UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Sede di Milano

Dottorato di ricerca in Impresa, Lavoro, Istituzioni e Giustizia Penale

Ciclo XXXV

S.S.D. IUS/13

La regolamentazione delle piattaforme digitali nell'Unione europea: una prospettiva transnazionale

Coordinatore:

Ch.mo Prof. Gabrio Forti

Tesi di dottorato di:

Giulio Monga

N Matricola: 4913331

Anno Accademico 2021/2022

Sommario

Ringraziamenti

Questo lavoro non sarebbe stato possibile senza il supporto costante del Prof. Pietro Franzina, al quale sono molto grado per essere stato la mia guida e il mio maestro in questi anni intensi di dottorato.

Un grazie sincero a tutti i colleghi e collaboratori della cattedra di diritto internazionale privato – Caterina, Mariangela, Marco, Giorgio, Omar – con cui abbiamo condiviso diversi e importanti pezzi di strada assieme.

Grazie a tutti i colleghi della scuola Impresa, Lavoro, Istituzioni e Giustizia Penale, ai docenti, allo staff e agli studenti dell'Università Cattolica, senza i quali la mia esperienza di dottorato non sarebbe stata la stessa. Grazie a tutti i colleghi, i docenti e le persone incontrate per strada durante il mio percorso accademico.

In ultimo, ma non per importanza, grazie alla mia famiglia e a tutti quelli che mi hanno incoraggiato e supportato in questo complesso ma bellissimo viaggio.

Introduzione

Questa dissertazione tratta della regolamentazione delle piattaforme digitali nell'ordinamento giuridico dell'Unione europea e, in particolare, dei rapporti che legano le persone che la piattaforma ha posto in contatto fra loro e dei rapporti intercorrenti fra tali persone e il gestore della piattaforma in questione: rapporti, questi, inevitabilmente caratterizzati dal ricorrere di elementi di internazionalità, e come tali implicanti un'analisi condotta sul terreno del diritto internazionale privato.

La tematica sarà esaminata da una prospettiva che, per un verso, intende valorizzare la dimensione transnazionale della vita di relazione che si svolge all'interno delle piattaforme, data dall'attitudine di queste a imprimere un ordine a rapporti che trascendono i confini nazionali, e, per un altro verso, si propone di dar conto del potere regolatorio esercitato, nei fatti, dai gestori delle piattaforme stese.

La tesi che verrà difesa si fonda sull'idea per cui le piattaforme sono dotate di un caratteristico connotato «istituzionale», dato dal potere dei relativi gestori di conformare con proprie regole – siano esse di natura contrattuale o tecnica – la vita di relazione che si svolge all'interno delle piattaforme stesse, spesso addirittura garantendo l'osservanza di tali regole attraverso l'intervento di propri organi o articolazioni, senza che si renda necessario ricorrere ad organi statali. Le caratteristiche appena segnalate indicano la spiccata capacità delle piattaforme ad autoregolarsi, peraltro confermata, nei fatti, dalla effettiva rivendicazione da parte delle maggiori piattaforme digitali di estesi poteri regolatori, più o meno impermeabili, quanto meno nelle intenzioni dei gestori, alle determinazioni degli Stati.

Sulla base di queste premesse, si sosterrà l'idea per cui, allo scopo di regolamentare in maniera efficace i rapporti e le fattispecie afferenti alle piattaforme, sia necessario adattare le tradizionali norme di fonte pubblica alla richiamata dimensione istituzionale delle piattaforme, tenendo conto della capacità di autoregolamentazione delle stesse.

Ci si propone di dimostrare che la strada da percorrere implica un dialogo, se non una collaborazione, tra gli attori della regolamentazione pubblica e regolari privati. Tale collaborazione, beninteso, non significa per i regolatori pubblici – gli Stati, l'Unione europea – abdicare alle proprie funzioni di tutela di interessi generali della popolazione demandando *in toto* la regolamentazione delle piattaforme a soggetti privati. Al contrario, essa dovrebbe fondarsi su una mutua fiducia tra regolatore pubblico, regolatore privato ed utente, in cui ai primi rimarrebbe in capo la determinazione dei principi generali cui la regolamentazione privata dovrebbe sottostare, oltre che il ruolo di supervisori del rispetto di tali principi. Ruolo, quest'ultimo, rafforzato dalla capacità di irrogare sanzioni e di valersi di forza coercitiva, che aiutano a garantire la predominanza dei regolatori pubblici rispetto a quelli privati.

L'angolatura da cui si studierà il problema è, come detto, quella dell'ordinamento giuridico dell'Unione europea, sia dal punto di vista del diritto materiale che da quello del diritto internazionale privato. La scelta è motivata dalla presa d'atto per cui le piattaforme – così come, in generale, la rete internet – abbiano un'intrinseca natura transnazionale, che ha portato da tempo il legislatore dell'Unione (e della Comunità prima) ad occuparsi della disciplina delle stesse, nella consapevolezza che i soli interventi degli Stati membri non sarebbero stati sufficienti per regolare in maniera esaustiva il fenomeno.

L'indagine prenderà il via (Capitolo 1) dall'analisi delle piattaforme come fenomeno economico-sociale per poi soffermarsi sugli aspetti giuridici connessi

alle stesse. Vedremo, in particolare, che le piattaforme sono infrastrutture digitali che consentono a soggetti stabiliti in tutto il mondo di interagire, permettendo la costituzione di rapporti giuridici, spesso in tempo reale, e svolgendo un ruolo di creatori di «mercati a più parti». Queste caratteristiche rendono le piattaforme degli ambienti giuridici contraddistinti da una duplice dimensione. Una «dimensione verticale», costituita dai rapporti tra utenti e gestori delle piattaforme, ed una «dimensione orizzontale», rappresentata dai rapporti tra gli utenti. L'architettura giuridica su cui si basano tali ambienti sono innanzi tutto le regole – sia contrattuali che tecniche – determinate dai gestori, che disciplinano unilateralmente i rapporti relativi alla «dimensione verticale» e sono in grado di influenzare quelli afferenti alla «dimensione orizzontale». Vedremo come, nel tentativo di qualificare e regolare i rapporti in questione, la dottrina e la giurisprudenza non siano giunte a soluzioni univoche.

Svolto questo inquadramento, ci soffermeremo, nel Capitolo 2, sulle pertinenti disposizioni del diritto materiale dell'Unione europea. In primo luogo, ci si occuperà, quindi, della Direttiva 2000/31/CE («Direttiva e-Commerce») e dell'evoluzione che, sin dalla sua adozione, ha interessato il regime di responsabilità degli *internet service provider* per i contenuti e le informazioni illecite dei propri utenti. In particolare, con l'apporto della Corte di Giustizia dell'Unione europea, si è passati da un regime di pressoché totale irresponsabilità ad un regime in cui vengono individuati peculiari figure di «*hosting provider*» attivi che, al sussistere di alcuni «indici di interferenza», rispondono delle informazioni e dei contenuti diffusi dagli utenti, trattandosi di figure sostanzialmente diverse da quelle – passive – a cui il legislatore aveva principalmente pensato in sede di elaborazione della direttiva.

L'evoluzione descritta segnala la propensione dell'ordinamento dell'Unione a responsabilizzare i gestori delle piattaforme, facendo leva sulla loro capacità di autoregolamentazione. Tale tendenza ha trovato riscontro in strumenti più recenti come il Regolamento UE 2019/1150 («Regolamento P2B») o la Direttiva UE 2019/790 («Direttiva Copyright»), in cui il legislatore dell'Unione ha proseguito nel percorso di responsabilizzazione dei *provider*, affidandosi inoltre ad essi, anche in qualità di regolatori che possono assumere funzioni «paragiurisdizionali», per il raggiungimento dei propri obiettivi. L'evoluzione in questione si è, inoltre, manifestata nel nuovo Digital Services Act europeo, entrato in vigore lo scorso 16 novembre 2022 ma che non sarà pienamente applicabile sino al 17 febbraio 2024.

Il capitolo si concluderà con l'analisi della giurisprudenza della Corte di Giustizia che, nel tentare di fornire una soluzione ai problemi qualificatori relativi ad alcune piattaforme digitali – segnatamente, Airbnb e Uber – ne ha di volta in volta indicato la natura di fornitori di servizi della società dell'informazione ovvero di fornitori dei servizi «sottostanti» offerti agli utenti della piattaforma stessa, raggiungendo sul punto conclusioni apparentemente discordanti. La problematica qualificatoria è rilevante ai nostri fini in quanto dalla soluzione della stessa discende l'applicabilità, o meno, ai *provider* di tali piattaforme di diversi strumenti legislativi al centro della nostra indagine, quali la Direttiva e-Commerce, il Regolamento P2B o lo stesso Digital Services Act.

Esaminati gli aspetti di diritto materiale, nel Capitolo 3 verrà svolta un'analisi relativa al funzionamento delle norme di diritto internazionale privato dell'Unione europea che hanno per oggetto rapporti giuridici e situazioni che nascono nell'ambito delle piattaforme digitali o risentono, ad altro titolo, delle dinamiche di queste ultime. L'indagine si riferirà sia ai rapporti afferenti alla dimensione «orizzontale» che a quelli relativi alla dimensione «verticale» della

vita di relazione interna alle piattaforme. Saranno, in particolare, prese in considerazione le pertinenti norme del Regolamento Bruxelles I*bis* sulla competenza giurisdizionale e il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, del Regolamento Roma I sulla legge applicabile alle obbligazioni contrattuali e del Regolamento Roma II sulla legge applicabile alle obbligazioni extracontrattuali, avendo a riguardo anche ai regimi da essi previsti a tutela delle parti deboli dei rapporti contrattuali, come consumatori e lavoratori.

L'esame di tali strumenti metterà in luce le difficoltà sottese all'applicazione di tali strumenti nel contesto delle piattaforme. Si tratta di difficoltà imputabili, oltre che ai problemi qualificatori discussi nel Capitolo 2, alle logiche «stato-centriche» e legate al concetto di territorialità su cui si fondano le norme di diritto internazionale privato dell'Unione, che mal si attagliano ad ambienti virtuali, come le piattaforme, in cui il potere regolatorio dei gestori esercita un'influenza significativa.

Dal tentativo di individuare eventuali nuovi paradigmi emerge la constatazione per cui la regolamentazione di fonte diversa da quella statale – ed in particolare quella privata – abbia tuttora uno spazio assai limitato nel diritto internazionale privato dell'Unione. Si rileva, al contrario, una duplice tendenza. Una giurisprudenziale, rappresentata dal tentativo di adattare le tradizionali norme di diritto positivo al mondo virtuale, individuando *ex novo* o mutuando criteri di collegamento utilizzati per altre situazioni. Una legislativa, costituita del proliferare di norme di chiara matrice «unilateralista» (come il GDPR, il Regolamento P2B o lo stesso Digital Services Act), che determinano autonomamente il proprio ambito di applicazione territoriale, oltre che materiale, prescindendo dall'applicazione delle norme di conflitto.

