi connessi all'intelligenza artificiale, v. G. GENSLER, L. BAILEY, *Deep Learning and Financial Stability*, Working Paper 2020, reperibile *online*.

[37] J. DANIELSSON, R. MACRAE, A. UTHEMANN, *Artificial Intelligence, financial risk management and systemic risk*, Systemic Risk Center, SRC Special Paper no. 13, November 2017, p. 3 reperibile *online*.

[38] Sul rischio di uniformità tra gli intermediari finanziari v. anche M. CARNEY, *The Promise of FinTech*, cit., p. 8.

attingere i dati necessari ai calcoli computazionali, il naturale corollario di una tale situazione sarà rappresentato da un'ulteriore uniformità dei risultati raggiungibili mediante l'utilizzazione di meccanismi di *deep learning*[39].

Alla luce di quanto precede, appare quindi palese come una diffusione su larga scala di algoritmi che tendono a ‹‹consigliare›› strategie di investimento similari possa tradursi in un rischio alla stabilità finanziaria in presenza di scenari di mercato imprevedibili, ossia frutto di evoluzioni del mercato di riferimento non calcolabili nemmeno attraverso le potenzialità proprie dell'intelligenza artificiale.

3.2. *Bias* e discriminazione.

In riferimento, invece, al rischio di discriminazione, si è affermato che l'utilizzazione di strumenti basati sull'intelligenza artificiale possa andare a cozzare con i canoni dell'inclusione finanziaria, della coesione sociale, della fiducia nel sistema finanziario e, infine, della dignità umana[40]. Come noto, in effetti, i principi di correttezza e buona fede posti alla base delle tradizioni costituzionali comuni dei paesi civilizzati impongono agli intermediari finanziari di garantire pari diritto di accesso ai servizi finanziari, senza discriminazioni derivanti dall'origine etnica, dalla religione, dal sesso, dal colore della pelle e dall'età. Senonché, la logica di funzionamento degli algoritmi, incentrata, come più volte affermato, principalmente su dati obiettivi come la storia finanziaria e lo *status* economico dei soggetti che richiedono un finanziamento, può involontariamente prescindere da considerazioni di correttezza ed equità dei rapporti sociali, escludendo *ex ante* qualsiasi possibilità di finanziamento di determinate categorie considerate storicamente meno affidabili da un punto di vista finanziario[41].

A ben vedere, tali problematiche non rivestono carattere di novità, atteso che già la direttiva europea 2008/48/CE imponeva agli Stati membri di prevedere nel proprio ordinamento il diritto del consumatore di ottenere informazioni sul rifiuto opposto da un intermediario creditizio ad una domanda di credito, indicando gli estremi della banca dati eventualmente consultata da quest'ultimo per la verifica del merito creditizio[42]. Questa disposizione è stata trasposta pressoché letteralmente dal nostro legislatore nel Testo Unico Bancario, il quale all'art. 125, c. 2, nel disciplinare la fattispecie del credito ai consumatori, afferma testualmente che «se il rifiuto della domanda di credito si basa sulle

[39] Cfr. in tal senso L. WALL, *Some financial regulatory implications of artificial intelligence*, in *Journal of Economics and Business*, 2018, pp. 55-63.

[40] Cfr. sul punto C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, 2016, p. 84 ss.

[41] G. GENSLER, L. BAILEY, *Deep Learning*, cit., p. 14; si veda anche K.N. JOHNSON, F.A. PASQUALE, J.E. CHAPMAN, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, in *Fordham Law Review*, 2019, n. 4, pp. 499-529.

[42] Cfr. direttiva 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE; in particolare considerando 29.

informazioni presenti in una banca dati, il finanziatore informa il consumatore immediatamente e gratuitamente del risultato della consultazione e degli estremi della banca dati»[43]. Legislazioni aventi la stessa finalità di tutela del contraente debole sono state, ovviamente, introdotte anche in altri ordinamenti giuridici extra-comunitari[44].

Tuttavia, i meccanismi di salvaguardia introdotti dal legislatore a favore degli utenti di servizi finanziari considerano soltanto la possibilità che le società finanziarie calcolino il merito creditizio dei primi sulla base della consultazione delle banche dati pubbliche o private che registrano le situazioni di inadempimento pregresse dei soggetti insolventi. Tali presidi di tutela non tengono, quindi, conto dei criteri operativi di concessione dei finanziamenti utilizzati attualmente dagli algoritmi basati sul *deep learning*. Ed invero, è stato rilevato che questi ultimi, pur essendo in grado di raggiungere risultati ottimali circa la corretta allocazione delle risorse finanziarie, fondano i propri calcoli anche sullo studio di dati non convenzionali, come le origini demografiche o il numero di interazioni sui *social network* dei richiedenti un prestito, che in precedenza non venivano (giustamente?) presi in considerazione[45].

In tale contesto, la sfida regolatoria che attende il legislatore ha, quindi, ad oggetto il raggiungimento di un adeguato bilanciamento tra l'esigenza di ottenere risultati predittivi efficienti e la necessità di non legittimare oltremodo prassi di concessione del credito scorrette, in quanto reiteratamente discriminatorie rispetto a determinate categorie di individui. In particolare, si dovrebbero, innanzitutto, individuare degli strumenti in grado di analizzare senza soluzione di continuità il funzionamento degli algoritmi, intervenendo tempestivamente qualora emergano delle tendenze di giudizio discriminatorie, e ciò a prescindere in concreto dalle modalità di correzione esterna delle anomalie (se prima, durante e/o dopo che i meccanismi di calcolo intelligente abbiano elaborato una determinata risposta)[46]. In secondo luogo, lo sforzo del legislatore dovrebbe essere diretto a evitare che gli eventuali meccanismi di salvaguardia della sfera giuridica dei singoli così individuati alterino la bontà delle stime degli algoritmi fino al punto da

[43] Cfr. d.lgs. 1° settembre 1993, n. 385 (c.d. T.U. delle leggi in materia bancaria e creditizia), art. 121 ss.

[44] Cfr. sul punto G. GENSLER, L. BAILEY, *Deep Learning*, cit., p. 14, i quali hanno citato sul punto la legislazione statunitense che è stata adottata in seguito all'introduzione di innovazioni metodologiche nel calcolo del merito creditizio dei titolari di carte di credito e, in particolare, il *Fair Housing Act*, il *Fair Credit Reporting Act* e l'*Equal Credit Opportunity Act*.

[45] Cfr. P. CROSMAN, *Can AI Be Programmed to Make Fair Lending Decisions*?, in *American Banker*, 27 September 2016, reperibile *online*, il quale a tal proposito cita come esempio di fattori considerati attualmente dagli algoritmi per la concessione di finanziamenti il corretto uso della punteggiatura o dello *spelling* delle parole utilizzate dagli aspiranti mutuatari durante la compilazione di una domanda di credito.

[46] Per un caso recente di controllo *ex post* del meccanismo di funzionamento di un algoritmo utilizzato per lo studio di domande di concessione di visti inglesi, v. H. WARRELL, *Home Office drops 'biased' visa algorithm*, in *Financial Times*, 4 August 2020.

rendere le stesse inaffidabili, precludendo *sine die* le possibilità di crescita economica insite nello sfruttamento delle nuove tecnologie[47].

3.3. Trasparenza.

Profondamente connesso alla tematica discriminatoria è il rischio che il funzionamento degli algoritmi sia insensibile alle istanze di trasparenza richieste per un'allocazione delle risorse economiche conforme ai canoni di correttezza e buona fede. Sebbene, infatti, i fornitori di servizi finanziari *online* si definiscano come degli agenti economici dotati di tutti i crismi della trasparenza, in realtà gli stessi tendono ad assumere un atteggiamento reticente qualora vengano sollevati interrogativi attinenti alla tecnologia e/o agli algoritmi utilizzati durante la fase di valutazione del merito creditizio degli aspiranti mutuatari[48].

A ben riflettere, da un lato, la pubblicazione dei dettagli di funzionamento di un algoritmo, ovvero dell'elenco esaustivo dei fattori presi in considerazione per il calcolo computazionale, andrebbe in concreto a ledere il diritto di proprietà intellettuale degli sviluppatori dei *software*: la diffusione sul mercato delle specifiche tecniche di algoritmi rivelatesi vincenti potrebbe, infatti, spingere i *competitor* della società finanziaria titolare della tecnologia oggetto dell'obbligo di *disclosure* a copiare il relativo meccanismo di funzionamento al fine di beneficiare anch'essi delle possibilità di guadagno offerte dall'intelligenza artificiale[49].

Dall'altro, la mancanza di adeguati livelli di trasparenza degli algoritmi incentrati sulla *deep learning* deriva dall'oggettiva incertezza su come tali sistemi computazionali raggiungano determinati risultati: le macchine dotate di intelligenza artificiale, infatti, possono auto-apprendere determinati collegamenti tra le variabili in gioco senza aver ottenuto sul punto istruzioni esterne, non sono strettamente limitate all'osservazione di regole logiche nel compiere calcoli computazionali e, soprattutto, possono seguire delle proprie regole e supposizioni nel produrre un risultato predittivo[50].

In conformità a tali osservazioni, la dottrina di riferimento afferma che l'inscrutabilità dei modelli basati sull'intelligenza artificiale da parte dei soggetti interessati che vorrebbero, a vario titolo, ottenere delle delucidazioni sul funzionamento

---

[47] Cfr. M. CARNEY, *The Promise of FinTech*, cit., p. 6 il quale sottolinea come l'utilizzazione di algoritmi basati sull'intelligenza artificiale nel mercato cinese abbia incrementato notevolmente la quota di finanziamenti disponibili sul mercato senza, al contempo, aumentare proporzionalmente il rischio di default: sebbene le ipotesi di micro credito concesse dalle piattaforme digitali cinesi non richiedano la prestazione di garanzie reali o personali, il tasso di insolvenza risulta infatti essere minore del 2%; sul punto v. anche G. GENSLER, L. BAILEY, *Deep Learning*, cit, p. 15.

[48] M. REYNOLDS, *Bias test to prevent algorithms discriminating unfairly*, in *NewScientist*, 2017, reperibile *online*.

[49] P. CROSMAN, *Can AI Be Programmed*, cit.

[50] *Ibidem*.

in concreto degli algoritmi pone dei rischi per la tenuta del sistema nel suo complesso. Ed invero, a titolo esemplificativo, in assenza di una motivazione precisa circa il rifiuto opposto ad una domanda di credito, i consumatori vedrebbero limitata la possibilità di far valere in giudizio l'eventuale lesione alla propria sfera giuridica. Allo stesso tempo, la mancanza di trasparenza sulla logica seguita da un algoritmo nel consigliare una determinata strategia di investimento potrebbe disincentivare gli amministratori di una società finanziaria dal seguirla per paura di essere, in un secondo momento, ritenuti responsabili dell'arrecamento di un grave danno al patrimonio sociale *ex*. art. 2392 ss. c.c., qualora la strategia di fatto seguita abbia prodotto un risultato negativo. Anche in tale contesto si auspica, quindi, il raggiungimento di un contemperamento degli interessi in gioco che consenta di non sacrificare sull'altare dell'efficienza esigenze di conoscibilità/trasparenza delle pratiche di finanziamento o investimento adottate dagli intermediari creditizi che utilizzano algoritmi intelligenti[51].

3.4. Lacune normative.

La breve analisi condotta in precedenza sui rischi legati all'intelligenza artificiale nel mercato finanziario ha confermato un problema di fondo: l'assenza di un quadro normativo *ad hoc* in grado di gestire le sfide sollevate dagli sviluppi della *deep learning*. Più esattamente, si è rilevato che tale *vulnus* dell'ordinamento giuridico, oltre a costituire il *fil rouge* delle problematiche sopra indicate, rappresenta una ulteriore fonte di rischio sistemico per l'economia nel suo complesso[52].

L'esperienza empirica ci ha mostrato, infatti, come risultati disastrosi si verifichino ogniqualvolta innovazioni tecnologiche sfuggono dall'applicazione di normative previamente introdotte al fine di contenere le disfunzioni del libero mercato. La crisi finanziaria del 2007-08 rappresenta a tal riguardo un caso emblematico: l'assenza di presidi normativi a fronte di fenomeni perversi come lo sviluppo esponenziale delle cartolarizzazioni, l'utilizzazione di innovativi contratti derivati a copertura del rischio di credito di controparte (c.d. *credit default swaps*), e la predisposizione di nuove tecniche di offuscamento dei rischi connessi ai mutui *sub-prime* hanno gettato le basi del crollo dei mercati poi verificatosi[53].

---

[51] G. GENSLER, L. BAILEY, *Deep Learning*, cit, p. 13.

[52] In senso conforme, L. MCPHIL, J. MCPHIL, *Machine Learning Implications for Banking Regulations*, 2019, reperibile *online*.