Queste tendenze segnalano la volontà dei regolatori pubblici di mantenere il controllo sulla rete nonostante il crescente potere regolatorio dei soggetti privati – tra cui i gestori delle piattaforme – attivi sulla stessa. Di più, l'utilizzo sempre più frequente di norme unilateraliste – rintracciabili sia nell'Unione che in altri contesti geografici e giuridici – pare rispondere al tentativo dei regolatori pubblici di estendere la propria sovranità sulla rete, proponendosi di disciplinare situazioni con un legame *prima facie* minimo con i rispettivi ordinamenti. Il rischio principale di questa impostazione è rappresentato dal «*regulatory overreaching*», fenomeno proprio di norme che, pur configurando un'applicazione (extra)territoriale assai estesa, hanno in realtà poche possibilità di applicazione reale alle fattispecie che si propongono di disciplinare. Nell'ambito delle piattaforme digitali, peraltro, il fenomeno è acuito dalla constatazione per cui gli Stati abbiano un bisogno strutturale della cooperazione delle piattaforme stesse per ottenere l'effettiva applicazione delle proprie norme online. Circostanza che, come vedremo, è già emersa sia nella giurisprudenza dell'Unione che in quella nordamericana.

A valle dell'esame delle pertinenti norme dell'Unione, nel Capitolo 4 ci si occuperà più da vicino del rapporto tra regolamentazione privata e pubblica nell'ambito delle piattaforme digitali. In particolare, dopo aver introdotto i concetti di *private regulation* e *lex informatica* si avrà modo di constatare come la dottrina tradizionale sia perlopiù poco propensa a conferire rilevanza a tali categorie nell'ambito del diritto internazionale privato, rimanendo viceversa legata ad un'impostazione giuspositivista.

Nonostante ciò, da un'analisi delle recenti tendenze si ricava come la dimensione istituzionale ed il potere regolatorio delle piattaforme digitali siano presi in considerazione dal legislatore dell'Unione nel definire le strategie normative in materia, senza peraltro che ciò si traduca in una assimilazione di

quest'ultimo alla potestà degli Stati. Vedremo, in particolare, che la Commissione europea ha individuato tre differenti approcci: la regolamentazione tradizionale attraverso il diritto di fonte pubblica («*top-down legislation*»), la valorizzazione dell'autoregolamentazione delle piattaforme e la promozione di strumenti e meccanismi di coregolamentazione.

Gli input della Commissione europea si sono tradotti in recenti strumenti normativi – sia di *top-down legislation* che di coregolamentazione – in cui, oltre alla già segnalata svolta unilateralista si scorge, dal punto di vista sostanziale, il tentativo del legislatore dell'Unione di controllare la dimensione istituzionale delle piattaforme attraverso la valorizzazione dei principi di «*accountability*» e trasparenza, anche grazie all'utilizzo e alla promozione di strumenti di *private regulation* quali i codici di condotta. È il caso, ancora una volta, del GDPR e del Regolamento P2B, in cui la funzione regolatoria e para-giurisdizionale delle piattaforme assume un'importanza decisiva. Centrale è, inoltre, il ruolo di strumenti come le sanzioni pecuniarie, che svolgono anche una funzione denominata in dottrina come «*market destroying measure*».

Il Capitolo 5 contiene un approfondimento dedicato ai rapporti tra regolamentazione pubblica e privata ai fini del contrasto alla diffusione di contenuti illeciti sulle piattaforme di *social network*. L'attenzione dedicata al tema è giustificata dalla presa d'atto del ruolo decisivo dei gestori delle piattaforme a riguardo, sia dal punto di vista tecnico che da quello regolatorio. I gestori delle piattaforme, infatti, sono per molti aspetti i soggetti nella posizione migliore per scovare e rimuovere i contenuti illegali. Tale attività, oltre ad essere necessaria per adeguarsi alle prescrizioni del diritto di fonte pubblica, costituisce spesso anche applicazione delle regole e *policy* di condotta di fonte privata determinate dagli stessi gestori, le quali, peraltro, potrebbero in alcuni casi contrastare con le stesse norme stabilite dai regolatori pubblici.

Per evidenziare la centralità del ruolo delle piattaforme, sarà svolta un'analisi del Facebook Oversight Board, l'organo indipendente costituito da Facebook allo scopo di gestire i reclami e le segnalazioni degli utenti del popolare *social network* relative ai contenuti in violazione delle regole dello stesso. L'Oversight Board costituisce, ad oggi, l'esempio più avanzato di autoregolamentazione di una piattaforma digitale. A sostegno di questa affermazione, il fatto che la composizione e il funzionamento dello stesso siano disciplinati da un apposito Atto Costitutivo («Oversight Board Charter») dal carattere «simil-costituzionale», che conferisce al Board il potere di interpretare le norme della *community* di Facebook e di emettere decisioni vincolanti per quest'ultimo.

I ragionamenti svolti in questo capitolo saranno atti a dimostrare come la rilevanza del ruolo delle piattaforme renda inevitabile, per i regolatori pubblici, stabilire una forma di collaborazione con i gestori delle stesse allo scopo di garantire l'applicazione delle proprie regole in materia di «contenuti illeciti» all'interno degli ambienti virtuali. Questa collaborazione – che, all'interno dell'Unione, ha assunto le sembianze di vari strumenti di coregolamentazione, come i codici di condotta – non significa, peraltro, una rinuncia dei regolatori pubblici a disciplinare quanto avviene nelle piattaforme a favore dei regolatori privati. Ai primi, infatti, spetta comunque la definizione dei principi fondamentali attraverso cui orientare e limitare il potere regolatorio dei soggetti privati allo scopo di raggiungere i propri obiettivi.

A questo proposito, peraltro, si evidenzierà come anche i gestori delle piattaforme sembrino riconoscere la prevalenza dei regolatori pubblici. Significativo, in questo senso, la circostanza per cui l'Atto Costitutivo del Facebook Oversight Board riconosca a più riprese il limite del diritto di fonte pubblica sia per il Board che per il *social network*. Come vedremo, infatti, essa stabilisce il divieto di eseguire decisioni del Board o di interpretare l'Atto Costitutivo in modo da portare a violazioni di legge. Importante è, inoltre, la specifica per

cui il Board non abbia la pretesa di «*enforce local law*», con ciò escludendo qualsiasi velleità di assimilazione ad un organo giurisdizionale di tipo statale.

Il sesto ed ultimo capitolo è dedicato al Digital Services Act, il già citato nuovo regolamento sui servizi digitali entrato in vigore nell'autunno 2022. L'analisi di questo strumento è rilevante in quanto lo stesso, piuttosto che costituire di per sé una rivoluzione, sviluppa ulteriormente le tendenze relative alle strategie regolatorie dell'Unione europea in materia di piattaforme digitali esaminate nel corso del presente lavoro, contribuendo a rafforzare le evidenze da noi raccolte. Ciò sia dal punto di vista del diritto materiale che di quello internazionalprivatista, oltre che per quanto riguarda il rapporto tra regolamentazione di fonte pubblica e di fonte privata.

Per quanto riguarda gli aspetti internazionalprivatisti, anche in questo regolamento viene fatto ricorso al metodo unilateralista allo scopo di determinarne l'ambito di applicazione, sia materiale che territoriale, prescindendo dalle norme di conflitto. Anche in questo caso, peraltro, il ricorso a questo metodo appare suscettibile di estendere in maniera piuttosto significativa la gittata del nuovo strumento, dando luogo a rischi di «*regulatory overreaching*» comunque mitigati dallo stesso regolamento.

Dal punto di vista del diritto materiale, il Digital Services Act, in primo luogo, interviene sulla disciplina relativa alla responsabilità degli *internet service provider* analizzata nel Capitolo 2. In particolare, il regolamento, pur mantenendo fermi i principi fondamentali della Direttiva e-Commerce, prosegue nel percorso di responsabilizzazione dei fornitori positivizzando le indicazioni della Corte di Giustizia sulla figura dell'*hosting provider* attivo e restringendo l'area di esenzione dalla responsabilità dei fornitori per i contenuti forniti dai propri utenti.

I medesimi obiettivi di responsabilizzazione sono alla base dell'articolato regime sui doveri di diligenza degli stessi previsto dal Digital Services Act. Questo regime, come vedremo, si caratterizza per l'adozione di un approccio «a strati», in quanto pone obblighi via via più stringenti a seconda delle diverse categorie di fornitori di servizi considerate, tra cui compaiono anche i fornitori di servizi di piattaforme online, che trovano quindi una prima definizione all'interno dell'ordinamento giuridico dell'Unione.

Le norme sui doveri di diligenza rispecchiano in gran parte le tendenze emerse nel corso della nostra indagine, in quanto si fondano sui principi della trasparenza e dell'*accountability* dei *provide*r, in capo ai quali sono posti doveri sempre più penetranti per garantire la sicurezza del mondo digitale e contrastare la diffusione di contenuti illegali. Centrale è, inoltre, la valorizzazione del potere regolatorio degli stessi fornitori e della dimensione istituzionale degli ambienti da questi gestiti, anche attraverso la promozione di strumenti di autoregolamentazione e di coregolamentazione, come i codici di condotta. Significative, a questo proposito, le disposizioni relative agli obblighi di conformazione dei «termini e condizioni» dei fornitori e quelle che, riconoscendone il potere regolatorio, impongono agli *hosting provider* di prevedere dei meccanismi di segnalazione e rimozione dei contenuti illegali da parte degli utenti («*notice and action*»), con il dovere di motivare l'eventuale rimozione dei contenuti in questione. Per i fornitori delle piattaforme, a questi obblighi si affianca quello di stabilire dei sistemi effettivi di gestione dei reclami, attraverso cui gli utenti possano impugnare le decisioni assunte a seguito della condivisione di contenuti illegali o incompatibili con i «termini e condizioni».

A queste norme segue un composito regime dedicato all'attuazione del Digital Services Act da parte delle autorità nazionali competenti («*digital enforce-*

ment»), in cui rivestono un'importanza centrale le sanzioni amministrative pecuniarie, analogamente a quanto accade nell'ambito di altri strumenti esaminati nel corso del presente lavoro, come il GDPR.

L'illustrazione del Digital Services Act è funzionale alla formulazione delle nostre conclusioni. In particolare, dalle indagini svolte emerge come la disciplina delle piattaforme digitali non possa prescindere da una collaborazione tra regolatori pubblici e privati.

Questo vale innanzi tutto per il diritto materiale, ove si rileva la tendenza del legislatore a valorizzare il potere regolatorio e para-giurisdizionale delle piattaforme, cercando di orientarlo al rispetto delle proprie regole grazie a meccanismi di «*accountability*» e trasparenza.