[53] Cfr. in tal senso G. GENSLER, L. BAILEY, *Deep Learning*, cit, p. 24, i quali citano al riguardo innanzitutto la situazione presente negli Stati Uniti, laddove le linee guida per lo sviluppo di modelli integrati di gestione interna del rischio attualmente in vigore sono state pubblicate soltanto nel 2011. Peraltro, una situazione similare è presente anche in quegli ordinamenti (Unione europea e Canada) in cui, nonostante la recente data di pubblicazione delle istruzioni di vigilanza sulla gestione dei rischi interni (2017), la vigilanza prudenziale è principalmente basata sull'utilizzazione di modelli statistici di calcolo di tipo lineare.

Nel caso che ci occupa, campanelli di allarme sono stati individuati, da un lato, nell'assenza di disposizioni adeguate avverso il rischio macro-sistemico delle società finanziarie, e dall'altro, nella mancanza di disposizioni prudenziali nei confronti delle società tecnologiche che collaborano a vario titolo nella produzione di servizi finanziari. Quanto al primo aspetto, si afferma che le metodologie interne di gestione dei rischi finanziari dovrebbero essere aggiornate al fine di considerare i rischi macroprudenziali che potrebbero derivare dall'adozione sistematica di algoritmi intelligenti. In particolare, la logica di funzionamento sottesa a tali tecnologie, potendo aumentare esponenzialmente la standardizzazione dei comportamenti nel mercato, dovrebbe spingere il legislatore a considerare con più attenzione la rilevanza del rischio di interconnessioni tra operatori finanziari[54]. In riferimento al secondo aspetto, si sottolinea che, come noto, le società tecnologiche svolgenti servizi ‹‹ancillari›› al funzionamento degli algoritmi *deep learning* non sono attualmente sottoposte alla legislazione sui mercati finanziari. In tale quadro, al fine di garantire un controllo completo del mercato finanziario, gli operatori *tech* che, ad esempio, offrono delle piattaforme digitali a beneficio degli intermediari creditizi potrebbero essere parzialmente sottoposti al rispetto di obblighi di trasparenza dell'attività svolta e/o di segnalazione delle operazioni rilevanti a favore delle autorità competenti[55].

Sotto altro versante, è stato affermato che le significative opportunità di efficienza e inclusione finanziaria connesse all'applicazione di algoritmi intelligenti nell'attività di allocazione delle risorse monetarie vengono precluse dall'incertezza sul quadro normativo eventualmente applicabile. A ben riflettere, la presenza di lacune normative in tale settore non crea soltanto un rischio alla stabilità finanziaria, bensì impedisce anche le possibilità di sviluppo economico che, in assenza di barriere normative, potrebbero altrimenti manifestarsi. Un'applicazione coerente di regole pertinenti consentirebbe, invece, di gettare le basi per quella certezza del diritto necessaria all'innovazione tecnologica rappresentata dal *fintech*[56].

In tale contesto, appare quindi ragionevole includere la tematica regolatoria come uno dei rischi legati all'avvento dell'intelligenza artificiale nel mercato finanziario. Invero, come affermato in tale paragrafo, l'assenza di un quadro normativo confacente alle caratteristiche proprie degli algoritmi intelligenti provoca, da un lato, l'emergere di rischi alla stabilità finanziaria e, dall'altro, impedisce il dispiegarsi di iniziative in grado di aumentare il grado di efficienza del sistema economico[57].

---

[54] *Ivi*, p. 28.

[55] *Ivi*, p. 30.

[56] Sull'incertezza regolatoria in merito alle tecnologie *fintech*, si vedano W. RINGE, C. ROUF, *Regulating Fintech in the EU: the Case for a Guided Sandbox*, in *European Journal of Risk Regulation*, 2020, pp. 604-629, spec. p. 612.

[57] Sull'incremento della produttività del sistema economico dovuto all'intelligenza artificiale si v. E. BRYNJOLFSSON, A. MCAFEE, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York, 2014, p. 92.

4. La risposta della Commissione europea: il principio «stessa attività, stesso rischio, stesse norme».

Una prima risposta alle problematiche sollevate dal fenomeno dell'intelligenza artificiale applicata al mercato dei capitali è stata fornita dalla Commissione europea lo scorso settembre 2020, in occasione della Comunicazione sulla strategia in materia di finanza digitale per l'UE[58]. Sulla scorta delle conclusioni raggiunte nel piano d'azione per le tecnologie digitali del 2018[59] e in altri documenti istituzionali come la relazione del Parlamento europeo sulla finanza digitale[60] e le raccomandazioni dell'*high-level forum* sull'Unione del mercato dei capitali[61], l'esecutivo europeo ha stabilito un obiettivo strategico generale per la transizione digitale finanziaria allo scopo di sfruttare tutte le opportunità offerte dalla finanza digitale, e quattro politiche di intervento per affrontare questioni particolari connesse con tale transizione.

Per quanto interessa la presente sede, la Commissione europea riconosce anzitutto che la fornitura di servizi finanziari da parte di imprese tecnologiche (a prescindere dalla dimensione, sia piccole che grandi) potrebbe produrre come effetti immediati: (i) il cambiamento del rapporto tra rischi micro e macroprudenziali; (ii) l'aumento della pressione competitiva; (iii) il miglioramento, in generale, della qualità dei servizi finanziari per i consumatori e le imprese[62].

In secondo luogo, l'esecutivo europeo afferma che non è sufficiente decantare le opportunità offerte dalla transizione digitale, bensì è necessario affrontare le nuove sfide e, soprattutto, i rischi legati al cambiamento in atto nel mercato finanziario. La fornitura di servizi finanziari da parte di nuovi partecipanti al mercato solleva, in particolare, il rischio che la normativa e la vigilanza finanziarie diventino anacronistiche in quanto non più in grado di assicurare, tre le altre finalità ad esse attribuite, la stabilità finanziaria, la protezione del consumatore, l'integrità e il corretto funzionamento del sistema economico. In tale ottica, la Commissione europea ritiene, quindi, opportuno prestare attenzione al principio ‹‹stessa attività, stesso rischio, stesse norme››, allo scopo di ‹‹salvaguardare la parità di condizioni tra gli istituti finanziari esistenti e i nuovi partecipanti al mercato››[63].

---

[58] COM(2020) 591 final, cit.

[59] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Piano d'azione per le tecnologie digitali: per un settore finanziario europeo più competitivo e innovativo, COM(2018) 109 final dell'8 marzo 2018.

[60] Proposta di risoluzione del Parlamento europeo recante raccomandazioni alla Commissione sulla finanza digitale: rischi emergenti legati alle cripto-attività - sfide a livello della regolamentazione e della vigilanza nel settore dei servizi, degli istituti e dei mercati finanziari (2020/2034(INL)).

[61] HIGH LEVEL FORUM ON THE CAPITAL MARKETS UNION, *Final Report: A New Vision for Europe's Capital Markets*, 2020, reperibile *online*.

[62] COM(2020) 591 final, cit., p. 3.

[63] *Ivi*, p. 5; in armonia, del resto, con il fondamentale principio di proporzionalità contenuto nell'art. 5, par. 4, del Trattato sull'Unione Europea, in base al quale «il contenuto e la forma dell'azione dell'Unione

In effetti, il problema principale che è stato riscontrato nel contesto europeo attiene, in buona sostanza, alla possibilità e/o convenienza dell'applicazione della legislazione sui mercati finanziari attualmente in vigore anche alle società tecnologiche che sfruttano metodologie di calcolo basate sull'intelligenza artificiale per offrire servizi finanziari. Le consultazioni pubbliche svolte dall'esecutivo europeo hanno, infatti, rilevato che nel settore in esame è presente una diffusa incertezza circa il trattamento normativo dei servizi finanziari forniti mediante l'utilizzazione di modelli computazionali intelligenti[64].

In attesa dell'adattamento della normativa e della vigilanza prudenziale al nuovo ecosistema finanziario, la cui data di scadenza è stata fissata al 2024, la Commissione europea ritiene che le imprese tecnologiche svolgenti – direttamente e/o indirettamente – servizi finanziari debbano essere sottoposte ad una normativa proporzionata e basata, come testé affermato, sul principio ‹‹stessa attività, stesso rischio, stesse norme››. Le motivazioni alla base di tale strategia si rinvengono, come facilmente intuibile, sia in considerazioni di natura micro e macroprudenziale, sia in valutazioni legate principalmente alla tutela della concorrenza e dei consumatori. Quanto al primo aspetto, si afferma che la fornitura di servizi di intermediazione creditizia da parte di soggetti estranei al perimetro di vigilanza bancario può recare nocumento alle esigenze di stabilità finanziaria. Quest'ultima potrebbe, infatti, essere alterata dall'agire di entità che, oltre a non godere di un'esperienza consolidata nel campo dei prestiti o della gestione patrimoniale, si ritroverebbero ad operare nel mercato finanziario senza soggiacere ai limiti prudenziali che invece sono storicamente imposti agli intermediari creditizi[65].

---

si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati». Esempi di applicazione del principio di proporzionalità nel settore finanziario si rinvengono sia nella riduzione dei requisiti patrimoniali per alcune imprese di investimento, sia nell'alleggerimento delle prescrizioni imposte alle banche di dimensioni ridotte: cfr. a tal riguardo la comunicazione *Invito a presentare contributi sul quadro di regolamentazione dell'UE in materia di servizi finanziari*, COM(2016) 855 final del 23 novembre 2016; relazione *Seguito all'invito a presentare contributi sul quadro di regolamentazione dell'UE in materia di servizi finanziari*, COM(2017) 736 final; regolamento (UE) 2019/876 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che modifica il regolamento (UE) n. 575/2013 per quanto riguarda il coefficiente di leva finanziaria, il coefficiente netto di finanziamento stabile, i requisiti di fondi propri e passività ammissibili, il rischio di controparte, il rischio di mercato, le esposizioni verso controparti centrali, le esposizioni verso organismi di investimento collettivo, le grandi esposizioni, gli obblighi di segnalazione e informativa e il regolamento (UE) n. 648/2012 (c.d. CRR II); direttiva (UE) 2019/878 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che modifica la direttiva 2013/36/UE per quanto riguarda le entità esentate, le società di partecipazione finanziaria, le società di partecipazione finanziaria mista, la remunerazione, le misure e i poteri di vigilanza e le misure di conservazione del capitale (c.d. CRD V).

[64] COM(2020) 590 final, cit., p. 12.

[65] In analogia, del resto, alle considerazioni di politica del diritto che in seguito alla crisi finanziaria del 2007-08 sono state sollevate nei confronti degli operatori appartenenti al c.d. sistema bancario ombra: sul punto si veda, tra gli altri, A. NESVETAILOVA (edited by), *Shadow Banking: into the limelight, in Shadow Banking. Scope, Origins and Theories*, London, 2017, p. 238 ss.; in senso conforme, N. BORST, *Shadow Deposits as a Source of Financial Instability: Lessons from the American Experience for China*, May 2013, in Peterson Institute for International Economics, No. PB13-14, reperibile *online*, in quale afferma testualmente che il sistema bancario ombra è nato per offrire agli investitori ordinari un modo per evitare le conseguenze negative della regolamentazione prudenziale allora applicata ai depositi bancari (c.d. *Regulation Q*).

In riferimento invece a questioni di politica concorrenziale e di tutela del consumatore, la Commissione sottolinea il rischio che la struttura di mercato potrà essere rivoluzionata dall'avvento di società tecnologiche che, in assenza di un ‹‹piano da gioco livellato››, potranno espandersi ulteriormente nella fornitura della stragrande maggioranza di servizi finanziari, affrontando al contempo costi di produzione nettamente inferiori rispetto agli altri operatori già attivi nel mercato dei capitali[66]. Se non adeguatamente affrontata, tale situazione di sperequazione regolamentare potrebbe comportare una fuoriuscita generalizzata dal mercato degli operatori finanziari che, *rebus sic stantibus*, non riuscirebbero a reggere la pressione concorrenziale imposta dalle imprese tecnologiche, con conseguente lesione delle posizioni giuridiche proprie degli utenti di servizi finanziari che subirebbero, di conseguenza, una limitazione della possibilità di scelta dei prodotti finanziari offerti sul mercato e aumento dei costi di finanziamento[67].

5. Prime considerazioni.

Nel cercare di commentare la strategia della Commissione europea in tema di finanza digitale, si ritiene importante affrontare, innanzitutto, gli aspetti positivi che tale presa di posizione da parte dell'esecutivo europeo comporta per il mercato finanziario. Nel procedere in tal senso, una menzione particolare deve essere rivolta fin da subito alla riduzione del livello di incertezza normativa che, sul punto, era stata sottolineata dai portatori di interesse nella consultazione pubblica precedente all'emanazione della strategia in esame[68].