Da un punto di vista internazionalprivatistico, invece, le difficoltà segnalate nelle pagine precedenti ed il proliferare di norme di matrice unilateralista dimostrano la parziale inadeguatezza delle regole esistenti. Esse dimostrano altresì l'emergere di nuovi paradigmi che, pur rimanendo nel solco della tradizionale impostazione giuspositivista, indicano un deciso cambio di rotta. Una svolta che rischia, in certi casi, di dar vita al «*regulatory overreaching*». Per evitare questo fenomeno, lo strumento principe cui il legislatore fa ricorso restano le sanzioni pecuniarie e la conseguente applicazione attraverso l'uso di poteri coercitivi, su cui gli Stati continuano ad esercitare il monopolio.

Le evidenze emerse dall'indagine indicano, pertanto, che l'Unione «vede» il fenomeno della *private regulation* nell'ambito delle piattaforme digitali e ingaggia con esso un dialogo, riconoscendo in tal modo l'effettività di quel fenomeno e le sue potenzialità «positive». Questo dialogo, tuttavia, non è concepito dal legislatore come un dialogo fra pari. Al contrario, l'Unione non rinuncia a regolare (o quanto meno a «orientare») la vita di relazione che si svolge sulle piattaforme, senza effettuare deleghe in bianco a favore dei gestori privati ma

cercando, piuttosto, di orientarne l'attività regolatoria, valorizzando la dimensione istituzionale degli ambienti da essi gestiti.

Capitolo 1 – Le piattaforme digitali e il diritto

SOMMARIO: 1 Le piattaforme digitali come fenomeno economico e sociale. – 2 I problemi qualificatori e regolatori sottesi all'utilizzo delle piattaforme digitali. –2.1 I rapporti giuridici che popolano le piattaforme digitali: tra dimensione «verticale» e dimensione «orizzontale». – 2.2 La dimensione istituzionale delle piattaforme: attori e procedimenti. – 2.3 L'importanza della tecnologia nell'autoregolamentazione delle piattaforme. – 3 Criticità legate all'impiego delle regole di diritto internazionale privato nell'ambito delle piattaforme e bisogno di nuovi paradigmi. – 4 Le angolature da cui si studierà il problema. – 5 La tesi: il carattere istituzionale delle piattaforme e l'inevitabile cooperazione tra attori pubblici e privati per la regolamentazione delle stesse.

1 Le piattaforme digitali come fenomeno economico e sociale

Le piattaforme digitali costituiscono uno dei maggiori protagonisti dell'economia e della società del ventunesimo secolo.

Per fornire alcuni numeri a sostegno di tale affermazione si pensi che, secondo il report[1] globale annuale del 2021 sull'utilizzo di Internet, social media, dispositivi mobili e mercato *e-commerce*, pubblicato dal portale *We Are Social* in collaborazione con la società canadese Hootsuite Inc, nel 2020 risultava che gli utenti di Internet si attestassero sui 4.66 miliardi. Di questi, ben 4.20 miliardi – ossia il 13% in più rispetto ai numeri del 2019 – risultavano presenti sulle piattaforme di social media.

Sempre secondo il menzionato report, il tempo speso sulle piattaforme social si è attestato, nel 2020, su due ore e venticinque minuti al giorno, pari a circa

[1] Digital 2021 Global Overview Report, pubblicato il 27 gennaio 2021 e consultabile al seguente link: https://datareportal.com/reports/digital-2021-global-overview-report

un'intera giornata lavorativa alla settimana. Le previsioni, per il 2021, parlavano di oltre 420 milioni di anni spesi collettivamente dall'umanità su tali piattaforme.

Significativi ed eloquenti sono anche i dati economici. In particolare, nel 2020 si stima che il volume di affari dei canali *e-commerce* abbia toccato i 665.6 miliardi di dollari in tutto il mondo, soltanto per quanto riguarda il settore della moda[2].

Allo stesso modo, forniscono un'idea della dimensione epocale del fenomeno i dati relativi all'utilizzo dei *social network* come strumento per informarsi. Soltanto in Italia, ad esempio, stando ai dati forniti dal sedicesimo rapporto annuale Censis sulla comunicazione, il 31,4% della popolazione italiana utilizza Facebook come principale mezzo d'informazione[3]. Ancora, si consideri che nel 2020 – anno di elezioni presidenziali e di pandemia – le stime del portale *Statista* riferiscono di 2.84 miliardi di dollari spesi per annunci di carattere politico sulle piattaforme di social media nei soli Stati Uniti d'America[4].

Si potrebbe proseguire a lungo con i numeri che segnalano l'importanza delle piattaforme digitali nella società contemporanea ma non è questa la sede per farlo, così come non è questa la sede per analizzare in maniera approfondita i

[2] Idem. Lo stesso report, peraltro, non prende in considerazione solo il settore della moda ma fornisce dati anche per quanto riguarda i seguenti settori: turismo e viaggi (593.6 miliardi), elettronica (501.8 miliardi), cibo e cura personali (413.8 miliardi), articoli per la casa (330.9 miliardi), giocattoli, fai da te e tempo libero (525.6 miliardi), musica digitale (21.73 miliardi), videogiochi (135.8 miliardi)

[3] Il report in questione è liberamente consultabile al seguente indirizzo: https://www.censis.it/comunicazione/16%C2%B0-rapporto-censis-sulla-comunicazione-0

[4] Dato consultabile al seguente indirizzo: https://www.statista.com/topics/3723/social-media-and-politics-in-the-united-states/

vari modelli economici alla base del successo delle piattaforme[5]. Ci si concentrerà qui invece sulla natura economico-sociale del fenomeno, per poi addentrarsi sulle problematiche regolatorie connesse allo stesso.

A tal proposito, è bene partire da una semplice definizione fornita dagli studiosi delle scienze economiche, a mente della quale le piattaforme sono «infrastrutture digitali che consentono a due o più gruppi di interagire[6]». Tale definizione si concentra su quella che è l'essenza primaria delle piattaforme, ossia la capacità di permettere l'interazione tra utenti nel mondo digitale.

Nell'ambito di una piattaforma, peraltro, l'interazione degli utenti può avere varie finalità, tanto economiche quanto sociali. Questo aspetto è stato valorizzato anche da una definizione fornita dalla Commissione Tedesca per i Monopoli che, ponendo enfasi sul ruolo di intermediari dei gestori, ha descritto le piattaforme come «intermediari che riuniscono vari gruppi di utenti in modo che questi possano interagire socialmente o economicamente[7]».

Sulla stessa scia si colloca anche la definizione data dalla Commissione europea, secondo cui: «Online platforms can be described as software-based facilities offering two-or even multi-sided markets where providers and users of

---

[5] Per approfondire il fenomeno da un punto di vista economico e per consultare informazioni statistiche ufficiale è utile consultare il documento di lavoro: Commission Staff Working Document, *Online Platforms – Accompanying the document Communication on Online Platforms and the Digital Single Market*, SWD(2016) 172 final, 25 maggio 2016, che accompagna la Comunicazione della Commissione europea COM(2016) 288 final.

[6] N. SRNICEK, *Platform Capitalism*, Polity Press, 2016, p. 43. V. in particolare il passaggio in una piattaforma digitale è definita come «a digital infrastructure that enables two or more groups to interact».

[7] Si veda in particolare la *Written evidence from Monopolkommission (OPL0046)* resa dalla Monopolkommission tedesca nell'ambito delle audizioni organizzate dalla House of Lords britannica in vista del report: House of Lords, *Select Committee on European Union*, 10th Report of Session 2015–16, *Online Platforms and the Digital Single Market*, HL Paper 129.
La testimonianza è consultabile qui:
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/written/23265.html.

content, goods and services can meet[8]». La Commissione Europea, peraltro, si spinge oltre nella valorizzazione della funzione economica delle piattaforme, sottolineandone il ruolo di creatori di mercati a più parti in cui fornitori ed utenti possono incontrarsi per scambiare beni e servizi.

Il carattere distintivo delle piattaforme rispetto altri mezzi di comunicazione (es. posta cartacea, telefono, fax e persino e-mail) sta nel fatto che mentre questi ultimi si limitano a mettere in contatto due o più soggetti, le piattaforme digitali costituiscono anche il luogo, seppur dematerializzato, in cui gli utenti interagiscono e realizzano attività che hanno rilevanza non solo economica ma anche sociale e giuridica.

Ogni giorno, infatti, acquistando merci su Amazon, scaricando film da Netflix, postando commenti o immagini su Facebook o ordinando cibo su Glovo, migliaia di utenti in tutto il mondo costituiscono rapporti giuridico-economici e stabiliscono relazioni sociali che si estrinsecano, in tutto o in parte, nell'ambito delle piattaforme stesse. In questo senso, le piattaforme digitali rappresentano dei veri e propri ambienti economici e sociali, in cui si svolge una parte sempre più consistente delle attività umane[9].

Negli ultimi decenni lo sviluppo e la crescita delle piattaforme digitali sono stati poderosi ed hanno interessato molteplici ambiti della vita sociale e settori economici. Si pensi, per riprendere gli esempi svolti in precedenza, all'impor-

---

[8] EU Commission Staff Working Document, *A Digital Single Market Strategy for Europe - Analysis and Evidence; Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe*, SWD(2015) 100 final, v. in particolare a p. 52. Accessibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100.

[9] V. ad esempio T. RODRÍGUEZ DE LAS HERAS BALLELL, *Rules for a Platform Economy: A Case for Harmonisation to Counter "Platform Shopping" in the Digital Economy*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 55-80, Schulthess, 2018

tanza assunta dai *social network* nel dibattito politico, alla crescita dell'*e-commerce*, così come al ruolo sempre più importante di piattaforme come Google Maps o Uber in settori cruciali come la mobilità.

Il successo delle piattaforme – sia come modello economico[10] che come luogo dematerializzato di aggregazione sociale, diffusione di informazioni o sviluppo del dibattito politico – viene spiegato da alcuni autori[11] prendendo in considerazione due elementi.

Il primo di essi attiene alla notevole capacità delle piattaforme di far incontrare la volontà delle parti in maniera agevole ed istantanea, a prescindere dal luogo fisico in cui queste si trovano. Il secondo riguarda invece la reputazione e la fiducia di cui le stesse piattaforme – e di conseguenza i loro gestori – godono. Fiducia e reputazione che sono proprio il motore che alimenta costantemente le piattaforme e che spingono gli utenti ad avvalersene per costituire rapporti giuridici ed economici, o comunque per svolgere attività socialmente rilevanti[12].