In secondo luogo, al fine di rendere l'analisi il più completa possibile, si cercherà di esporre anche alcune criticità della proposta avanzata dall'esecutivo europeo per affrontare il sempre più probabile avvento delle società tecnologiche nell'industria finanziaria. In tale contesto, l'interrogativo che ci si pone attiene per lo più all'opportunità di affrontare una tematica così innovativa come il ricorso agli algoritmi intelligenti nel mercato dei capitali mediante l'applicazione di un principio generale che, seppur

[66] Sulla limitazione della concorrenza derivante dall'operatività delle società tecnologiche v. J.B. BAKER, *The Antitrust Paradigm. Restoring a Competitive Economy*, Cambridge, Massachusetts, 2019, p. 119; in senso conforme, A. ARGENTATI, *Le banche nel nuovo scenario competitivo*, cit., p. 451 la quale, nell'esaminare in chiave critica la probabile espansione delle *Big Tech* nel settore finanziario in senso lato, sottolinea la necessità di applicare un set uniforme di regole in caso di prestazione di servizi bancari.

[67] COM(2020) 590 final, cit., pp. 17-18; EUROPEAN BANKING AUTHORITY, *EBA's FinTech Roadmap. Conclusions from the consultation on the EBA's approach to financial technology (Fintech),* 15 March 2018, reperibile *online*; ID., *Regulatory Perimeter, Regulatory Status and Authorisation Approaches in Relation to Fintech Activities – Report*, 18 July 2019, reperibile *online*.

[68] Per delle considerazioni sulla necessità storica dell'Unione europea di raggiungere adeguati livelli di certezza del diritto al fine di assecondare le capacità di sviluppo delle imprese europee si veda F. GALGANO, *Lex mercatoria*, Bologna, 4ª ed., 2001, p. 133, il quale richiama a tal proposito la prima direttiva europea emanata a questi fini il 9 marzo 1968.

necessario per determinati aspetti, rischia di risultare insufficiente nell'affrontare le nuove sfide regolatorie rappresentate dal *fintech*.

Ciò posto, gli ultimi due paragrafi di tale scritto cercheranno di analizzare questi elementi, fornendo all'uopo delle prime considerazioni sulla strategia più volte citata della Commissione europea in tema di finanza digitale.

5.1. La strategia europea come primo passo necessario.

Data la rapida evoluzione del sistema finanziario, il legislatore europeo non poteva più permettersi di assumere un atteggiamento indifferente nei confronti dell'intelligenza artificiale, posticipando ulteriormente la pubblicazione di iniziative normative aventi ad oggetto l'offerta di prodotti e servizi finanziari mediante lo sfruttamento di algoritmi c.d. intelligenti. A ben vedere, l'importanza della presa di posizione assunta dalla Commissione europea può essere spiegata mediante due ragioni intimamente connesse tra loro e legate alle peculiari caratteristiche dell'economia finanziaria contemporanea.

La prima ragione si rinviene nell'annoso problema dalla carenza di incentivi all'assunzione spontanea di comportamenti virtuosi[69]: nel mercato dei capitali, come noto, la *ratio* della regolamentazione finanziaria è quella di far adottare agli intermediari finanziari una gestione sana e prudente della propria attività che, in assenza di coazione esterna, gli stessi difficilmente seguirebbero[70]. Nel caso di specie, in mancanza di un quadro normativo prudenziale rivolto anche alle società tecnologiche interessate alla fornitura di servizi finanziari, queste ultime difficilmente avrebbero adottato un *modus operandi* tale da contemperare tutti gli interessi in gioco, ed evitando in particolare la diffusione di esternalità negative nel sistema economico. La dottrina maggioritaria, invero, è costante nell'affermare che la delicatezza sistemica delle attività svolte nel mercato finanziario non può spingere il settore pubblico a regredire di fronte alle ipotesi di autoregolamentazione privata. Sebbene quest'ultima sia un fattore in grado di aumentare il livello di efficienza del sistema economico, l'esperienza empirica ha dimostrato come la stessa non sia in grado di assicurare protezione avverso le turbolenze finanziarie di natura sistemica che si manifestano ciclicamente nelle economie capitaliste[71].

La seconda ragione trova, invece, fondamento nella corrente di pensiero che propugna l'incapacità delle legislazioni dettagliate a governare un'economia in continua

[69] È pacifico in dottrina che il compito della regolamentazione sia proprio quello di ottenere dei risultati in termini di benessere collettivo che il mercato, a causa dei suoi insuccessi, non riesce a generare spontaneamente: si v. a tal proposito R. BOWLES, *Diritto e Economia*, Bologna, 1985, p. 229.

[70] Cfr. C. GOODHART, *Introduzione*, in T. PADOA-SCHIOPPA, *Regole e Finanza. Contemperare Libertà e Rischi*, Bologna, 2004, p. 21.

71 Cfr. in senso conforme A. ADMATI, M. HELLWIG, *The Bankers' New Clothes: What's Wrong With Banking and What to Do About It*, Princeton, 2014; T. PADOA-SCHIOPPA, *Regole e Finanza*, cit., p. 67.

trasformazione. Più esattamente, in caso di repentini mutamenti della realtà dovuti all'innovazione, è stato affermato che l'obiettivo di correggere le disfunzioni di mercato non può assolto in maniera adeguata con «la rigidità delle leggi»[72]. Queste ultime potrebbero, infatti, esonerare dalle azioni di vigilanza tutti quegli operatori economici che, sfruttando l'innovazione tecnologica al fine di offrire servizi finanziari, riescono a superare agevolmente il campo di applicazione della disciplina tradizionale. Al contrario, gli sviluppi tecnologici non riuscirebbero ad eludere quelle disposizioni di vigilanza che trovano, invece, fondamento su principi di natura generale i cui obiettivi, essendo ontologicamente di natura ampia, hanno maggiore capacità di resistenza al rischio di obsolescenza. Tale conclusione risulta particolarmente opportuna per il mercato finanziario del ventunesimo secolo che, come indicato in precedenza, tende sempre più ad abbracciare fenomeni di innovazione tecnologica in grado di bypassare le normative di vigilanza nel tempo introdotte dai legislatori nazionali[73].

D'altro canto, è stato più volte affermato che una regolamentazione prevalentemente rigida e basata su prescrizioni e controlli invasivi non si è mai armonizzata *in toto* con le caratteristiche proprie del mercato finanziario. L'evidenza empirica ha, in realtà, dimostrato che quest'ultimo settore dell'economia necessita di una regolazione flessibile che sia in grado di privilegiare non tanto l'aspetto puramente formale della corrispondenza di un determinato comportamento al dettato legislativo, quanto piuttosto l'obiettivo delle autorità di vigilanza di raggiungere un efficiente livello di stabilità finanziaria[74].

Sulla scorta di quanto precede, si può quindi affermare che la scelta della Commissione europea di ricorrere alla flessibilità insita nel principio generale «stessa attività, stesso rischio, stesse norme» al fine di regolamentare la prestazione di servizi finanziari da parte di imprese tecnologiche, oltre ad essere conforme ai canoni di equità

72 F. GALGANO, *Lex mercatoria*, cit., p. 234.

73 Si veda in tal senso T. PADOA-SCHIOPPA, *Regole e Finanza*, cit. p. 108 il quale a tal proposito citava il caso del fallimento della *Enron* in cui la situazione di insolvenza era stata «mascherata» da criteri contabili dettagliati che non erano più in grado di rappresentare la realtà circostante; sulle innovazioni finanziarie che, eludendo le regolamentazioni prudenziali allora vigenti, hanno condotto allo scoppio della bolla immobiliare statunitense del 2007 cfr. R.S. CARNELL, J.R. MACEY, G.P. MILLER, *The Law of Financial Institutions*, 5th ed., New York, 2013, p. 30 ss., in cui si cita a tal proposito il ruolo del modello «*originate-to-distribute*», i *mortgage-backed securities* (MBS) e i *collateralized debt obligation* (CDO); sul tema si veda anche R.A. POSNER, *La crisi della democrazia capitalistica*, Milano, 2014, p. 167 ss. in base al quale uno dei problemi fondamentali della regolamentazione finanziaria si rinviene proprio nel suo «cronico» ritardo rispetto alla velocità insita nell'innovazione finanziaria. Questo concetto viene, in estrema sintesi, riassunto nella massima attribuita dall'Autore a Kenneth Posner, storico *Manager Director* di *Morgan Stanley*, secondo la quale «le banche muovono a t+1 e i regolatori rispondono a t+2»; M. CLARICH, *Populismo, sovranismo e Stato regolatore: verso il tramonto di un modello?*, in *Rivista della regolazione dei mercati*, 2018, n. 1, pp. 1-19, a p. 7; B.S. BERNANKE, T.F. GEITHNER, H.M. PAULSON JR., *Firefighting. The Financial Crisis and Its Lessons*, New York, 2019, p. 8, i quali nel descrivere il rischio di obsolescenza della regolamentazione finanziaria utilizzano la metafora del fiume che, al fine di evitare l'ostacolo rappresentato delle rocce, scorre attorno ad esse.

74 M. RAMAJOLI, *Self regulation, soft regulation e hard regulation nei mercati finanziari*, in *Rivista della regolazione dei mercati*, 2016, n. 2, pp. 53-71, a p. 64.

e certezza del diritto, rappresenti un primo passo necessario nella sfida regolatoria rappresentata dalla transizione digitale[75].

5.2. L'opportunità di un c.d. *regulatory sandbox*?

L'aggettivo necessaria con cui è stata definita nel paragrafo precedente la strategia della Commissione europea in esame lascia, tuttavia, irrisolta la questione della sua eventuale sufficienza. Più precisamente, ad un primo esame critico sembrerebbe destare qualche perplessità il fatto che un mero principio generale possa elevarsi a panacea nei confronti di tutte le problematiche che gli studiosi della materia hanno ricondotto all'agire degli algoritmi intelligenti. Come indicato nel terzo paragrafo, anzitutto, il ricorso all'intelligenza artificiale comporta una serie di rischi più o meno innovativi che la legislazione attualmente in essere nel mercato finanziario non affronta nella sua interezza. Sebbene tematiche come la salvaguardia della trasparenza o la tutela avverso comportamenti discriminatori rappresentino regole di condotta poste a fondamento del mercato mobiliare, la nuova veste che tali rischi assumono in caso di applicazione di algoritmi basati sul *deep learning* non viene presa in considerazione dalla normativa prudenziale vigente. Di conseguenza, la mera enunciazione del principio che attività e rischi simili debbano subire un trattamento normativo similare potrebbe risultare una strategia legislativa claudicante se i primi sollevano, come nel caso di specie, problematiche nuove che, a causa del loro aspetto innovativo, non sono state mai affrontate dal *rulebook* finanziario vigente nell'Unione europea[76].

In secondo luogo, il ruolo crescente che sta assumendo l'innovazione tecnologica nel settore in esame pone in risalto il tema del grado di comprensione, da parte delle pubbliche autorità, delle modalità di funzionamento proprie degli algoritmi intelligenti. È stato al riguardo rilevato che la predisposizione a valle di soluzione giuridiche adeguate all'evoluzione in essere del mercato finanziario non può prescindere da una conoscenza a monte delle nuove soluzioni di allocazione del capitale ad alta intensità tecnologica: a titolo esemplificativo, gli obblighi di informazione e di valutazione dell'idoneità e adeguatezza degli strumenti finanziari previsti dalla disciplina MIFID II[77] a tutela della posizione giuridica dell'investitore dovrebbero essere aggiornati allo scopo di considerare

75 Sulla necessità di non lasciare il settore finanziario al libero mercato cfr. H. MINSKY, *Stabilizing an Unstable Economy*, New York, 2008 (prima ed. 1986), p. 325.

76 Per un'analisi delle difficoltà di riconduzione del *fintech* all'interno delle categorie giuridiche tradizionali, cfr. C. BRUMMER, *Disruptive Technology and Securities Regulation*, in *Fordham Law Review*, 2015, issue 3, pp. 997-1052, reperibile *online*.

77 Cfr. direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE, in particolare la sezione 2 relativa alle disposizioni volte a garantire la tutela degli investitori (art. 24 ss.).

le tecnicalità insite nella progettazione degli algoritmi, ovvero nelle metodi di sfruttamento delle informazioni confluite in quest'ultimo[78].

Al fine di risolvere il nodo normativo del processo di innovazione attualmente in atto, parte della dottrina ha proposto di regolamentare il fenomeno del *fintech* mediante c.d. *regulatory sandboxes*, ossia luoghi non fisici di sperimentazione controllata dalle autorità di vigilanza in cui gli operatori economici possono offrire nuovi soluzioni finanziarie a consumatori reali, sottostando al contempo ad una applicazione proporzionale della legislazione in tema di mercati finanziari[79]. In tal modo, si garantiscono innovazione e apprendimento a favore, rispettivamente, delle imprese e delle autorità di vigilanza atteso che, da un lato, si attenua il rischio che processi innovativi vengano bloccati sul nascere dalle costose barriere regolatorie presenti nel mercato finanziario, e, dall'altro, si consente una conoscenza ‹‹sul campo›› della logica di funzionamento sottostante le nuove tecnologie[80].

In particolare, si afferma in primo luogo che il ricorso ad un *regulatory sandbox* potrebbe rimuovere la barriera all'entrata nel mercato finanziario rappresentata dall'incertezza normativa. Le tempistiche di una riforma legislativa del settore finanziario alla luce delle sfide rappresentate dal *fintech* dovrebbero, infatti, tener conto della

[78] In senso conforme si v. R. LENER, *Il paradigma dei settori regolati*, cit., p. 203

[79] Per una definizione istituzionale di «regulatory sandboxes» si v. EBA, *Discussion Paper on EBA's approach to financial technology (FinTech)*, EBA/DP/2017/02, 2017, p. 7, in cui si afferma testualmente che «regulatory 'sandboxes' provide financial institutions and non-financial firms with a controlled space in which they can test innovative FinTech solutions with the support of an authority for a limited period of time, allowing them to validate and test their business model in a safe environment»; v. anche EUROPEAN SUPERVISORY AUTHORITIES (ESAs), Joint Committee, *FinTech: Regulatory Sandboxes and Innovation Hubs – Report*, 7 January 2019, reperibile *online*.

[80] Cfr. in tal senso M. CARNEY, *The Promise of FinTech*, cit., p. 13, il quale, nel proporre un aggiornamento delle pratiche di vigilanza alla luce delle sfide rappresentate dal *fintech*, citava il fortunato progetto di *sandbox* lanciato dalla Financial Conduct Authority (FCA) in Gran Bretagna nel 2014: cfr. al riguardo https://www.fca.org.uk/firms/innovation/regulatory-sandbox; in senso conforme si veda anche W. RINGE, C. ROUF, *Regulating Fintech in the EU*, cit., p. 612. Per quanto concerne il nostro ordinamento giuridico, iniziative delle autorità di vigilanza aperte all'innovazione tecnologica nel mercato finanziario hanno assunto natura sia operativa, sia regolamentare. Quanto alla prima modalità, i riferimenti corrono, in particolare, al canale di dialogo con gli operatori economici attivato dalla Banca d'Italia (cfr. Canale FinTech) e al progetto «Insurance Blockchain Sandbox» (IBS), una sperimentazione collettiva di prodotti assicurativi basati sulla tecnologia *blockchain* in cui l'IVASS svolge il ruolo di *Institutional Partner*. In riferimento, invece, l'aspetto normativo, una disciplina *ad-hoc* sul *regulatory sandbox* finalizzata a sperimentare soluzioni *fintech* è stata recentemente introdotta dall'art. 36, commi 2*bis*-2*septies*, della legge 28 giugno 2019, n. 58 di conversione del d.l. 30 aprile 2019, n. 34 (c.d. d.l. Crescita). In particolare, sulla base di tale novella legislativa, si attribuisce al Ministro dell'economia e delle finanze, sentiti la Banca d'Italia, la Consob e l'IVASS, il compito di emanare un regolamento contenente condizioni e modalità di svolgimento di una sperimentazione relativa alle attività di tecno-finanza (*FinTech*). Nelle more dell'adozione del regolamento in esame, il MEF ha condotto una consultazione pubblica, aperta ai soggetti interessati (associazioni di categoria, centri di ricerca, università, studi professionali), che si è conclusa il 31 marzo 2020. Per dei primi commenti dottrinali cfr. C. SANDEI, *Le "Initial Coin Offering" nel prisma dell'ordinamento finanziario*, in *Rivista di diritto civile*, 2020, pp. 391-416; F. CAPRIGLIONE, *Industria finanziaria, innovazione tecnologica, mercato*, in *Rivista trimestrale di diritto dell'economia*, 2019, pp. 372-410; E. MACCHIAVELLO, *FinTech*, cit., p. 456; M.T. PARACAMPO, *Dalle regulatory sandboxes al network dei facilitatori di innovazione tra decentramento sperimentale e condivisione europea*, in *Rivista di Diritto Bancario*, 2019, pp. 219-236, reperibile *online*.

necessaria fase di analisi da parte delle autorità *competenti* dei rischi legati alla transizioni digitale[81]. Senonché, questa attività di analisi, potendo comportare un periodo di studio più o meno lungo, potrebbe lasciare il settore *fintech* in una sorta di ‹‹area grigia›› caratterizzata, ovviamente, da un'incertezza assoluta sulla normativa applicabile ai prodotti e/o servizi offerti che si risolverebbe, in ultima istanza, in una rinuncia a investire in innovazione[82]. La predisposizione di una *regulatory sandbox*, invece, consentirebbe ai nuovi operatori interessati alla prestazione di servizi finanziari di testare le rispettive soluzioni *tech* in un ambiente in cui non c'è spazio per incertezza normativa atteso che le regole del gioco sono fissate *ex ante* dalle autorità di vigilanza sulla base delle reali necessità di tutela della stabilità finanziaria[83].

In secondo luogo, si sostiene che l'applicazione di una *regulatory sandbox* migliorerebbe la capacità delle autorità di vigilanza di adempiere le rispettive finalità istituzionali. La possibilità di potersi interfacciare con le nuove soluzioni tecnologiche fin da una fase precoce consentirebbe, a ben considerare, alle autorità di riferimento di raccogliere dati specifici sulle transazioni svolte durante la fase di sperimentazione che, in assenza di un *sandbox*, difficilmente potrebbero essere analizzati. Ciò consentirebbe alle autorità di riferimento di migliorare le capacità di comprensione e gestione dei rischi connessi all'intelligenza artificiale, garantendo così sia il buon funzionamento del mercato, sia la tutela della posizione degli utenti di servizi finanziari. Se si considerano, invero, i rischi di comprensibilità, trasparenza e discriminazione connessi all'utilizzazione di algoritmi intelligenti nel mercato finanziario, ben si comprende la centralità strategica, per le autorità di vigilanza, rappresentata dalla disponibilità di dati precisi sul funzionamento delle nuove tecnologie[84].

Oltre a giovare la posizione delle imprese tecnologiche e delle autorità di vigilanza, si afferma in terzo luogo che un *regulatory sandbox* migliorerebbe anche la posizione dei consumatori. Questi ultimi, infatti, da un lato si potrebbero ritrovare a godere di una maggiore quantità di prodotti finanziari offerti dall'industria finanziaria: l'aumento della pressione concorrenziale nel settore in esame, come noto, comporterebbe un incremento della qualità dei servizi offerti e, allo stesso tempo, una riduzione generalizzata dei costi

[81] Basti pensare all'orizzonte temporale cinquennale indicato nella strategia della Commissione europea per riformare la legislazione finanziaria alla luce della transizione digitale.

[82] Sul rischio della regolamentazione di inibire l'avvio di nuove iniziative nel campo del *fintech* cfr. C. PORZIO, G. SAMPAGNARO, *Rischi delle banche connessi a Fintech*, in F. MAIMERI, M. MANCINI (a cura di), *Le nuove frontiere dei servizi bancari*, cit., p. 333.

[83] Cfr. sul punto W. RINGE, C. ROUF, *Regulating Fintech in the EU*, cit, p. 614, i quali hanno citato come esempio paradigmatico il report «Lessons Learned» della FCA pubblicato nel 2017 in cui si è dimostrato come il *sandbox* inglese, creando un ambiente normativo *market-friendly*, sia riuscito a incrementare il grado di innovazione nel settore finanziario: *Regulatory Sandbox: Lessons Learned Report*, October 2017, reperibile *online*.

[84] Sulla necessità della risorsa dati in presenza di algoritmi intelligenti si veda, tra gli altri, FSB, *Artificial intelligence and machine learning*, cit., p. 28; W. RINGE, C. ROUF, *Regulating Fintech in the EU*, cit., p. 615.

di finanziamento. Dall'altro, la possibilità di ideare uno spazio di sperimentazione con regole di comportamento stabilite in anticipo dalle autorità di vigilanza ridurrebbe il rischio che prodotti innovativi vengano offerti sul mercato da società tecnologiche non regolamentate[85].

I benefici connessi alla scelta di campo a favore di un regime pilota potrebbero, tuttavia, andare perduti qualora si optasse per delle soluzioni eterogenee all'interno dei vari Stati membri[86]. La vocazione *cross-border* dei servizi finanziari offerti dalla ‹‹tecno-finanza›› sembra richiedere, in effetti, la predisposizione di un *regulatory sandbox* pan-europeo attraverso il quale costruire una regolamentazione armonizzata del mercato unico dei capitali. Nel sottolineare i benefici connessi a tale strategia, gli studiosi della materia affermano, invero, che una sperimentazione singola delle regole applicabili al *fintech* a livello euro-unitario potrebbe assumere i connotati di un «luogo privilegiato sia di vigilanza proattiva sui vari rischi paventati, sia di propulsione per eventuali interventi normativi di correzione o di nuova introduzione»[87].

Le possibilità di sviluppo legate all'utilizzazione di un *regulatory sandbox* europeo non sono state ignorate dalla Commissione europea che, in occasione della pubblicazione della strategia sulla finanza digitale in esame, ha anche proposto l'ideazione di un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (*Distributed Ledger Technology* nella terminologia anglosassone). Nello specifico, l'esecutivo europeo ha giustificato tale scelta sulla base dei seguenti obiettivi: (i) garantire la certezza del diritto applicabile ai mercati secondari delle cripto-attività; (ii) sostenere l'innovazione tecnologica mediante l'eliminazione degli ostacoli normativi; (iii) assicurare la tutela dei consumatori e degli investitori; (iv) preservare adeguati livelli di stabilità finanziaria. Al fine di promuovere tali risultati, la Commissione europea ha, quindi, affermato che «è necessario un regime pilota volto a garantire che le modifiche più ampie alla legislazione vigente in materia di servizi finanziari siano basate su dati concreti»[88].

---

[85] Cfr. al riguardo EBA, *Discussion Paper on EBA's approach to financial technology*, cit., p. 47, in cui si afferma che l'assenza di standard regolatori precisi, impedendo la capacità di vagliare il livello di *compliance* nel mercato di riferimento, comporta una riduzione della capacità dei consumatori di stimare le caratteristiche e il grado di rischio di prodotti finanziari innovativi.

[86] Sulla necessità di creare standard internazionali di regolazione di fenomeni come la sicurezza informatica e lo sviluppo dell'intelligenza artificiale, cfr. S. VENKATARAMAKRISHNAN, *Mastercard, SoftBank and others call on G7 to create tech group*, in *Financial Times*, 22 March 2021, in cui si riporta la richiesta avanzata da varie multinazionali ai governi delle principali economie avanzate di creare, in armonia al modello adottato con la costituzione del *Financial Stability Board*, un forum di coordinamento internazionale dedicato alla regolazione *cross-border* delle innovazioni tecnologiche.

[87] Sul punto v. M.T. PARACAMPO, *Dalle regulatory sandboxes al network dei facilitatori*, cit., p. 234 e connessa bibliografia citata.

[88] Cfr. Proposta di Regolamento del Parlamento europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito, COM(2020) 594 final del 24 settembre 2020, p. 2.

In tale contesto, risulta difficile comprendere le motivazioni che abbiano spinto l'esecutivo europeo a proporre un *regulatory sandbox* soltanto per le tecnologie di registro distribuito, scegliendo invece di regolamentare il fenomeno dell'intelligenza artificiale applicata al mercato finanziario mediante il datato principio «stessa attività, stesso rischio, stesse norme». Come è stato affermato in precedenza, la necessità di fondare la strategia di azione su tale principio, sebbene rappresenti un primo passo necessario, potrebbe rivelarsi non sufficiente ad affrontare gli innovativi rischi insiti nell'agire degli algoritmi intelligenti. Il ricorso ad un regime pilota anche per tale aspetto della finanza digitale avrebbe, forse, coadiuvato l'applicazione del principio generale «stessa attività, stesso rischio, stesse norme» nella predisposizione di una nuova architettura di regolazione e vigilanza del mercato finanziario in grado di contemperare le ragioni dell'impresa con le esigenze di protezione sia dell'investitore-risparmiatore sia, più in generale, della stabilità finanziaria. L'uso dell'intelligenza artificiale nel settore finanziario rappresenta, del resto, una realtà che solleva delle nuove sfide difficilmente risolvibili mediante l'uso di vecchi schemi concettuali[89].

[89] In tal senso si vedano le osservazioni di H. MINSKY, *Stabilizing an Unstable Economy*, cit., p. 116 in base al quale «policy cannot be once-and-for-all proposition: as institutions and relations change so does the policy that is needed to sustain coherence».