2 I problemi qualificatori e regolatori sottesi all'utilizzo delle piattaforme digitali

Come detto, gli utenti delle piattaforme compiono ogni giorno attività giuridicamente rilevanti: dall'acquisto di beni, al *download* di film o canzoni sino alla condivisione di commenti o contenuti. Le attività in questione implicano la costituzione di rapporti di diritto privato e conferiscono alle piattaforme le

[10] Idem, p. 55. In particolare, l'autrice definisce le piattaforme come il modello architettonico principale dell'economia digitale contemporanea e il modello organizzativo dominante per le attività economiche, i *social network* e il *business* emergente nella scena digitale contemporanea.
[11] I. PRETELLI, *The Economic Rise of Digital Platforms' Business Models and its Impact in the Conflict of Laws*, in in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 17-53, Schulthess, 2018.
[12] Idem, p. 19.

vesti, oltre che di ambienti economici e sociali, di ambienti giuridici, che pertanto abbisognano di regole per disciplinare quanto avviene su di essi.

Nell'ottica del diritto privato, in particolare, due sono le dimensioni rilevanti delle piattaforme digitali. Vi è una dimensione statica, che attiene alla funzione di «cornice» assolta dalle piattaforme in quanto tali, e una dimensione dinamica, che attiene ai rapporti contrattuali che vengono conclusi (e spesso eseguiti) all'interno di quella cornice, nonché agli illeciti che possono essere commessi nel medesimo ambito.

L'applicazione delle norme di diritto privato ai rapporti che si svolgono nel quadro di una piattaforma ne presuppone la qualificazione, cioè la sussunzione sotto le categorie di cui si servono le norme privatistiche per leggere i fenomeni che le stesse si propongono di disciplinare. Tanto la dottrina quanto la giurisprudenza non sono tuttavia pervenute al riguardo a soluzioni univoche consolidate[13]. Ciò provoca numerose incertezze dal punto di vista regolatorio che, come vedremo, sono peraltro acuite dal carattere intrinsecamente transnazionale delle piattaforme e riguardano anche profili di diritto internazionale privato.

I richiamati problemi qualificatori derivano del fatto che le piattaforme digitali, per via dei profili di novità che presentano rispetto ad altre forme di intermediazione, non sembrano lasciarsi accostare pacificamente alle figure giuridiche che vengono in gioco nel mondo non digitale.

[13] A questo proposito v. *ex multis* T. RODRÍGUEZ DE LAS HERAS BALLELL, *op. cit*. 9, pag. 63. In questo passaggio l'autrice, in particolare, rileva come permangano molte incertezze in merito alla natura giuridica delle piattaforme ed al ruolo dei gestori, nonostante che: «*the concept of a platform is well-described in technological terms and is widely understood as a business model*»; v. anche G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in Rivista trimestrale di diritto e procedura civile, Vol. 72, n. 2, pp. 411-440, 2018.

Come avremo modo di vedere meglio in seguito[14], nella giurisprudenza della Corte di Giustizia dell'Unione europea i gestori di piattaforme sono stati considerati, a vari fini, come dei fornitori di servizi (motivo per cui nel prosieguo ci si riferirà agli stessi anche con espressioni come «fornitori», «prestatori di servizi», «*provider*», mutuate dal linguaggio del diritto dell'Unione). Tale accostamento, tuttavia, non fornisce risposte soddisfacenti in merito alla natura degli ambienti da essi gestiti e non permette di ricavare un paradigma generale. Il gestore di una piattaforma, come si vedrà meglio in seguito, infatti, non si limita a mettere in contatto due o più soggetti, ma fissa anche standard tecnici e regole di condotta che finiscono col dar vita ad un ambiente sociale particolare, dotato di regole di funzionamento proprie.

In dottrina, vi è chi ha tentato di accostare le piattaforme alle realtà di cui si occupano le norme concernenti gli enti a carattere associativo, come le associazioni e le fondazioni. Alcuni autori hanno persino ipotizzato che le piattaforme segnalerebbero l'esistenza di un nuovo tipo di entità giuridica diverso sia dalle persone fisiche che dalle persone giuridiche, portando al conio del neologismo «persone digitali[15]».

---

[14] Rinviando per approfondimenti più specifici al Capitolo 2, ed in particolare al par. 4, si citano a tal proposito sin da ora le seguenti pronunce della Corte di Giustizia dell'Unione Europea, in cui i gestori delle piattaforme sono stati considerati, a vari fini, come dei fornitori di servizi: CGUE, C-434/15, *Asociación Profesional Élite Taxi* c. *Uber Systems Spain SL*, 20 dicembre 2017; CGUE, C-320/16, *Uber France SAS* c. *Nabil Bensalem*, 10 aprile 2018. Diversa la qualificazione fornita della stessa Corte UE nella sentenza *L'Oréal* c. *Ebay*, in cui la Corte ha invece posto enfasi sul ruolo, assunto dal gestore, di «prestatore intermediario di servizi della società dell'informazione» ai sensi degli artt. 12-15 della Direttiva 2000/31/CE (cfr. CGUE, C- 324/09, *L'Oréal SA e altri* c. *eBay International AG e altri*, 12 luglio 2011). Sulla stessa scia di questa ultima pronuncia, ribaltando quanto affermato nei due casi relativi ad Uber, si è collocata la Corte nel caso *Airbnb Ireland*, in cui la piattaforma è stata considerata un prestatore di un «servizio della società dell'informazione» ai sensi dell'art. 2, lett. a) della Direttiva 2001/31/CE (cfr. CGUE, C-390/18, *Airbnb Ireland*, 19 dicembre 2019).

[15] V. a questo proposito: I. PRETELLI, *op. cit.* 11, p. 45; L. AMMANNATI, *Verso un diritto delle piattaforme digitali?*, in federalismi.it, n° 7/2019, p. 16. Disponibile online al seguente link: https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=38331&content=&content_author=

2.1 I rapporti giuridici che popolano le piattaforme digitali: tra dimensione «verticale» e dimensione «orizzontale»

Approcciandosi alle questioni poc'anzi rilevate, occorre innanzi tutto muovere dall'analisi dei rapporti giuridici che si costituiscono nell'ambito delle piattaforme digitali.

A tal riguardo, va in primo luogo evidenziato come tali rapporti possano avere tanto il carattere della stabilità (es. l'iscrizione ad un *social network*, la sottoscrizione di un abbonamento ad una piattaforma per l'ascolto della musica in *streaming*) quanto quello dell'istantaneità (ad esempio l'acquisto di un bene di consumo su una piattaforma *e-commerce*).

I predetti rapporti presentano una duplice dimensione anche dal punto di vista soggettivo-relazionale[16]. Da una parte, infatti, vi è una dimensione «verticale» rappresentata dalle relazioni stabilite tra gli utenti ed i gestori delle piattaforme (es. il contratto che lega un utente a Facebook) mentre dall'altra va presa in considerazione una dimensione «orizzontale», che attiene ai rapporti che possono stabilirsi tra gli utenti stessi grazie all'intermediazione della piattaforma (è il caso, ad esempio, della vendita di prodotti *online* da parte di imprese o persone fisiche). L'analisi di tale duplice dimensione è necessaria per indagare al meglio il fenomeno delle piattaforme dal punto di vista giuridico.

La dimensione verticale trova, generalmente, il proprio elemento costitutivo in un contratto. Nell'ambito di una piattaforma, infatti, ciascun utente conclude di norma un accordo di tipo contrattuale con il gestore della piattaforma

[16] T. RODRÍGUEZ DE LAS HERAS BALLELL, *op. cit*. 9, p. 64.

stessa (es. di abbonamento o, più comunemente, di iscrizione ad una piattaforma[17]). L'accordo in questione – in genere rappresentato dai «termini e condizioni» o dalle «condizioni generali» della piattaforma – costituisce anche la fonte del rapporto giuridico tra l'utente e il gestore della piattaforma e disciplina i rispettivi obblighi e diritti delle parti.

Tramite detto accordo il gestore definisce, delimita e stabilisce le condizioni che regolano le proprie attività ed il proprio ruolo di fornitore di servizi (ad esempio motori di ricerca, sistemi di pagamento) ma anche, come vedremo meglio in seguito, di regolatore privato e di supervisore dell'applicazione delle regole da esso stesso stabilite. L'accordo di cui si discorre, oltre che regolare i rapporti tra utente e gestore, è quindi ciò che conforma, da un punto di vista giuridico, l'architettura e l'organizzazione delle piattaforme digitali.

La dimensione orizzontale attiene invece alle interazioni tra i singoli utenti delle piattaforme. Gli utenti, come detto, interagiscono tra di loro in vari modi, ad esempio scambiando informazioni, condividendo contenuti artistici, scrivendo commenti o recensioni, negoziando e concludendo accordi di varia natura.

Si è già avuto modo di vedere come le interazioni tra utenti possano dare luogo a relazioni giuridicamente rilevanti, come contratti – ad esempio di compravendita o aventi ad oggetto la fornitura di servizi – ma anche fatti illeciti, come violazioni di diritti di proprietà intellettuale, lesione di diritti della personalità o trattamenti illegittimi di dati personali. È importante qui aggiungere come tali rapporti, oltre che dalle norme di diritto di fonte pubblica, proprio perché si originano nell'ambito di una piattaforma digitale sono regolate anche dalle *policy* e regole di condotta della piattaforma stessa, le quali trovano

[17] Idem, in particolare, sempre a p. 64, l'autrice utilizza l'espressione «*membership agreement*» per descrivere i contratti conclusi tra gestori ed utenti delle piattaforme digitali e che ne animano la dimensione «verticale».

la propria fonte negli accordi contrattuali tra utenti e gestore che connotano la dimensione verticale di cui si è detto poc'anzi.

L'intreccio tra la dimensione verticale e quella orizzontale appena richiamato vale, a parere di una convincente dottrina[18], a distinguere da un punto di vista qualificatorio le piattaforme digitali da analoghe infrastrutture tecnologiche caratterizzate soltanto dal rapporto tra gestore – in qualità di fornitore di un servizio – ed utente.

Tali strutture costituiscono uno schema utilizzato per la fornitura di alcuni tra i più comuni servizi presenti sul mercato, come motori di ricerca o sistemi e applicazioni delle c.d. *smart-home* (es. assistenti virtuali, serrature domotiche). Esse, pur essendo assimilabili alle piattaforme da un punto di vista tecnico, se ne distinguono da un punto di vista socio-giuridico in quanto non permettono l'interazione tra utenti e, di conseguenza, l'instaurazione di rapporti giuridici diretti tra questi ultimi. In altre parole, si tratta di strutture in cui, da un punto di vista relazionale, non è presente la dimensione «orizzontale» di cui si è poc'anzi parlato. Detta assenza non consente, pertanto, la creazione delle comunità virtuali tipiche delle piattaforme digitali nell'ambito di questi ambienti con la conseguenza che, all'interno di essi, il gestore agirà soltanto come fornitore del proprio servizio e non anche come regolatore e supervisore dei rapporti tra gli utenti. Caratteristica quest'ultima che, come vedremo, connota in maniera decisiva il ruolo dei *provider* delle piattaforme ai fini del ragionamento che sarà svolto nelle successive pagine.