ABSTRACT: La crisi economica indotta dalla pandemia Covid-19 ha reso improrogabile la necessità di creare un settore finanziario UE maggiormente aperto al progresso tecnologico. È ormai pacifico come la finanza digitale possa rappresentare un fattore in grado di rendere il mercato dei capitali euro-unitario maggiormente efficiente e tale da reggere la pressione concorrenziale esercitata dalle grandi imprese di paesi terzi, Cina e Stati Uniti *in primis*. In tale contesto, lo scorso 29 settembre 2020 la Commissione europea ha presentato alle Istituzioni europee una nuova strategia in materia di finanzia digitale per l'UE allo scopo, da un lato, di rilanciare e modernizzare l'economia europea, e, dall'altro, di apprestare strumenti di tutela a fronte dei rischi provenienti dal ricorso all'innovazione tecnologica nel campo della finanza.
Dopo aver analizzato gli effetti positivi e negativi che possono derivare dall'utilizzo dell'intelligenza artificiale (AI) nel settore in esame, il presente lavoro si focalizza sulle misure proposte dall'esecutivo europeo per disciplinare il fenomeno della fornitura di servizi finanziari da parte di società *Tech*. In particolare, l'oggetto di tale studio è dedicato all'utilizzo del principio «stessa attività, stesso rischio, stesse norme» che la Commissione europea sembrerebbe intenzionata a porre alla base della futura regolamentazione dei rischi legati alla trasformazione digitale. Sebbene tale principio rappresenti un primo passo necessario nell'affrontare le sfide che attendono il mercato europeo, si afferma che queste ultime, dato il loro carattere innovativo, avrebbero forse necessitato anche dell'utilizzazione di un regime pilota (c.d. *regulatory sandbox*).

PAROLE CHIAVE: fintech, BigTech, Commissione europea, intelligenza artificiale, regime pilota.

The European Commission's new digital finance strategy: quid iuris *for (future) financial services provided by Tech companies?*

ABSTRACT: The economic crisis induced by the Covid-19 pandemic has made imperative the creation of an EU financial sector that is more open to technological progress. It is undeniable that digital finance may devise an EU capital market more efficient and able to withstand the competitive pressure exerted by large companies located in countries as China and the United States. In this context, on 29 September 2020, the European Commission presented to the European institutions a new digital finance strategy with the aim, on the one hand of revitalising and modernising the European economy and, on the other, providing protection against the risks arising from the use of technological innovation in the capital markets.

After analysing the consequences that may arise from the use of artificial intelligence (AI), this paper focuses on the measures proposed by the European Commission to properly regulate the provision of financial services by Tech companies. In particular, the subject of this study is dedicated to the use of the principle of «same activity, same risk, same rules» that the European institutions want to place at the basis of regulation of risks linked to digital transformation. Although this principle represents a necessary first step in addressing the challenges facing the European capital markets, it is argued that the innovative nature of these challenges might also have required the use of a regulatory sandbox.

KEYWORDS: fintech, BigTech, European Commission, artificial intelligence, regulatory sandbox.

La rilevanza delle competenze professionali della forza lavoro nella transizione digitale europea

Carlo Valenti*

SOMMARIO: 1. Il processo di digitalizzazione dell'Unione europea tra vecchie e nuove iniziative. – 2. Gli ostacoli alla piena transizione digitale: dall'analfabetismo informatico allo *skill mismatch*. – 3. Il processo di *upskilling* e *reskilling*: il caso francese del *Compte personnel de formation*. – 4. Osservazioni conclusive.

1. Il processo di digitalizzazione dell'Unione europea tra vecchie e nuove iniziative.

Tra le priorità strategiche dell'Unione europea figura ormai da molto tempo e in modo sempre più sistematico l'obiettivo della trasformazione digitale, che nelle sue molteplici sfaccettature costituisce sia un'opportunità non indifferente per favorire lo sviluppo e la crescita del tessuto socioeconomico, sia una sfida costante sul piano internazionale per affermare la propria indipendenza tecnologica[1]. Appare infatti inevitabile che il fenomeno della digitalizzazione finisca per intrecciarsi indissolubilmente alle principali iniziative europee in qualità di elemento ormai imprescindibile, essendo questo dotato di capacità pervasive tali da interessare trasversalmente la sfera sociale, economica, giuridica e amministrativa. Si pensi ad esempio a come la forte spinta tecnologica nel corso degli anni abbia portato non solo all'efficientamento dei modelli organizzativi e produttivi delle imprese risultante nella nascita della c.d. quarta rivoluzione industriale[2], ma anche al graduale processo di aggiornamento e ammodernamento dell'apparato normativo[3].

È dunque in tale prospettiva che la Commissione europea ha profuso un continuo impegno nello sviluppo delle tecnologie dell'informazione e della comunicazione (TIC), le quali, pur non essendo espressamente richiamate nelle disposizioni dei TFUE, hanno

* Dottorando di ricerca in Scienze giuridiche europee ed internazionali, Università degli Studi di Verona.

[1] Per un approfondimento sul tema della sovranità digitale si veda: C. HOBBS (ed.), *Europe's digital sovereignty: From rulemaker to superpower in the age of Us-China rivalry*, European Council on Foreign Relations essay collection, 2020, n. 336, reperibile *online*.

[2] Sui cambiamenti nel mondo del lavoro scaturiti in seguito alla diffusione del modello dell'Industria 4.0 si vedano: K. SCHWAB, *The Fourth Industrial Revolution*, New York, 2017; F. SEGHEZZI, *La nuova grande trasformazione. Lavoro e persona nella quarta rivoluzione industriale*, Bergamo, 2017.

[3] A tal riguardo, si prendano a titolo esemplificativo per l'ordinamento italiano le sostanziali modifiche apportate in materia penale ai reati informatici con il passaggio dalla legge 23 dicembre 1993, n. 547 alla legge 18 marzo 2008, n. 48, nonché la riscrittura nella disciplina lavoristica dei controlli a distanza *ex* art. 4 della legge 20 maggio 1970, n. 300 da parte del decreto legislativo 14 settembre 2015, n. 151.

trovato spazio all'interno delle politiche settoriali e orizzontali, soprattutto nell'ambito industriale e commerciale, oltreché dell'istruzione e della ricerca e dello sviluppo[4]. Volendo ripercorrere le principali tappe del processo di digitalizzazione, è possibile osservare come gli interventi strategici – inizialmente incentrati su un complessivo potenziamento delle infrastrutture tecnologiche e delle reti *internet* per favorire la comunicazione e la connessione – abbiano gradualmente interessato finalità sempre più attinenti al progresso sociale ed economico, quali l'alfabetizzazione informatica della popolazione, il rafforzamento dei servizi digitali pubblici e privati, la creazione di un'identità digitale legalmente riconosciuta e la costruzione di un mercato unico digitale[5]. Del resto, è proprio nelle numerose e potenziali applicazioni di tali strumenti che l'Unione europea ha trovato un valido mezzo per sostenere la cooperazione tra i Paesi membri ed essere più competitiva sul piano internazionale.

In merito alle iniziative più rilevanti, è innanzitutto doveroso menzionare i primi sforzi intrapresi tra il 1983 e il 1988 con i programmi quadri ESPRIT e RACE, i quali, pur non costituendo delle vere e proprie azioni strategiche comunitarie, concernevano la promozione della ricerca e dello sviluppo del settore ICT in un'ottica di maggiore diffusione degli strumenti telematici[6]. In particolare, questi erano volti a potenziare le tecnologie delle telecomunicazioni (es. *software*, microelettronica avanzata, sistemi per l'elaborazione delle informazioni) e investire così nella competitività industriale europea.

È infatti nel quinquennio successivo – periodo in cui vengono introdotti rispettivamente il Libro verde sullo «sviluppo del mercato comune dei servizi e delle apparecchiature di telecomunicazione»[7] nel 1987 e il Libro bianco «Crescita, competitività, occupazione»[8] nel 1993 – che hanno preso forma delle strategie organiche e unitarie in materia di TIC fortemente focalizzate sul progresso del piano sociale e produttivo e sul potenziamento degli strumenti telematici e dell'informazione.

In tale prospettiva, si è andato progressivamente concretizzando il progetto della «Società dell'Informazione per Tutti», che tramite le azioni programmatiche di *eEurope*[9]

[4] In particolare, agli artt. 179-190 TFUE sulle disposizioni in materia di ricerca e sviluppo tecnologico.

[5] Il mercato unico digitale, il cui fondamento giuridico è derivabile dagli artt. 4, 26, 27, 114 e 115 TFUE, può essere descritto come una struttura unitaria e priva di barriere interne alla diffusione dei servizi e delle tecnologie digitali, che incentiva il commercio *online* e favorisce gli investimenti in infrastrutture tecnologiche.

[6] Cfr. D. ASSIMAKOPOULOS, R. PIEKKARI e S. MACDONALD, *ESPRIT: Europe's Response to US and Japanese Domination*, in R. COOPEY (edited by), *Information Technology Policy: An International History*, Oxford, 2004, pp. 247-263; L. MYTELKA e M. DELAPIERRE, *The alliance strategies of European firms in the information technology industry and the role of Esprit*, in *Journal of Common Market Studies*, 1987, vol. 26, n. 2, pp. 231-253.

[7] Cfr. COM(87) 290 final del 30 giugno 1987.

[8] COM(1993) 700 def. del 5 dicembre 1993. Per un approfondimento si rimanda a G. PARAMITHIOTTI, *Il Libro Bianco di Delors per la crescita economica, la competitività e l'occupazione in Europa*, in *Il Politico*, 1995, vol. 60, n. 2 (173), pp. 293-311.

[9] Il programma *eEurope* (COM(2000) 130 definitivo dell'8 marzo 2000) si è articolato tra il 2000 e il 2010 circa in tre fasi (*eEurope* 2002, *eEurope* 2005 e i2010) e ha promosso una massiccia diffusione

ha intrapreso un intenso percorso di liberalizzazione nel campo tecnologico; ciò è stato perseguito incentivando l'utilizzo di *internet* da parte di cittadini e imprese e promuovendo investimenti nella formazione digitale della popolazione, nonché cercando al contempo di definire un quadro normativo adatto a favorire l'*e-commerce* e a sfruttare il potenziale insito nell'economia digitale per conseguire una maggiore crescita, produttiva e occupazionale, dell'Unione europea.

Tuttavia, è con l'introduzione nel 2010 della Strategia Europa 2020 – brevemente riassumibile come un ampio programma strategico di investimenti in cinque aree prioritarie[10] per favorire la ripresa in seguito ai danni della Grande Recessione finanziaria del 2008 – che si può osservare una forte centralità del tema della transizione digitale e una migliore organicità delle politiche sulle TIC. L'ambiziosa visione di lungo periodo qui contenuta si basava in particolare sull'instaurazione di un modello di crescita intelligente, sostenibile e inclusivo, obiettivo che richiedeva necessariamente la definizione di un sistema economico fondato sull'efficienza e la competitività, oltreché in grado di garantire alti livelli occupazionali e di coesione sociale[11].

Per perseguire queste finalità, la Commissione europea ha inserito tra i pilastri fondamentali di tale iniziativa la c.d. Agenda digitale europea[12], vale a dire un piano contenente una serie di risultati programmatici da conseguire entro il 2020 in materia di tecnologie digitali: questa si prefiggeva tra l'altro il complesso compito di rafforzare la connettività mediante TIC e stimolare gli investimenti in ricerca e sviluppo, mirando non solo a favorire l'alfabetizzazione informatica della popolazione e la diffusione dell'*e-government*, ma anche ad aggiornare il quadro normativo in funzione del consolidamento del mercato unico digitale[13]. In questo modo, ha pertanto perseguito il potenziamento delle infrastrutture tecnologiche e l'accrescimento delle competenze in ambito digitale, sfruttando il potenziale della digitalizzazione per conseguire un modello di crescita sostenibile e inclusivo.

A tal riguardo, occorre sottolineare che tra i numerosi interventi legislativi[14] volti

---

delle TIC al fine di rafforzare l'economia europea in un'ottica di maggiore competitività e sostenibilità. Tra i principali obiettivi figuravano la riduzione dei costi di navigazione *internet*, la promozione delle competenze digitali della popolazione e un rafforzamento della sicurezza delle reti informatiche e dei servizi pubblici digitali.

[10] COM(2010) 2020 del 3 marzo 2010. Le aree prioritarie comprendevano in particolare ricerca e sviluppo, occupazione, integrazione sociale, istruzione e sostenibilità climatica ed energetica.

[11] Si vedano a tal proposito M. JESSOULA, C. AGOSTINI, S. SABATO, *Europa 2020 e lotta alla povertà: obiettivi hard, processi soft, governance in fieri*, in *Politiche Sociali*, 2014, n. 1, pp. 101-118; E. MARLIER, D. NATALI e R. VAN DAM, *Europe 2020: Towards a more social Eu?*, Bruxelles, 2010; P. POCHET, *Eu 2020. Social impact of the new form of European governance*, in *Etui Policy Brief*, 2010, n. 5.

[12] COM(2010) 245 definitivo del 19 maggio 2010.

[13] Per un approfondimento si veda G. CAGGIANO, *Il quadro normativo del mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato Unico Digitale, dati personali e diritti fondamentali*, in *Eurojus.it*, 2020, fasc. spec., pp. 13-49, reperibile *online*.

[14] Cfr. M. MACIEJEWSKI, I. OZOLINA, J. FERGER, C. PIAGUET, J. APAP, M. DESOMER, A. GRONBECH JORGENSEN, B. HARDT, B. LEFORT, B. MATIC, S. VANHOUCKE, *EU Mapping: Overview of Internal Market*

al completamento del mercato unico digitale europeo entro il 2015 – promossi principalmente mediante un massiccio ricorso a direttive, proposte legislative, regolamenti e comunicazioni – le iniziative chiave si sono concentrate in particolare sulla liberalizzazione e sul potenziamento dei servizi di *e-commerce* e delle infrastrutture di comunicazione, sull'accrescimento della fiducia dei consumatori verso la rete, sul rilancio dell'*e-government* e sull'aggiornamento della normativa in materia di protezione dei dati[15].

Non potendo affrontare dettagliatamente in questa sede tutte le misure intraprese nell'ultimo decennio per la realizzazione del mercato unico digitale, si ritiene importante soffermarsi sui due principali interventi attribuibili all'Agenda digitale europea: da un lato, la Strategia per il mercato unico digitale in Europa[16], che dal 2015 ha cercato di gettare le basi in un'ottica di sostenibilità e coesione per una maggiore digitalizzazione del tessuto sociale e produttivo[17]. Tra queste figuravano ad esempio la promozione dei servizi digitali per imprese e consumatori europei e il rafforzamento dell'*e-commerce*, obiettivi da conseguire mediante la definizione di un quadro normativo in grado di massimizzare la diffusione della tecnologia e favorire così la crescita dell'economia digitale per l'Unione europea. In particolare, tale strategia si prefissava il compito di rimuovere tutti gli ostacoli all'accesso e all'utilizzo dei servizi *online* da parte dei cittadini e delle imprese (es. geoblocchi ingiustificati tra Paesi membri), andando al contempo a rinnovare l'apparato giuridico europeo per poter garantire la protezione dei dati e un chiaro trattamento delle informazioni personali sulla rete[18].

Dall'altro, la strategia per la «Digitalizzazione dell'industria europea» (DEI)[19], lanciata nel 2016 per favorire l'implementazione delle azioni finalizzate alla trasformazione digitale delle imprese e, in definitiva, il conseguimento di una maggiore competitività industriale. In tale prospettiva, la Commissione europea ha voluto raccomandare ai Paesi membri di attuare tutte le misure necessarie a garantire un'agile

and Consumer Protection related legislation, European Parliament, Study for the IMCO Committee, Bruxelles, 2015, PE 536.317, pp. 19-23, reperibile *online*.

[15] Appare infatti chiaro come non si potesse svincolare la promozione del mercato unico digitale dal rafforzamento delle norme a tutela dei dati personali, della sicurezza *online* e della *privacy* dei cittadini.

[16] Cfr. COM(2015) 192 final del 6 maggio 2015.

[17] Tra i principali traguardi perseguiti da tale strategia occorre sottolineare il processo di ammodernamento in materia di dati e l'eliminazione delle barriere informatiche tra Paesi membri (abolizione dei costi di *roaming*, portabilità dei contenuti digitali, sblocco del commercio elettronico, ecc.), che miravano in definitiva a superare i vincoli normativi vigenti all'interno dell'Unione Europea per la promozione dell'economia digitale.

[18] Cfr. 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).

[19] Cfr. COM(2016) 180 final del 19 aprile 2016. Per un approfondimento, si veda: J.S. MARCUS, G. PETROPOULOS, T. YEUNG, *Contribution to growth: The European Digital Single Market. Delivering economic benefits to citizens and businesses*, European Parliament, Study for the Committee on the Internal Market and Consumer Protection, Lussemburgo, 2019, reperibile *online*.

transizione verso il nuovo scenario derivante dalla digitalizzazione del mercato globale[20]. La Strategia DEI si basava soprattutto su cinque pilastri[21] per agevolare un effettivo ingresso nella Quarta Rivoluzione Industriale, spaziando in particolare dalla creazione di una piattaforma virtuale comune di iniziative nazionali per la digitalizzazione industriale e di centri d'innovazione digitale (DIH) sul territorio alla definizione di un quadro normativo *digital-friendly* e al rafforzamento delle competenze della popolazione europea. Sulla base di questi obiettivi, si intendeva dare seguito a una serie di investimenti finanziari e di iniziative legislative coordinate per promuovere il rilancio industriale e sfruttare il potenziale tecnologico.

Arrivati dunque alla conclusione del piano decennale dell'Agenda Digitale, appare rilevante sottolineare come l'Unione europea abbia non solo fatto notevoli progressi[22] nel processo di transizione digitale, ma anche riformulato da ultimo la propria politica digitale in vista della fine del 2020, sostenendo che la nuova strategia debba bilanciare in modo ancor più accurato la necessità di sfruttare il pieno potenziale della digitalizzazione per la crescita economica con la dimensione etica e sostenibile dello sviluppo. È infatti opinione del Consiglio dell'Unione europea che la tecnologia debba necessariamente essere al servizio della popolazione e delle imprese per «accrescere la competitività digitale ed economica e la coesione digitale in tutta l'Unione»[23].

A tal riguardo, il conseguimento di questi ambiziosi obiettivi – ulteriormente reso indispensabile in seguito ai danni e alle disuguaglianze generati dalla pandemia da Covid-19 – intende passare in particolare dalla promozione dell'intelligenza artificiale, dal rafforzamento della cybersicurezza, da un maggiore impiego della tecnologia *blockchain* e dei sistemi *cloud* e dall'accrescimento delle competenze digitali della popolazione. Del resto, la crisi pandemica ha dimostrato quanto sia essenziale la componente tecnologica nel contesto odierno, fattore sul quale l'Unione europea intende fondare la propria ripartenza per il post-pandemia.

Per questo motivo, l'annuncio della strategia «*Digital Compass*» per la definizione delle priorità in materia di digitalizzazione da conseguire entro il 2030 e la decisione di destinare almeno il 20% dei fondi stanziati per la ripresa e il rilancio dai danni della pandemia al programma di transizione digitale[24] costituiscono certamente dei segnali importanti da parte della Commissione europea. Sarà pertanto necessario attendere i futuri sviluppi per comprendere al meglio la direzione intrapresa con le politiche per il

[20] In merito ai progressi fatti in tal senso si veda per il caso spagnolo: L. MELLA MÉNDEZ, *Industria 4.0 e la sfida della formazione in Spagna*, in *Diritto delle Relazioni Industriali*, vol. 28, n. 2, 2018, pp. 413-429.

[21] A tal proposito, si rimanda alla scheda di approfondimento del mercato unico digitale dell'Unione Europea «Pillars of the Digitising European Industry initiative», reperibile *online*.

[22] Sui primi esiti dell'iniziativa DEI, si veda EUROPEAN COMMISSION, *Digitising European Industry: Progress so far, 2 Years after the Launch*, Bruxelles, 2018, reperibile *online*.

[23] Comunicato stampa del Consiglio dell'UE, 7 giugno 2019.

[24] Cfr. COM(2020) 456 final del 27 maggio 2020.

decennio 2020-2030, che tra le principali priorità si pongono ad ora la promozione della competitività e dell'innovazione europea, nonché la creazione di nuovi posti di lavoro e un complessivo miglioramento delle condizioni di vita della popolazione.

2. Gli ostacoli alla piena transizione digitale: dall'analfabetismo informatico allo *skill mismatch*.

Osservando nel complesso le strategie programmatiche attuate dall'Unione europea negli ultimi anni, è possibile notare come le nuove tecnologie siano considerate dei «fattori abilitanti» in grado di garantire la crescita e il progresso sul piano sociale ed economico. Se infatti negli anni Ottanta si era preso ad esempio il modello di sviluppo giapponese basato sulla spinta tecnologica, all'inizio nuovo millennio il parametro di riferimento si era già spostato verso l'approccio statunitense incentrato su flessibilità, innovazione e competitività, essendo questo visto come un metodo innovativo per favorire una rapida e prosperosa crescita economica. È invece dal 2010 che si fa gradualmente spazio un modello strategico più incentrato sulla sostenibilità e l'inclusività per uno sviluppo più coeso dell'Unione europea, logica ulteriormente confermata alla luce dei bruschi cambiamenti intercorsi dall'insorgere della crisi pandemica da Covid-19; quest'ultima ha infatti dimostrato quanto sia dispensabile accelerare la sopramenzionata trasformazione tecnologica e investire maggiormente sulla digitalizzazione dei servizi, sull'interconnessione delle banche dati, sullo sviluppo di infrastrutture informatiche moderne e reti veloci.

A tal proposito, appare chiaro che il nuovo piano decennale per la transizione digitale – incentrato su diversi settori chiave e molteplici ambiti d'intervento[25] – debba necessariamente affrontare con maggiore attenzione la questione delle competenze digitali: se è vero, infatti, che il progetto della digitalizzazione europea deve innanzitutto basarsi sul rafforzamento della connettività e dei servizi digitali pubblici e privati, questo non può altresì prescindere da un più cospicuo investimento nell'apprendimento continuo, finalizzato soprattutto all'accrescimento delle capacità tecniche e professionali. Del resto, il mancato possesso di adeguate conoscenze digitali da parte della popolazione andrebbe inevitabilmente sia a limitare le potenzialità derivanti dalla trasformazione tecnologica, sia a rallentarne il complessivo processo di implementazione.

Volendo comprendere in modo più chiaro i progressi fatti nel corso degli anni dall'Unione europea in materia di digitalizzazione e capitale umano, è doveroso rimettersi

[25] La nuova «bussola per il digitale» che andrà a determinare gli obiettivi da conseguire entro il 2030 pare ad oggi interessare le seguenti aree tematiche: economia dei dati e tassazione del digitale, connettività e cybersicurezza, sovranità digitale, intelligenza artificiale, digitalizzazione della giustizia e della sanità, servizi digitali, istruzione e competenze digitali.

a quanto evidenziato dal *Digital Economy and Society Index* (DESI)[26], vale a dire un indicatore che permette di osservare in modo dettagliato la situazione socioeconomica dei Paesi membri. A tal riguardo, per quanto concerne i dati relativi all'ultimo rapporto DESI, è possibile costatare come, nonostante ormai l'85% dei cittadini europei utilizzi *internet* pressoché quotidianamente per motivi personali o lavorativi, il tasso di analfabetismo informatico[27] si attesti ancora al 42%. Tale risultato, pur essendo il frutto di un graduale miglioramento verificatosi negli ultimi cinque anni, evidenzia un quadro non incoraggiante, in cui solamente il 58% dei cittadini europei risulta realmente in possesso di competenze digitali basilari[28]. Si pensi inoltre al caso della popolazione italiana, ben al di sotto della media europea e collocata all'ultimo posto nei parametri inerenti al capitale umano con un tasso di analfabetismo informatico del 58%.

Un simile ritardo nella padronanza delle basilari competenze informatiche – che ormai figurano come requisito fondamentale ai fini dell'assunzione anche per le prestazioni lavorative a bassa e media qualificazione – contribuisce non solo ad acuire il problema dei «giacimenti occupazionali inutilizzati» 29, ma anche ad accrescere il *mismatch* tra domanda e offerta di lavoro[30]. In particolare, ci si intende riferire sia al disallineamento che intercorre tra le competenze offerte dai lavoratori e quelle effettivamente richieste dalle imprese (*skill mismatch*), sia all'impossibilità di acquisire le figure professionali dotate delle abilità desiderate nell'attuale mercato del lavoro (*skill shortage*)[31]. Tali esternalità negative sono spesso frutto mancata corrispondenza tra le conoscenze teoriche e pratiche maturate dalla forza lavoro durante il periodo di formazione e quanto effettivamente ricercato dai datori di lavoro.

Simili fenomeni risultano particolarmente problematici, specialmente se a fronte di

[26] Il *Digital Economy and Society Index* fornisce dal 2014 un dettagliato resoconto annuale circa il livello di digitalizzazione dell'Unione Europea, monitorando le aree tematiche di maggiore interesse (es. connettività, capitale umano, utilizzo di internet, integrazione della tecnologia digitale, servizi pubblici digitali) ed evidenziando per ciascun indicatore le lacune e i progressi svolti dai rispettivi Paesi membri.

[27] Con l'espressione «analfabetismo informatico» si intende il mancato possesso delle basilari competenze digitali che permettono di utilizzare un computer o di ricercare e comprendere le informazioni presenti sulla rete.

[28] Mentre quelli con competenze al di sopra del livello base si attestano al 33%.

[29] Così P. ICHINO, *L'intelligenza del lavoro. Quando sono i lavoratori a scegliersi l'imprenditore*, Segrate, 2020, pp. 1-20. Tale incremento delle posizioni lavorative vacanti si manifesta nel caso in cui risulti impossibile occupare tali impieghi scoperti a causa dell'assenza di profili idonei o delle competenze necessarie da parte dei soggetti in cerca di lavoro.

[30] Per un approfondimento sul tema, si vedano CEDEFOP, *Hai quello che serve? Lo skill mismatch in Europa*, Nota informativa Cedefop, giugno 2010, reperibile *online*; ILO, *Skills mismatch in Europe: Statistics Brief*, Ginevra, 2014, reperibile *online*.