2.2 La dimensione istituzionale delle piattaforme: attori e procedimenti

Le analisi appena svolte consentono di introdurre la lettura giuridica che si privilegerà nel corso del presente lavoro, ossia quella che vede le piattaforme digitali come un fenomeno collettivo a valenza istituzionale.

[18] Idem, p. 65.

È collettivo, da un lato, poiché le piattaforme, pur propiziando delle relazioni che sono normalmente bilaterali – tanto nella dimensione «verticale» quanto in quella «orizzontale» – si rivolgono per loro natura ad una molteplicità di soggetti e vi si rapportano in modo globale. Il fenomeno ha, poi, un carattere istituzionale perché una piattaforma presuppone la costituzione e la condivisione di un modello organizzativo al quale tutti coloro che vogliono agire sulla stessa devono adattarsi, come emerge dalle considerazioni svolte a proposito della «dimensione verticale».

Il modello in questione viene stabilito dai gestori delle piattaforme, che sono coloro che determinano le regole e le *policy* di condotta che governano le stesse. In questo senso, quindi, essi agiscono come dei veri e propri regolatori privati[19], dettando norme e precetti a cui tutti gli utenti di una piattaforma debbono conformarsi se desiderano agire sulla stessa. Ciò rende quindi le piattaforme digitali degli ambienti giuridici in gran parte autoregolati.

Gli strumenti con cui i gestori stabiliscono ed impongono le proprie regole sono vari. In primo luogo, tali regole trovano, come detto, la propria fonte nelle condizioni generali di una piattaforma. Le condizioni in questione vengono stabilite direttamente dai gestori e sono accettate dagli utenti sin dal momento dell'iscrizione, pena l'impossibilità di operare sulla piattaforma stessa. Dette condizioni costituiscono, pertanto, lo strumento che regola il rapporto contrattuale tra un utente ed il gestore. Un rapporto che è strutturalmente segnato da un profondo squilibrio e in cui i gestori dispongono di un notevole potere nei

[19] Si vedano a questo proposito: A. MILLS, *The Law Applicable to Cross-Border Defamation on Social Media: Whose law governs free speech in 'Facebookistan'?*, in Journal of Media Law, Vol. 7, n. 1, pp. 1-35, 2015; C. BUSCH, *Self-Regulation and Regulatory Intermediation in the Platform Economy*, in M. CANTERO GAMITO, H.W. MICKLITZ (a cura di), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, pp. 115-134, Edward Elgar, 2019; M. CANTERO GAMITO, *Regulation.com. Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda*, in European Journal of Legal Studies, Vol. 9, n. 2, pp. 53-68, 2017.

confronti degli utenti, che si fonda anche sull'utilizzo dei dati personali di questi ultimi[20].

Peraltro, come abbiamo già avuto modo di anticipare in occasione dell'analisi della «dimensione verticale» dei rapporti giuridici che interessano le piattaforme digitali, tramite le condizioni generali i gestori non si limitano a disciplinare i propri rapporti con gli utenti (*i.e.* le condizioni a cui viene fornito il servizio tipico della piattaforma) ma stabiliscono delle regole che – in tutto o in parte, direttamente o indirettamente – si applicano a tutte le attività che possono avvenire nell'ambito di una piattaforma digitale, conformando in questo senso la struttura giuridico-organizzativa di tali ambienti.

A tal proposito, una convincente ricostruzione dottrinale individua tre modalità attraverso cui i gestori esercitano il proprio potere regolatorio nell'ambito di una piattaforma[21].

La prima di esse riguarda la capacità di una piattaforma – e delle proprie condizioni – di influenzare e conformare il contenuto dei contratti che vengono conclusi tra gli utenti di essa. Ad esempio, sono le regole di Airbnb a stabilire i termini di cancellazione delle prenotazioni degli appartamenti offerti in locazione tramite la propria piattaforma, lasciando agli utenti soltanto la possibilità di scegliere tra alcune opzioni prestabilite e non modificabili[22]. Si tratta di rapporti a cui il gestore della piattaforma non prende normalmente parte, limitandosi invece a propiziarli mettendo a disposizione l'ambiente virtuale in cui la volontà degli utenti si incontra, ma sui quali le regole da esso stabilite assumono in questo modo una rilevanza decisiva.

---

[20] I. PRETELLI, op. cit. 11, p. 27.

[21] V. C. BUSCH, *op. cit.* 19, p. 117 ss.

[22] Consultabili al seguente indirizzo: https://www.airbnb.it/home/cancellation_policies. A commento si veda C. BUSCH, *op. cit.* 19, p. 119.

Un altro strumento attraverso cui le piattaforme esercitano il proprio potere regolatorio è costituito delle *policy* e dalle regole di condotta (spesso chiamate anche con termini quali «*community guidelines*» o «*netiquette*») al cui rispetto gli utenti sono vincolati[23] – sovente tramite un esplicito richiamo da parte delle condizioni generali – e la cui violazione può anche portare all'esclusione dalla piattaforma. Le regole in questione, di applicazione generale, hanno spesso a che fare con questioni etiche e possono riguardare tanto attività che avvengono e si estrinsecano completamente sulla piattaforma – come la condivisione di contenuti offensivi, illegali o discriminatori[24] – quanto comportamenti da tenere sia all'interno che all'esterno dello spazio virtuale[25]. Quest'ultimo aspetto, come vedremo, ha conseguenze in merito all'effettiva capacità dei gestori di garantire il rispetto di tali regole da parte dei propri utenti.

Un terzo elemento preso in considerazione dalla dottrina[26] è rappresentato dai sistemi reputazionali («*reputation systems*»), ossia i meccanismi attraverso cui le piattaforme raccolgono o consentono ai propri utenti di pubblicare commenti o recensioni relative alla piattaforma stessa o al comportamento di altri utenti, sia che questi siano venditori di beni o fornitori di servizi – si pensi ad

---

[23] Idem a p. 119.

[24] A questo proposito si vedano ad esempio le diverse linee guida e *netiquette* relativa al divieto di diffusione di contenuti o alla tenuta di condotte di incitamento all'odio adottate negli ultimi anni dai principali *social network*. V. in particolare le policy di: (i) Twitter: https://help.twitter.com/it/rules-and-policies/hateful-conduct-policy; (ii) Facebook: https://www.facebook.com/business/help/170857687153963?id=208060977200861

[25] V. in questo senso le linee guida di Uber per gli Stati Uniti, le quali impongono la c.d. «*no sex policy*» ai propri autisti e *rider*: https://www.uber.com/legal/community-guidelines/us-en/. V. a commento: M. FINCK, *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy*, LSE Law, Society and Economy Working Papers, n. 15, London School of Economics and Political Science Law Department, 2017; C. BUSCH, *op. cit.* 19, p. 119. Si vedano altresì gli «Standard della community» di Airbnb, che impongono delle regole comportamentali per i conduttori degli immobili («*guest*»). A titolo di esempio, gli standard in questione prevedono: «Non dovresti creare disturbo all'interno degli spazi comuni e ai vicini, né dovresti considerarli alla stregua di una semplice "reception" o non rispondere ai loro appelli». Gli standard in questione sono consultabili al seguente link: https://www.airbnb.it/trust/standards?_set_bev_on_new_domain=1637501739_NWNmOWNmY2M5M2Rj.

[26] V. in questo senso: C. BUSCH, *op. cit.* 19, p. 120; M. CANTERO GAMITO, *op. cit.* 19, p. 60.

esempio alle recensioni su TripAdvisor – che acquirenti o fruitori, come nel caso dei commenti sul comportamento degli ospiti durante i periodi di soggiorno che possono essere pubblicati dai locatori di immobili su Airbnb. L'importanza di tali sistemi è ritenuta cruciale per il modello di *business* delle piattaforme[27], il cui successo è spesso conseguenza dalla fiducia di cui esse godono tra i propri utenti.

Da un punto di vista regolatorio la rilevanza dei sistemi reputazionali viene individuata nella loro capacità di influenzare il comportamento degli utenti inducendoli al rispetto di canoni di condotta spontaneamente originatisi nell'ambito di una piattaforma. La circostanza che il loro comportamento sia costantemente oggetto di valutazioni e giudizi espressi pubblicamente contribuisce, infatti, a far sì che le attività degli utenti e dei gestori siano – oltre che improntate al rispetto delle *policy* e delle regole della piattaforma – caratterizzate da comportamenti che consentano di conquistare la fiducia degli altri soggetti che agiscono sulla piattaforma. In questo senso, i sistemi reputazionali contribuiscono alla generazione spontanea di canoni di condotta[28] a cui ciascun utente o gestore è tenuto a conformarsi, pena la sostanziale perdita di fiducia di cui gode lo stesso all'interno della piattaforma, quale conseguenza delle recensioni o dei pareri negativi degli altri utenti. Perdita di fiducia che

[27] Si veda a questo proposito M. CANTERO GAMITO, op. cit. 19, p. 60, per cui: «*Platform businesses, in particular those belonging to the Sharing Economy, are largely designed around trust regimes and reputational ordering*». Si veda anche C. KUNER, *The 'Internal Morality' of European Data Protection Law*, 2008, disponibile su SSRN: https://ssrn.com/abstract=1443797 o http://dx.doi.org/10.2139/ssrn.1443797. In questa opera in particolare l'autore, a proposito della Direttiva 95/46/CE in materia di protezione dei dati personali osserva come «Besides 'legal' enforcement methods such as fines, injunctions, criminal penalties etc., 'soft' penalties such as adverse publicity are an important incentive to comply with data protection law, since damage to a company's reputation can ultimately cause it more harm in the marketplace than can a fine».

[28] Idem, p. 61. V. anche C. BUSCH, *op. cit.* 19, p. 121ss

può avere degli effetti devastanti, sino al punto di costringere un utente ad abbandonare del tutto una piattaforma[29].

In questo modo, argomentano alcuni autori[30], i sistemi reputazionali, oltre a dar vita a consuetudini e pratiche che contribuiscono all'autoregolamentazione di una piattaforma («*race to the top*»), costituiscono anche uno strumento di controllo della comunità virtuale ivi presente, assolvendo a funzioni di verifica e monitoraggio che incentivano condotte in linea con le menzionate pratiche.

2.3 L'importanza della tecnologia nell'autoregolamentazione delle piattaforme

A connotare la dimensione istituzionale delle piattaforme e la loro tendenza all'autoregolamentazione contribuisce in maniera decisiva anche il fatto che i gestori delle stesse siano i medesimi soggetti che stabiliscono e governano l'architettura e le regole tecniche che permettono a ciascun utente di agire su tali ambienti.