[31] Cfr. G. BRUNELLO, P. WRUUCK, *Skill Shortages and Skill Mismatch in Europe: A Review of the Literature*", in *IZA DP*, 2019, n. 12346, pp. 3-26; CEDEFOP, *Insights into skill shortages and skill mismatch. Learning from Cedefop's European skills and jobs survey*, Bruxelles, 2018, reference series n. 106, pp. 12-17, reperibile *online*; ID., *The skill matching challenge. Analysing skill mismatch and policy implications*, Bruxelles, 2010, reperibile *online*.

un utilizzo sempre maggiore di personale ICT da parte delle imprese[32] si considerano le crescenti difficoltà di reperimento di personale specializzato (*data analyst*, *software developer*, ecc.) che contribuiscono a lasciare scoperte le posizioni lavorative più richieste. Pertanto, sebbene il recente progresso tecnologico abbia contribuito a rendere sempre più efficienti i modelli produttivi e organizzativi del lavoro, appare chiaro come questo al contempo non solo aumenti la domanda di profili professionali altamente qualificati, ma finisca anche per deteriorare inevitabilmente il valore delle competenze preesistenti e accelerare il processo di «obsolescenza delle conoscenze»[33].

Per questo motivo, pare potersi affermare che il disallineamento delle competenze tra domanda e offerta di lavoro – anche frutto del crescente divario tra le esigenze delle imprese in materia di professionalità e quanto offerto attualmente dalla forza lavoro[34] – rappresenti sia un mancato sfruttamento dei benefici che possono derivare della digitalizzazione, sia una perdita di efficienza non indifferente per quanto riguarda la produttività delle imprese[35].

Di conseguenza, il rafforzamento della professionalità della forza lavoro può essere considerato come fattore abilitante per agevolare la transizione digitale europea, oltreché come strumento per garantire migliori occasioni di inserimento e rinserimento lavorativo. È infatti grazie al conseguimento di una maggiore occupabilità[36] che la popolazione in età lavorativa può fronteggiare i rapidi cambiamenti di un mercato del lavoro sempre più specializzato e influenzato dal progresso tecnologico. Del resto, una piena transizione digitale permetterebbe di affrontare gli *shock* esterni con maggiori strumenti e risorse, nonché di incrementare la competitività e la crescita occupazionale dell'Unione europea. In tale prospettiva, acquisisce una forte rilevanza il tema delle politiche attive di accrescimento delle competenze professionali, dal momento che sembrano porsi tra soluzioni più idonee a contrastare l'obsolescenza delle conoscenze, il *mismatch* delle

[32] Sempre secondo l'ultimo rapporto DESI, mentre solamente il 15% delle piccole imprese europee impiega personale specializzato ICT, è possibile osservare un forte e continuo aumento percentuale per quelle di medie dimensioni (42,5%) e per le grandi attività (75%).

[33] Sull'effetto dei processi di digitalizzazione nel mondo del lavoro si vedano a titolo esemplificativo P. TULLINI, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. TULLINI (a cura di), *Web e lavoro, Profili identitari e di tutela*, Torino, 2017, pp. 3-20; M. WEISS, *Digitalizzazione: sfide e prospettive per il diritto del lavoro*, in *Diritto delle Relazioni Industriali*, 2016, n. 3, pp. 651-663.

[34] Cfr. M. VELCIU, *Job mismatch – effects on work productivity*, in *SEA - Practical Application of Science*, 2017, vol. 5, issue 15, pp. 395-398.

[35] In tale ottica, questa esternalità negativa è stata descritta dal Boston Consulting Group come una sorta di «tassa nascosta» sull'efficienza e la produttività dei paesi dell'OCSE, che concerne oltre 1,3 miliardi di persone in tutto il mondo e genera una perdita di produttività globale del 6%. Si vedano J. PUCKETT, V. BOUTENKO, L. HOTEIT, K. POLUNIN, S. PERAPECHKA, A. STEPANENKO, E. LOSHKAREVA, G. BIKKULOVA, *Fixing the Global Skills Mismatch*, Boston Consulting Group, report 15 gennaio 2020, reperibile *online*.

[36] Pur non essendovi una definizione univoca, tale espressione può essere riassunta come la capacità da parte di un individuo di mantenere un impiego o di trovarne di nuovi grazie al valore del proprio bagaglio professionale.

competenze e, in definitiva, l'effetto delle c.d. *disruptive innovation*[37].

3. Il processo di *upskilling* e *reskilling*: il caso francese del *Compte personnel de formation*.

Le continue trasformazioni derivanti dall'attuale processo di digitalizzazione, come rilevato in precedenza, hanno portato il mondo del lavoro a porre un'attenzione sempre maggiore sul valore delle competenze professionali e delle conoscenze cognitive della forza lavoro[38], essendo queste non solo motivo di valore aggiunto per la parte datoriale, ma anche elemento fondamentale delle principali prestazioni lavorative odierne. Del resto, le imprese dotate di capitale umano qualificato e in grado di adattarsi, se non anticipare, le sfide dovute ai cambiamenti socioeconomici sono quelle che riescono a adottare correttamente e con più facilità le nuove tecnologie all'interno dei propri modelli organizzativi e produttivi, andando così a risultare più competitive sul mercato.

Tuttavia, come evidenziato dalle analisi contenute nel rapporto DESI per il 2020, la popolazione europea appare ancora contraddistinta da livelli di analfabetismo informatico non indifferenti e basse percentuali di specializzati in ambito ICT. Tale problematica, unita al crescente disallineamento delle competenze, finisce per avere delle inevitabili ricadute sulla capacità delle attività europee di inserire all'interno dei propri modelli organizzativi e produttivi le nuove tecnologie[39], costituendo così un limite alla competitività sul piano internazionale. Appare pertanto chiaro come il forte impatto della digitalizzazione, che ha interessato in modo sempre maggiore il mondo del lavoro, richieda inevitabilmente un costante processo di adeguamento delle competenze della forza lavoro sia per acquisire una professionalità maggiormente spendibile, sia per adeguarsi i cambiamenti che il progresso tecnologico sta portando sul piano sociale[40].

In tale prospettiva, assumono una forte rilevanza le misure per la riqualificazione e l'accrescimento delle competenze della popolazione, essendo queste in grado di agevolare il processo di transizione verso l'era digitale, oltreché verso i nuovi modelli produttivi e organizzativi nel mondo del lavoro. Tali iniziative permettono infatti, da un

[37] Proprio per questa ragione rientra tra gli obiettivi programmatici da conseguire entro il 2025 una drastica riduzione dell'analfabetismo informatico grazie a maggiori investimenti nelle competenze della forza lavoro e nell'istruzione digitale. Sul tema, si veda: V. FILÌ, F. COSTANTINI, *Legal Issues in the Digital Economy. The Impact of Disruptive Technologies in the Labour Market*, Newcastle upon Tyne, 2019.

[38] S. CIUCCIOVINO, *Le nuove questioni di regolazione del lavoro nell'industria 4.0 e nella gig economy: un "problem framework" per la riflessione*, in *Diritto delle Relazioni Industriali*, 2018, n. 4, p. 1059.

[39] A tal riguardo, occorre precisare che l'Unione Europea si trova al momento in una posizione di svantaggio rispetto agli Stati Uniti anche causa delle barriere strutturali che rallentano gli investimenti nella digitalizzazione e l'adozione delle nuove tecnologie da parte delle imprese. Si veda in merito EIB, *Who is prepared for the new digital age? - Evidence from the EIB Investment Survey*, European Investment Bank report, 2020, reperibile *online*.

[40] Si pensi a tal proposito alla crescente diffusione dell'*e-government* e dei servizi pubblici digitali per i cittadini.

lato, di rafforzare l'occupabilità della forza lavoro alla luce della crescente precarizzazione del lavoro e frammentazione della vita lavorativa e fornire così maggiori protezioni dal rischio di disoccupazione[41] e, dall'altro, di favorire l'apprendimento continuo durante tutto l'arco della vita per l'intera popolazione[42].

Volendo pertanto osservare un esempio di politica di *lifelong learning*[43] della popolazione, appare interessante soffermarsi sulla strategia adottata dal Ministero del lavoro francese dal 2014, che ha cercato di semplificare non solo il piano della formazione continua, ma anche quello previdenziale. Tale ripensamento complessivo delle misure assistenziali e occupazionali ha visto innanzitutto l'abrogazione del *droit individuel à la formation* (DIF) a seguito dell'introduzione della legge 5 marzo 2014, n. 288 in favore del *Compte personnel de formation* (CPF) nel 2015, che si è affermato come principale meccanismo di finanziamento pubblico per la formazione continua[44]. Mentre il precedente dispositivo aveva introdotto per i lavoratori del settore pubblico e privato un diritto individuale a ricevere della formazione continua annuale per l'aggiornamento professionale, il nuovo conto personale ha inteso estendere tale riconoscimento a tutti i cittadini francesi in età per il lavoro a prescindere dalla condizione occupazionale posseduta; si va dunque a definire un diritto soggettivo alla formazione continua per tutta la durata della vita lavorativa ed esercitabile sulla base della quantità di lavoro annuale effettivamente svolto. In particolare, il CPF ha inizialmente inteso fornire a tutti i soggetti dai 16 anni in su un credito da utilizzare per il proprio accrescimento professionale, ovvero fino a 24 ore all'anno per un massimo cumulativo di 150 ore in cinque anni. È possibile dunque notare come il modello francese abbia inteso definire nella sua ambiziosa riforma un diritto individuale alla formazione continua universalmente riconosciuto sulla base della cittadinanza, capitalizzabile nel tempo ed esercitabile autonomamente durante tutto l'arco della vita lavorativa.

Risulta inoltre importante sottolineare come le novità introdotte tra il 2014 e il 2018 abbiano riguardato tra l'altro non solo un'ampia riforma della formazione professionale,

[41] In particolare, il possesso di solide competenze professionali e trasversali garantisce per un lavoratore non solo un minore rischio di perdita del lavoro, essendo i profili qualificati più difficili da reperire sul mercato del lavoro, ma anche maggiori opportunità e minori tempi di attesa per il rinserimento lavorativo. Sul tema dell'occupabilità, si vedano B. CARUSO, *Occupabilità, formazione e "capability" nei modelli giuridici di regolazione dei mercati del lavoro*, in *Diritto del lavoro e delle relazioni indistriali*, 2007, fasc. 113; M. ROCCELLA, *Formazione, occupabilità, occupazione nell'Europa comunitaria*, *ivi*, 2007, fasc. 113, pp. 187-241.

[42] In tal senso anche la Raccomandazione 17 giugno 2004, n. 195 dell'Organizzazione Internazionale del Lavoro (OIL) relativa alla formazione continua e allo sviluppo delle risorse umane, che promuove la definizione di misure in grado di favorire l'apprendimento permanente della popolazione e il rafforzamento dell'occupabilità. Si veda a tal proposito A. CARR, K. BALASUBRAMANIAN, R. ATIENO, J. ONYANGO, *Lifelong learning to empowerment: beyond formal education*, in *Distance Education*, 39(5), 2018, pp. 69-86.

[43] Con tale espressione ci si intende riferire al tema dell'apprendimento continuo, formale o informale, per tutto il corso della vita della popolazione.

[44] Cfr. L. CASANO, *Ripensare i Fondi Interprofessionali per la formazione continua: uno sguardo ai progetti di riforma francesi*, in *Bollettino Adapt*, n. 12, 26 marzo 2018, reperibile *online*.

ma anche un intervento congiunto sul sistema pensionistico e previdenziale che ha portato a un ripensamento complessivo delle misure assistenziali e occupazionali. In seguito all'introduzione della legge 17 agosto 2015, n. 994 e alla successiva attuazione con la legge 8 agosto 2016, n. 1088[45], il CPF è divenuto parte integrante del *Compte personnel d'activité* (CPA), ovvero un conto individuale ampio e multifunzionale per i cittadini francesi per gestire la propria posizione previdenziale ed esercitare in modo più autonomo i diritti maturati. In particolare, si è cercato di definire una piattaforma digitalizzata per il cittadino che includesse sia il sopramenzionato *Compte personnel de formation*, sia il *Compte professionnel de prévention* (C2P)[46] e il *Compte engagement citoyen* (CEC): da un lato, il C2P si è concentrato sui soggetti maggiormente esposti a fattori di rischio per la salute nell'ambito dei lavori usuranti, istituendo un sistema di capitalizzazione del credito volto ad ottenere dei benefici sul piano previdenziale; tra questi spiccano ad esempio la riduzione dell'orario di lavoro a parità di retribuzione, pensionamenti anticipati o l'attivazione di programmi formativi per poter aspirare ad attività lavorative meno usuranti. In questo modo, si è cercato di compensare l'onerosità e la pericolosità dei lavori assegnando «punti di difficoltà»[47] in proporzione all'intensità dei fattori di rischio.

Dall'altro, il CEC è stato progettato sia per coinvolgere i cittadini nel volontariato, sia per garantire ai disoccupati di intraprendere attività di servizio alla comunità per maturare dei crediti per il proprio CPF e finanziare così i percorsi di rinserimento lavorativo[48]. A questo proposito, è interessante notare la scelta adoperata nel preferire un arricchimento del conto personale mediante azioni di volontariato anziché consentire direttamente i versamenti monetari da parte dei beneficiari.

Pertanto, è possibile osservare come l'efficienza del CPF rispetto al DIF sia data dalla possibilità di contribuire a maturare del credito per la propria formazione professionale non solo mediante la consueta attività lavorativa, ma anche tramite lo svolgimento di attività di volontariato; tale formulazione permette infatti sia a chi si trova già in possesso di un impiego, sia ai soggetti in cerca di lavoro di poter incrementare il proprio conto.

---

[45] Per un approfondimento, si vedano S. D'AGOSTINO, S. VACCARO, *Nuove tutele per i lavoratori: il diritto soggettivo alla formazione Francia e Italia a confronto*, in *Professionalità studi*, 2020, vol. 3, p. 137 ss.; C. TOURRES, *Un "conto personale di attività" per il lavoratore del futuro: il caso francese*, in *Bollettino Adapt*, 25 gennaio 2016, reperibile *online*.

[46] Quest'ultimo è stato introdotto con *ordonnance* del 22 settembre 2017, n. 1389, che ha riformato il precedente *Compte personnel de prévention de la pénibilité* (C3P).

[47] Vengono stabilite delle soglie di pesantezza per determinare l'impatto dei lavori usuranti, svolgendo una valutazione in base all'intensità e al numero di fattori di rischio per la salute (pressione, temperature estreme, rumori, ecc.) e alla durata minima dell'esposizione (50-120 notti o 900 ore all'anno). In particolare, viene assegnato un punto ogni tre mesi di esposizione a fattore di rischio, stabilendo il limite complessivo del conto a 100 punti, ovvero venticinque anni di esposizione ai rischi professionali.

[48] In particolare, tale strumento permette di acquisire fino a 240 euro all'anno su un massimo di 720 euro complessivi impegnandosi in organizzazioni di volontariato riconosciute con finalità sociali (es. educative, scientifiche, umanitarie, sportive, familiari o culturali).

Tuttavia, è forse con le successive novità apportate dalla legge 5 settembre 2018, n. 771 «per la libertà di scegliere il proprio futuro professionale» che si è potuta riscontrare una maggiore fungibilità del CPF, avendo questa provveduto a riformare il sistema di maturazione del credito. In particolare, è stato sancito il passaggio dal sistema di capitalizzazione su base oraria a una monetaria, convertendo le ore del CPF in credito effettivo secondo un rapporto di 15 euro all'ora[49]. A questo cambiamento ha fatto inoltre seguito un'ampia campagna di promozione del sistema dei conti nel 2019, che ha cercato di incentivare una gestione autonoma da parte dei cittadini mediante la creazione della c.d. applicazione «*Mon Compte Formation*»[50]. In questo modo, è stata data la possibilità di consultare con maggiore facilità sia i crediti maturati per ogni conto personale, sia il catalogo degli enti abilitati dal Ministero del lavoro francese all'erogazione della formazione continua.

A questo proposito, è opportuno sottolineare come il processo di digitalizzazione del CPA e il lancio di una specifica applicazione abbiano portato non solo ad un rapido aumento degli utenti, ma anche a una massiccia attivazione dei corsi[51]. In merito a questi ultimi, occorre altresì menzionare come la riforma del sistema di maturazione del credito e la promozione della piattaforma digitale unica per i conti abbiano portato a una riduzione del costo medio dei servizi da 2.370 euro a 1.200, incentivando così l'aumento della competitività tra gli enti di formazione. Tale riforma, dunque, si è prefissata, da un lato, di riformare il tema della formazione continua per adeguarla ad un mercato del lavoro sempre più frammentato e, dall'altro, di rivedere le tutele e i meccanismi di protezione sociale in un'ottica di maggiore autodeterminazione. Dunque, sebbene il CPA possa rischiare di apparire come un tentativo di minare parte del sistema di protezione sociale a causa dell'introduzione di un sistema fondato sulla capitalizzazione del credito, questo può essere comunque considerato come un notevole passo avanti verso l'estensione delle politiche di apprendimento permanente a tutta la popolazione.

Infatti, la graduale semplificazione delle complesse modalità di accesso e utilizzo del sistema ha permesso di accrescere la responsabilità dei singoli cittadini nella gestione autonoma del proprio percorso professionale. A questo proposito, è significativo notare come il legame tra formazione continua e individuo sia cambiato dal 2004 al 2019, passando da un diritto al contratto di lavoro a un'attribuzione personale della persona. In

[49] In particolare, i lavoratori possono maturare annualmente fino a 500 euro di credito per un totale complessivo di 5.000 euro. Tale importo viene inoltre elevato fino a 800 euro all'anno per un totale di 8000 euro per i beneficiari con disabilità o basso livello di qualificazione.

[50] L. CASANO, *Il governo francese lancia Moncompteformation: il diritto alla formazione, su piattaforma*, in *Bollettino Adapt*, n. 42, 25 novembre 2019, reperibile *online*.

[51] Dal 21 novembre 2019, il Ministero del lavoro ha registrato una media di 25.000 *download* al giorno dell'applicazione (600.000 dopo il primo mese) e la validazione di oltre 32.000 corsi di formazione (lingue, patente di guida, certificazione delle competenze, assistenza all'imprenditoria, ecc.). Già in precedenza era stato inoltre rilevato dal Ministero del lavoro francese come il numero di CPF creati fosse aumentato dai 2.496.809 nel 2015 alle 5.468.534 unità circa del 2018. Cfr. MINISTÈRE DU TRAVAIL DE LA RÉPUBLIQUE FRANÇAISE, *Lancement de MonCompteFormation*, press dossier, 21 novembre 2019.

tale prospettiva, il sistema dei conti personali di apprendimento sembra potersi porre come un modello innovativo per promuovere le politiche occupazionali e formative all'interno dell'Unione europea, soprattutto per quei paesi che ancora non dispongono di strumenti adeguati a garantire l'apprendimento continuo della popolazione.

4. Osservazioni conclusive.

Alla luce dei cambiamenti che il fenomeno della digitalizzazione sta apportando soprattutto sul piano socioeconomico, appare chiaro che anche il mondo del lavoro finisca inevitabilmente per confrontarsi sempre più con le nuove sfide dell'era digitale, come il tema dell'accrescimento continuo delle competenze professionali della popolazione in età lavorativa. Se infatti la graduale implementazione della transizione digitale europea ha contribuito a rendere più efficienti i modelli produttivi e organizzativi delle impese grazie alle nuove tecnologie disponibili, è altrettanto vero che negli anni un simile progresso ha cambiato radicalmente la domanda di professionalità e il tipo di mansioni richieste alla forza lavoro[52]. Ciò può essere ad esempio riscontrato nella maggiore predilezione per i soggetti contraddistinti da forti abilità cognitive e autonomia decisionale, dal momento che, come sottolineato in precedenza, questi risultano in grado di adattarsi meglio ai cambiamenti e permettono alle imprese di adottare più velocemente le nuove tecnologie.

Per questo motivo, risulta necessario che le politiche per lo sviluppo tecnologico procedano di pari passo con le strategie di *upskilling* e *reskilling*, andando ad interessare gradualmente tutta la popolazione europea. Si prospetta indispensabile accrescere la portata e l'efficacia delle misure di *lifelong learning* per promuovere un processo di apprendimento continuo dell'intera comunità[53]; del resto, l'evoluzione del tessuto sociale e produttivo derivante dal continuo progresso tecnologico rende necessaria una migliore adattabilità ai cambiamenti[54].

In tale ottica – essendo necessario che le politiche di riqualificazione e accrescimento delle competenze interessino tutta la popolazione, seppur con particolare attenzione alla fascia in età lavorativa – pare potersi affermare che il dispositivo francese del *Compte Personnel d'Activité* (CPA) costituisca un modello *best practice* da seguire per un rafforzamento complessivo della formazione professionale dell'Unione europea. Infatti, la sopramenzionata misura si è dimostrata in grado di coinvolgere un'ampia

[52] Si veda: M. BROLLO, *Tecnologie digitali e nuove professionalità*, in *Diritto delle Relazioni Industriali*, 2019, n. 2, pp. 468-491.

[53] Cfr. OECD, *Improving the Quality of Non-Formal Adult Learning: Learning from European Best Practices on Quality Assurance, Getting Skills Right*, Paris, 2021.

[54] Si pensi a tal proposito al crescente sviluppo dell'*e-government*, che sta portando la pubblica amministrazione ad erogare un numero sempre maggiore di servizi mediante il supporto della tecnologia TIC. Per poter sfruttare al meglio l'efficienza derivante dalla semplificazione burocratica e amministrativa non è sufficiente, infatti, il solo possesso di adeguate infrastrutture e piattaforme informatiche, ma risulta anche necessario che la popolazione sia in grado di utilizzare autonomamente tali servizi.

percentuale dei cittadini francesi mediante una struttura tale da prediligere la formazione dei lavoratori e dare al contempo la possibilità ai soggetti non in possesso di impiego di finanziare il proprio credito formativo mediante attività di volontariato e socialmente utili[55].

Viene dunque da chiedersi se le nuove strategie programmatiche che seguiranno, come la nuova Agenda europea delle competenze per la competitività sostenibile, l'equità sociale e la resilienza[56], andranno a contemplare la diffusione di simili strumenti per l'accrescimento professionale. Del resto, appare ormai chiaro come il sopramenzionato obiettivo dell'alfabetizzazione informatica e dell'accrescimento delle competenze professionali della popolazione non possa prescindere dalla definizione di un quadro normativo adeguato a sostenere misure di *upskilling* e *reskilling*[57]. La crescente e continua rilevanza della digitalizzazione all'interno delle politiche di sviluppo europee rende tra l'altro indispensabile dare una maggiore centralità al tema dell'apprendimento continuo non solo per favorire le transizioni occupazionali della forza lavoro nell'ottica dei c.d. «mercati transizionali del lavoro», ma anche per permettere alla popolazione di sfruttare i benefici della trasformazione digitale della società.

In tale prospettiva, appare senza dubbio incoraggiante la volontà della Commissione europea di lanciare dal 2021 un «Patto per le competenze» per favorire un clima cooperativo e di impegno comune tra imprese, lavoratori ed enti territoriali per lo sviluppo di un modello per le iniziative di *lifelong learning*[58]. Simili iniziative di accrescimento professionale confermano infatti l'impegno da parte della Commissione europea di rafforzare i sistemi di formazione e renderli adeguati alle nuove esigenze dettate dall'era della digitalizzazione, specialmente se affiancati da strategie programmatiche di ampia visione come il Piano d'azione per l'istruzione digitale (2021-2027)[59].

[55] V. *supra*, par. 3.

[56] COM(2020) 274 final del 1° luglio 2020. Tale iniziativa intende riprendere i principali obiettivi introdotti dall'Agenda delle Competenze del 2016 (COM(2016) 381 final del 10 giugno 2016), tenendo comunque in considerazione le altre recenti strategie per lo sviluppo digitale del tessuto socioeconomico, come la Strategia digitale europea e la Strategia industriale e per le piccole e medie imprese.

[57] Cfr. CEDEFOP, *Empowering adults through upskilling and reskilling pathways. Volume 1: adult population with potential for upskilling and reskilling*, Bruxelles, 2020, reference series, n. 112, reperibile *online*.

[58] Il Patto per le competenze si fonda inoltre sulla creazione dei *knowledge* e *networking hub*, ritenuti un mezzo indispensabile per costruire una solida rete per i servizi di orientamento professionale.

[59] Piano d'azione per l'istruzione digitale 2021-2027. Ripensare l'istruzione e la formazione per l'era digitale, COM(2020) 624 final del 30 settembre 2020.

ABSTRACT: Il presente contributo prende in considerazione il tema della professionalità della forza lavoro all'interno dell'attuale transizione digitale dell'Unione europea, soffermandosi in particolare sul ruolo che il rafforzamento delle competenze può assumere nelle politiche di sviluppo del tessuto socioeconomico. In tale prospettiva, si intende richiamare in chiave interdisciplinare ad alcune delle principali problematiche che, anche alla luce della recente situazione pandemica, ostacolano la piena implementazione del processo di digitalizzazione europeo, come l'analfabetismo informatico e l'aumento dello *skill mismatch*.

PAROLE CHIAVE: digitalizzazione, competenze professionali, analfabetismo informatico, disallineamento delle competenze, apprendimento continuo.

The importance of workforce skills in the European digital transition

ABSTRACT: This paper examines the issue of the professional skills of the workforce within the current digital transition of the European Union, focusing on the role that the enhancement of competences can play in the definition of socio-economic development policies. In this perspective, the essay intends to cover with an interdisciplinary approach some of the main issues that, also in the light of the recent pandemic situation, hinder the full implementation of the European digitisation process, such as computer illiteracy and the increase in skill mismatch.

KEYWORDS: digitalisation, professional skills, computer illiteracy, skill mismatch, lifelong learning