Nell'ambito di una piattaforma, infatti, ogni attività giuridicamente rilevante deve avvenire, oltre che in conformità con le norme di condotta e gli obblighi contrattuali poc'anzi esaminati, anche nel rispetto dei protocolli e delle regole tecniche su cui si fonda la piattaforma. Ciò è necessario in quanto, in mancanza, non sarebbe semplicemente possibile per un soggetto effettuare alcuna operazione sulla piattaforma stessa. Ne discende che il gestore è in grado, attraverso le proprie scelte tecniche, di decidere cosa un utente può o non può fare nell'ambito della propria piattaforma.

---

[29] V. C. BUSCH, *op. cit.* 19, p. 121.

[30] Idem, v. pag. 122. V. anche M. CANTERO GAMITO, *op. cit.* 19, p. 60.

La tecnologia assume in questo senso una rilevanza decisiva nell'orientare, anche da un punto di vista giuridico, il comportamento degli utenti di una piattaforma digitale[31].

Tale affermazione si colloca nel solco di una tesi dottrinale[32] che, sin dallo sviluppo di internet negli anni '90, afferma come le regole tecnologiche assumano, nello spazio virtuale, una funzione normativa paragonabile – e in alcuni casi persino superiore – a quella statale. Tale dottrina, sulla quale torneremo più approfonditamente in seguito (v. *infra*: Capitolo 4, par. 2), riassume il fenomeno con espressioni tipo «*Lex Informatica*» o «*Code Is Law*» e riconosce a colui che stabilisce l'architettura tecnica di un determinato spazio virtuale – il gestore per quanto riguarda una piattaforma digitale – un potere regolatorio assai marcato nell'ambito dell'ambiente da esso amministrato.

Il potere dei gestori emerge in maniera più evidente se si considerano i caratteri fondamentali delle regole tecniche che governano una piattaforma digitale.

Senza pretese di addentrarsi in analisi approfondite di tipo tecnico, basti qui rilevare come dette regole si basano su algoritmi che sono in grado di identificare un obiettivo e mettere in atto automaticamente i meccanismi necessari a perseguirlo[33] grazie alla costante attività di elaborazione dei dati raccolti dalla

---

[31] V. in questo senso C. BUSCH, *op. cit.* 19, p. 126; M. FINCK, *op cit.* 25.

[32] V. in questo senso i seguenti contributi: L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, 1999 – si veda anche la seconda edizione: L. LESSIG, *Code and Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006; J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in Texas. Law Review, Vol. 76, n. 3, 1998. Vedi anche, più di recente: A. STEMLER, *Regulation 2.0: The Marriage of New Governance and Lex Informatica*, in Vanderbilt Journal of Entertainment & Technology Law, Vol. 19, n. 1, pp. 87-132, 2016.

[33] L. AMMANNATI, op. cit. 15, p. 16.

piattaforma. In questo modo gli algoritmi sono in grado di produrre automaticamente – e spesso in tempo reale – determinati effetti al ricorrere di specifici presupposti che vengono stabiliti dai gestori.

Sulla scorta di tali premesse, la dottrina[34] ha individuato due ampie modalità attraverso cui si concretizza quella che è stata definita come «*algorithmic regulation*». La prima è quella identificabile come «*intelligent enforcement*» (o anche «*perfect enforcement*»), in cui l'algoritmo individua la violazione ed agisce automaticamente in tempo reale senza intervento umano. Tale modalità viene utilizzata in ambito contrattuale per garantire il rispetto dei termini convenuti tra le parti (uno degli esempi fatti in dottrina si riferisce ai sistemi di monitoraggio che talora vengono installati sui veicoli da compagnie assicurative o società di noleggio che permettono di verificare in tempo reale che il conducente stia adempiendo ai propri obblighi di guidare in maniera sicura). La seconda modalità è invece definita come «*pre-emptive enforcement*», in cui l'algoritmo è utilizzato per identificare preventivamente possibili violazioni o eventi dannosi e mettere in atto contromisure idonee a prevenirle (tipico esempio di ciò sono gli strumenti di valutazione del rischio sulla base di *big data* utilizzati da compagnie di assicurazione o da operatori finanziari).

L'utilizzo di algoritmi sempre più avanzati anche nell'ambito delle piattaforme digitali fa sì che le regole che governano le stesse non abbisognino di azioni coercitive di soggetti esterni – ed in particolare delle autorità statali – per poter essere correttamente applicate in tali ambienti. Grazie all'algoritmo, ad esempio, una piattaforma è in grado di scovare rapidamente un contenuto non in linea con le proprie *policy* o illegale e di rimuoverlo automaticamente

[34] Idem, p. 16; V. anche K. YEUNG, *Algorithmic regulation and intelligent enforcement*, in M. LODGE (a cura di), *Regulation Scholarship in Crisis?*, Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science – Discussion Paper n. 84, pp. 50-61, 2016.

in poco tempo[35], così come di prevenire alla radice il compimento di determinate azioni.

In questo senso le regole stabilite dai gestori risultano, nell'ambito di una piattaforma, più efficaci e facilmente applicabili delle stesse norme di fonte pubblica, le quali nella maggior parte dei casi necessitano invece della cooperazione dei gestori o di altri soggetti terzi per poter spiegare i propri effetti nello spazio virtuale[36].

3 Criticità legate all'impiego delle regole di diritto internazionale privato nell'ambito delle piattaforme e bisogno di nuovi paradigmi

La regolamentazione delle piattaforme digitali solleva anche delle questioni di diritto internazionale privato, dal momento che tali ambienti, così come le relazioni che si svolgono al loro interno, presentano un carattere quasi inevitabilmente transfrontaliero, in quanto coinvolgono persone stabilite in più parti del mondo e favoriscono l'istituzione di rapporti raramente destinati ad esaurirsi nell'orizzonte di un unico paese.

---

[35] V. K. YEUNG, *op. cit.* 34, p. 51.

[36] A sostegno di questa affermazione si veda quanto affermato dalla Supreme Court of Canada nel caso *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34, [2017] 1 S.C.R. 824, 28 giugno 2017. Nella pronuncia, in particolare, la suprema corte canadese ha ammesso come, per poter effettivamente dare seguito alle proprie ingiunzioni sulla rete fosse necessaria la cooperazione di Google: «The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates – globally». Per un commento vedi *ex multis*: I. PRETELLI, *op. cit.* 11, p. 42; J. DASKAL, *Google Inc. v. Equustek Solutions Inc.*, in American Journal of International Law, Vol. 112, n. 4, pp. 727-733, 2018; C. ETTELDORF, *Canadian Supreme Court on Google: Effective Legal Protection Tops Jurisdictional Boundaries,* in European Data Protection Law Review (EDPL), Vol. 3, n. 3, pp. 384-386, 2017; M. DOUGLAS, *A Global Injunction Against Google,* in The Law Quarterly Review, Vol. 134, n. 2, pp. 181-187, 2018. Disponibile su SSRN: https://ssrn.com/abstract=3137526

Ne consegue che le piattaforme siano oggetto di norme di diversi ordinamenti giuridici statali o regionali che – inevitabilmente – disciplinano il fenomeno secondo angolazioni e sensibilità diverse, risultando non raramente in conflitto tra di loro[37].

I conflitti in questione interessano tanto la regolamentazione dei rapporti fra gestori e utenti che connotano la dimensione «verticale» delle piattaforme, quanto quella delle relazioni che si costituiscono tra i singoli utenti che, come si è visto, animano la dimensione «orizzontale». Essi riguardano, inoltre, diversi ambiti del diritto che vengono in rilievo nell'ambito delle piattaforme: dal diritto dei contratti alla responsabilità extracontrattuale, dalla proprietà intellettuale alla protezione dei dati personali, dalla tutela dei consumatori al diritto del lavoro, sino alla normativa in materia di concorrenza e pratiche commerciali scorrette.

Come si è già avuto modo di anticipare, anche dal punto di vista internazionalprivatista sono molte le incertezze legate al fenomeno giuridico delle piattaforme. Le incertezze in questione derivano, in particolare, dalla conformazione delle attuali regole di diritto internazionale privato.

In primo luogo, tali norme risultano, infatti, in gran parte ispirate a logiche territoriali che male si attagliano ad ambienti come le piattaforme che sono, al contrario, generalmente privi di ancoraggi territoriali ed attraversati da interessi – la protezione dei dati personali, ad esempio – perlopiù immateriali e, come tali, non agevolmente collocabili nello spazio. Ciò rende difficile,

---

[37] V. ad esempio: T. LUTZI, *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 129-146, Schulthess, 2018, p. 133; G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE,* in Diritto dell'informazione e dell'informatica, fasc. 4-5, p. 697-718, 2015.

nell'ambito delle piattaforme, l'applicazione dei tradizionali criteri di collegamento internazionalprivatistici basati sulla territorialità. Si pensi, ad esempio, alla difficoltà di individuare con certezza il «luogo di esecuzione[38]» di una determinata obbligazione o «il luogo in cui l'evento dannoso è avvenuto[39]» nell'ambito di una piattaforma digitale[40]. L'applicazione di simili criteri – tanto per determinare la legge applicabile quanto ai fini della competenza giurisdizionale – richiede infatti l'individuazione di un luogo fisico in qualche modo collegato alla piattaforma considerata: operazione che, come abbiamo già avuto modo di intuire e avremo modo di approfondire in seguito, non è sempre agevole e risulta in certi momenti pressoché impossibile[41].

L'utilizzo di tali criteri, peraltro, può spesso condurre all'individuazione di più ordinamenti potenzialmente competenti ed è in questo senso suscettibile di minare i capisaldi su cui si fondano le stesse norme di diritto internazionale privato, primo tra tutti il principio della prevedibilità, che è uno degli obiettivi principali delle regole internazionalprivatistiche del sistema dell'Unione europea[42].

L'altra caratteristica delle norme di diritto internazionale privato che ne complica l'applicazione nell'ambito delle piattaforme digitali è rappresentata dalle

---

[38] V. a questo proposito art. 7, n. 1 Regolamento (UE) n. 1215/2012 ("Bruxelles I*bis*").

[39] V. a questo proposito: art. 7, n. 2 Regolamento (UE) n. 1215/2012 ("Bruxelles I*bis*"); art. 4, par. 1, Regolamento (CE) n. 467/2007 ("Roma II").

[40] V. I. PRETELLI, *op. cit.* 11, p. 27.

[41] Idem a p. 21, dove l'autrice fornisce una utile ricognizione sui punti di incontro tra mondo virtuale e mondo fisico nell'ambito delle piattaforme digitali. Sul punto v. meglio *infra* Capitolo 3).

[42] Vedi ad esempio: considerando 15 del Regolamento (UE) n. 1215/2012 ("Bruxelles I*bis*"), secondo cui «È opportuno che le norme sulla competenza presentino un alto grado di prevedibilità […]»; considerando 16 del Regolamento (CE) n. 593/2008 ("Roma I"), secondo cui: «Per contribuire al conseguimento dell'obiettivo generale del presente regolamento, che è la certezza del diritto nello spazio giudiziario europeo, le regole di conflitto di leggi dovrebbero offrire un alto grado di prevedibilità […]»; considerando 16 del Regolamento (CE) n. 467/2007 ("Roma II"), secondo cui: «Norme uniformi dovrebbero migliorare la prevedibilità delle decisioni giudiziarie e assicurare un ragionevole equilibrio tra gli interessi del presunto responsabile e quelli della parte lesa […]».

logiche «stato-centriche» su cui esse tuttora si fondano. Tali norme – sia che si esprimano in termini generali ed astratti, come è nel caso delle norme di conflitto, sia che si traducano in comandi specifici e concreti, come accade con il riconoscimento delle decisioni – assolvono, infatti, esclusivamente la funzione di risolvere conflitti tra ordinamenti statali, senza prendere in considerazione – se non indirettamente, come nel caso del Regolamento Roma I[43] – sistemi normativi di matrice diversa, ivi inclusi quelli di matrice privata (c.d. «*private regulation*[44]»).

Per queste ragioni le regole di diritto internazionale privato faticano ad agire in ambienti come le piattaforme digitali che, come si è visto, sono invece modellati da norme – siano esse *policy* di condotta o standard tecnici – stabilite da regolatori privati (i gestori) e che non di rado si trovano in conflitto con le norme statali (o regionali) che pretendono di applicarsi alle attività che si svolgono nell'ambito di tali ambienti.

Lungi dall'aver trovato delle risposte univoche, lo studio dei richiamati conflitti tra norme di fonte pubblica e privata costituisce una nuova frontiera del diritto internazionale privato[45].

Nell'ambito delle piattaforme digitali questo intreccio è, peraltro, legato a doppio filo al tema del controllo di internet[46]. Sulla rete, e di conseguenza su

---

[43] V. in particolare considerando 13, a mente del quale «Il presente regolamento non impedisce che le parti includano nel loro contratto, mediante riferimento, un diritto non statale ovvero una convenzione internazionale».

[44] V. *ex multis*: J. BOMHOFF, A. MEUWESE, *The Meta-regulation of Transnational Private Regulation*, in Journal of Law and Society, Vol. 38, n. 1, pp. 138-162, 2011; O. KAHN-FREUND, *General Problems of Private International Law,* Sijthoff, 1976, p. 272; R. MICHAELS, *The Re-State-ment of Non-State Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism*, in Wayne Law Review, Vol. 51, n. 3, p. 1209-1260, 2005; R. MICHAELS, *True Lex Mercatoria: Law Beyond the State*, in Indiana Journal of Global Legal Studies, Vol. 14, n. 2, 2007; R. WAI, *Transnational Liftoff and Juridical Touchdown: Regulatory Function of Private International Law in an Era of Globalization*, in Columbia Journal of Transnational Law, Vol 40, n. 2, pp. 209-274, 2002.

[45] J. BOMHOFF, A. MEUWESE, *op. cit.* 44, p. 49.

[46] V. *ex multis*: J.L. GOLDSMITH-T. WU, *Who Controls the Internet? Illusion of a Borderless World*, Oxford University Press, 2006; D.J. SVANTESSON, *Private International Law and the Internet* (3rd

una piattaforma, si trovano, infatti, ad agire attori di diverso tipo, sia pubblici che privati, ciascuno dei quali persegue delle finalità specifiche e rivendica una propria fetta di sovranità[47]. Per tale ragione, si è assistito negli ultimi tre decenni ad un massiccio intervento di natura «politica» da parte di Stati ed organizzazioni internazionali – tra tutte l'Unione europea – che, nel regolare la materia, hanno via via tentato sempre di più di definire, spesso estendendolo, l'ambito di applicazione territoriale della propria legislazione e giurisdizione[48]. Massicci interventi che sono stati anche le risposta al proliferare di un certo strapotere regolatorio[49] di grandi attori privati che agiscono sulla rete,

edition), Kluwer Law International, 2016; D.J. SVANTESSON, *Sovereignty in International Law – How the Internet Changed Everything, but not for Long*, in Masaryk University Journal of Law and Technology, Vol. 8, n. 1, pp. 137-155, 2014.

[47] V. *ex multis*: J.L. GOLDSMITH-T. WU, *op. cit.* n. 46; J.L. GOLDSMITH, *Against Cyberanarchy*, University of Chicago Law Occasional Paper, n. 40, 1999; J. DASKAL, *Borders and Bits*, in Vanderbilt Law Review, Vol. 71, n. 1, pp. 179-240, 2018; G. RESTA, *op. cit.* 37; G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani*, Editoriale Scientifica, 2018; V. ZENO-ZENCOVICH, *Intorno alla decisione del caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, in Diritto dell'informazione e dell'informatica, Vol. 31, fasc. 4-5, pp. 683-696, 2015. A livello istituzionale, si veda anche il seguente documento commissionato dal Parlamento europeo in merito alla «Sovranità digitale» europea: T. MADIEGA, *Digital Sovereignty for Europe*, EPRS Ideas Paper, PE 651.992, 2020, disponibile online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992.

[48] V. *ex multis*: F. BIGNAMI-G. RESTA, *Human Rights Extraterritoriality: the Right to Privacy and National Security Surveillance*, in E. BENVENISTI, G. NOLTE (a cura di) *Community Interests Across International Law*, pp. 357-380, Oxford University Press, 2019; A. BRADFORD, *The Brussels Effect*, in Northwestern University Law Review, Vol. 107, n. 1, pp. 1-67, 2012; A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020; C. KUNER, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, in International Data Privacy Law, Vol. 5, n. 4, pp. 235-245, 2015; G. RESTA, *op. cit.* 37; D.J. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and its Practical Effect on U.S. Businesses*, in Stanford Journal of International Law, Vol. 50, n. 1, pp. 53-117, 2014; V. ZENO-ZENCOVICH, *op. cit.* 47; D.J. SVANTESSON, *A "Layered Approach" to Extraterritoriality of Data Privacy Laws*, in International Data Privacy Law, Vol. 3, n. 4, pp. 278-286, 2013; D.J. SVANTESSON, *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, in Santa Clara Journal of International Law, Vol. 13, n. 2, pp. 517-571, 2015; B. VAN ALSENOY, M. KOEKKOEK, *Internet and Jurisdiction after Google Spain: the Extra-Territorial Reach of the EU's "Right to be Forgotten"*, KU Leuven, Working Paper n. 153, 2015.

[49] V. *ex multis*: G. SARTOR, M.V. DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/UE*, in *Diritto dell'informazione e dell'informatica,* fasc. 4-5, pp. 657-680, 2014.

dei quali i gestori di piattaforme rappresentano una componente assai rilevante.

Gli interventi in questione non hanno tuttavia risolto le questioni di diritto internazionale privato poc'anzi presentate ma sono al contrario spesso sfociati in fenomeni di «*regulatory overreaching*[50]», vale a dire l'incapacità di una norma di trovare applicazioni concrete alle fattispecie che si prefigge di regolare determinando ed estendendo unilateralmente il proprio ambito di applicazione.

Nel prosieguo del presente lavoro si tenterà pertanto di contribuire al dibattito sulla regolamentazione delle piattaforme anche dal punto di vista del diritto internazionale privato, partendo dalla constatazione per cui per questi fini si rendano necessari nuovi paradigmi che tengano conto della dimensione istituzionale delle piattaforme e del potere regolatorio dei loro gestori.

4 Le angolature da cui si studierà il problema

Il presente lavoro affronterà i problemi regolatori sottesi all'utilizzo delle piattaforme digitali cui si è avuto modo di accennare in una prospettiva transazionale ed internazionalprivatista.

L'analisi si focalizzerà principalmente sul diritto dell'Unione europea, pur senza trascurare un confronto con le soluzioni praticate in altri contesti geografici e politici, primi tra tutti gli Stati Uniti d'America, paese in cui hanno sede alcuni tra i maggiori gestori di piattaforme a livello globale.

L'indagine si concentrerà, in particolare, su due filoni. Punto di partenza saranno le norme di diritto materiale dell'Unione che affrontano, direttamente o indirettamente, il fenomeno delle piattaforme digitali. Come avremo modo di

[50] V. ad esempio: D.J. SVANTESSON, *The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach*, EUI Working Papers, RCAS 2015/45, Robert Schuman Centre for Advanced Studies - Florence School of Regulation, 2015; D.J. SVANTESSON, *Extraterritoriality and Targeting in the EU Data Privacy Law: the Weak Spot Undermining the Regulation*, in International Data Privacy Law, Vol. 5, n. 4, pp. 226-234, 2015

vedere, infatti, il legislatore dell'Unione europea ha dimostrato negli ultimi anni una speciale attenzione per il mondo digitale, che ha portato all'adozione di diversi strumenti di diritto materiale[51]. Tale attenzione è ulteriormente aumentata a seguito del lancio, da parte della Commissione europea, della strategia relativa alla creazione di un c.d. Mercato Unico Digitale (Digital Single Market)[52], avvenuto a cavallo tra il 2014 e il 2015.

[51] Tra gli strumenti normativi adottati dal legislatore, sia precedenti che successivi al lancio della Digital Single Market Strategy, si citano ad esempio: Direttiva 2000/31/CE sul commercio elettronico, la Direttiva 2002/58/CE sulla protezione dei dati personali nel settore delle comunicazioni elettroniche – apparsa in *GU L 201 del 31.7.2002, pagg. 37–47*; Direttiva (UE) 2015/1535 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione – apparsa in *GU L 241 del 17.9.2015, pagg. 1–15*; 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) (Testo rilevante ai fini del SEE) – apparso in *GU L 119 del 4.5.2016, pagg. 1–88*; Regolamento (UE) 2017/1128 relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno – apparso in *GU L 168 del 30.6.2017, pagg. 1–11*; Regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (Testo rilevante ai fini del SEE) – apparso in *GU L 303 del 28.11.2018, pagg. 59–68*; Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (Testo rilevante ai fini del SEE) – apparso in *GU L 151 del 7.6.2019, pagg. 15–69*; Regolamento (UE) 2019/1150 sulla trasparenza nei confronti degli utenti commerciali delle piattaforme digitali – apparso su *GU L 186 dell' 11.7.2019, pagg. 57–79*.

[52] La Digital Single Market Strategy, ossia il progetto relativo alla creazione di un Mercato Unico Digitale (Digital Single Market), è stata lanciata nel 2014 dalla Commissione Juncker, che l'ha inserita tra le priorità (la numero 2) del proprio programma di governo (*Un nuovo inizio per l'Europa – Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico* – Strasburgo, 15 luglio 2014). L'estratto del programma relativo alla Digital Single Market Strategy è stato inserito nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 6 maggio 2015. Reperibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

Nel quadro della predetta strategia, si segnalano, in ultimo, due regolamenti entrati in vigore nell'autunno 2022 e derivanti dalla medesima proposta legislativa relativa a un «pacchetto sui servizi digitali[53]» presentata dalla Commissione nel dicembre 2020. Si tratta, in particolare, del Regolamento UE 2022/1925 sui mercati digitali[54] («Digital Markets Act») e del Regolamento UE 2022/2065 sui servizi digitali[55] («Digital Services Act»).

Il primo è un regolamento in materia di concorrenza, pensato per tutelare i mercati digitali affrontando le conseguenze negative derivanti dai comportamenti di determinate piattaforme che, nel corso degli anni, hanno assunto il ruolo di controllori dell'accesso ai mercati stessi («*gatekeeper*»). Esso persegue, infatti, lo scopo di contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti i *gatekeeper* siano equi e contendibili in tutta l'Unione, a vantaggio sia degli utenti commerciali che degli utenti finali[56]. Questo regolamento non sarà trattato nel presente lavoro, così come non lo saranno, più in generale, le tematiche specificamente attinenti alla concorrenza nei mercati in cui agiscono le piattaforme digitali[57], che saranno

---

[53] La pagina informativa sul Digital Services Act Package è consultabile al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package. La proposta originaria relativa al Digital Markets Act è reperibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN. La proposta originaria relativa al Digital Services Act è reperibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

[54] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) (Testo rilevante ai fini del SEE), apparso in *GU L 265 del 12.10.2022, pagg. 1–66*.

[55] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (Testo rilevante ai fini del SEE), apparso in *GU L 277 del 27.10.2022, pagg. 1-102.*

[56] Art. 1, par. 1 DMA.

[57] Per approfondire queste tematiche si vedano *ex multis*: F. DE LONGIS, *L'agenda digitale europea. Mercato, tecnologia e regolamentazione*, Guerini Next, 2016; V. FALCE (a cura di), *Competition Law*

soltanto tangenzialmente lambite quando ci si occuperà del c.d. Regolamento P2B (v. *infra*: Cap. 2, par. 3.1) o degli aspetti relativi al diritto internazionale privato (v. *infra*: Cap. 3, par. 4.3).

Il Digital Services Act costituisce, invece, il primo insieme di norme comuni sugli obblighi e sulle responsabilità dei fornitori di servizi intermediari online applicabili all'interno del Mercato Unico Europeo. Esso, tra le altre cose, affronta direttamente le questioni della regolamentazione delle piattaforme e del potere regolatorio dei loro gestori, ponendo in capo a questi precisi obblighi di trasparenza e «*accountability*» (formula che da qui in avanti si preferirà ai vari tentativi di traduzioni del concetto in lingua italiana con espressioni tipo «responsabilizzazione» o «responsabilità»). Il Digital Services Act, si argomenterà meglio nel prosieguo, si colloca, quindi, tra quegli strumenti del diritto dell'Unione che sembrano riconoscere e legittimare il potere regolatorio dei gestori delle piattaforme, cercando al contempo di limitarlo e di orientarlo al rispetto dei valori perseguiti dall'ordinamento dell'Unione. Ad esso sarà dedicato l'intero Capitolo finale (v. *infra*: Cap. 6).

L'altro filone di ricerca su cui si concentrerà il presente lavoro sarà costituito dalle principali misure legislative dell'Unione europea nel campo del diritto internazionale privato dei rapporti patrimoniali, ossia il Regolamento UE n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (Bruxelles I*bis*), il Regolamento CE n. 593/2008 sulla legge applicabile alle obbligazioni contrattuali (Roma I) e il Regolamento CE n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali (Roma II).

Enforcement in Digital Markets, Giappichelli, 2021; A. NICITA, A. MANGANELLI, *Regulating Digital Markets – The European Approach*, 2022.

L'analisi di questi regolamenti verrà condotta tenendo conto delle particolarità del fenomeno delle piattaforme e alla luce dei già citati strumenti di diritto materiale adottati negli ultimi decenni dall'Unione e che interessano, direttamente o indirettamente, il fenomeno delle piattaforme o comunque la vita di relazione «digitale» di professionisti e consumatori. Per gli aspetti che il diritto internazionale privato dell'Unione non copre, un'attenzione specifica sarà dedicata alle pertinenti norme di diritto materiale in settori come la protezione dei dati personali o contenute nei medesimi strumenti relativi alle piattaforme digitali che saranno esaminati nel presente lavoro.

Centrale, tanto nell'analisi dei profili di diritto materiale quanto di quelli internazionalprivatisti, sarà lo studio del già richiamato intreccio tra le tradizionali norme di fonte pubblica con le regole, *policy* di condotta e standard tecnici stabiliti unilateralmente dai gestori delle piattaforme, la cui esistenza connota la dimensione istituzionale delle stesse piattaforme. L'indagine su tale intreccio sarà svolta a partire da una ricognizione generale – seppur per forza di cose limitata – della c.d. «*private regulation*», ossia il fenomeno per cui, in determinati settori, si assiste ad una regolamentazione effettuata non dai tradizionali attori pubblici ma da soggetti privati[58]. Saranno quindi affrontate le ricadute transnazionali dovute alla proliferazione di tali forme di regolamentazione

[58] Nel rimandare al Capitolo 4 per una disamina del fenomeno della *private regulation*, si menzionano sin da ora, *ex multis*, le seguenti opere sul tema: J. BOMHOFF, A. MEUWESE, *op. cit.* 44; F. CAFAGGI, *The Architecture of Transnational Private Regulation*, EUI Working Paper LAW 2011/12, 2011; F. CAFAGGI, *New Foundations of Transnational Private Regulation,* in Journal of Law and Society, Vol. 38, n. 1, pp. 20-49, 2011; C. SCOTT, F. CAFAGGI, L. SENDEN, *The Conceptual and Constitutional Challenge of Transnational Private Regulation*, in Journal of Law and Society, Vol. 38, n. 1, pp. 1-19, 2011; F. CAFAGGI, *A Comparative Analysis of Transnational Private Regulation: Legitimacy, Quality, Effectiveness and Enforcement*, EUI Working Paper LAW 2014/15, 2014; K. PURNHAGEN, *Mapping Private Regulation – Classification, Market Access and Market Closure Policy and Law's Response*, in Journal of World Trade, Vol. 49, n. 2, pp. 309–324, 2015; F. CAFAGGI, *Regulating Private Regulators*, in S. CASSESE (a cura di), *Research Handbook on Global Administrative Law*, pp. 212-241, Edward Elgar 2016.
Si veda anche: F. CAFAGGI, A. RENDA, *Measuring the Effectiveness of Transnational Private Regulation*, 2014. Disponibile su SSRN al seguente link: https://ssrn.com/abstract=2508684.

privata e sarà prestata attenzione a come la dottrina tradizionale internazionalprivatista si rapporta con le norme di fonte diversa da quella statale. Lo studio si sposterà quindi sul ruolo della *private regulation* nell'ambito delle piattaforme digitali ed alla relazione di quest'ultima con il diritto di fonte pubblica all'interno dei predetti ambienti virtuali.

5 La tesi: il carattere istituzionale delle piattaforme e l'inevitabile cooperazione tra attori pubblici e privati per la regolamentazione delle stesse

Il presente lavoro ha l'obiettivo di verificare l'esistenza di paradigmi nuovi che permettano di risolvere, in una prospettiva transnazionale, i problemi regolatori sottesi all'utilizzo delle piattaforme digitali. La ricerca di tali paradigmi, in particolare, si innesta sull'ipotesi di lavoro richiamata, ossia che le piattaforme rivestano fondamentalmente un carattere istituzionale e debbano dunque essere analizzate, giuridicamente, a partire da tale loro natura.

L'analisi partirà, inevitabilmente, da una ricognizione delle criticità sottese all'utilizzo dei tradizionali metodi regolatori ed internazionalprivatisti. Criticità che sono ben esemplificate dal proliferare di norme di diritto internazionale privato di chiara matrice unilateralista[59], con cui i diversi ordinamenti statali e ragionali pretendono di estendere la propria sovranità sulla rete e sulle piattaforme digitali. L'analisi empirica dimostra, infatti, la scarsa effettività pratica di tali norme negli ambienti virtuali, che conduce sovente a fenomeni di «*regulatory overreaching*».

Alle difficoltà derivanti dall'utilizzo del metodo internazionalprivatista ortodosso e del diritto di fonte pubblica si contrappone lo strapotere regolatorio dei gestori delle piattaforme che, come si è visto, sono coloro che determinano

[59] Sul concetto di «unilateralismo» nel diritto internazionale privato e sulla sua contrapposizione al concetto di «multilateralismo» si vedano *ex multis*: O. KAHN-FREUND, *op. cit.* 44, p. 234; W. WENGLER, *The General Principles of Private International Law* (Volume 104), in *Collected Courses of the Hague Academy of International Law*, Sijthoff, 1961, p. 328.

le regole comportamentali e tecniche che governano tali ambienti. Regole che, peraltro, risultano «*self-enforcing*», in quanto non abbisognano di forze coercitive esterne per produrre i propri effetti. Come si è visto, questi fattori risultano decisivi per conferire alle piattaforme la richiamata dimensione istituzionale.

Verificata la bontà di tale ipotesi, occorrerà quindi chiedersi se ed in che modo la richiamata lettura del fenomeno imponga una riconsiderazione delle norme attuali che pretendono di applicarsi nell'ambito delle piattaforme.

In particolare, si cercherà di sostenere come, ai fini di una corretta e più efficace regolamentazione delle piattaforme, sia necessario adattare le norme di fonte pubblica alla dimensione istituzionale di tali ambienti. A tal riguardo, la strada da percorrere sembra essere quella di una collaborazione – piuttosto che di una risoluzione di conflitti, tipica del metodo tradizionale internazionalprivatista – tra regolamentazione pubblica e privata, basata tra l'altro su un sistema di regolamentazione «a strati», già invocato da parte della dottrina[60]. Vedremo, quindi, come tanto il legislatore dell'Unione quanto alcune pronunce giurisprudenziali[61] abbiano già intrapreso tale percorso, riconoscendo il carattere inevitabile di una collaborazione con i regolatori privati al fine di una più efficace regolamentazione delle piattaforme.

La suddetta collaborazione, peraltro, non dovrebbe significare per gli Stati – o per ordinamenti regionali come l'Unione europea – abdicare alle proprie funzioni di tutela di interessi generali della popolazione demandando *in toto* la regolamentazione di ambienti cruciali per la società di oggi, quali sono le piattaforme, a soggetti privati. Al contrario essa dovrebbe fondarsi su una mutua fiducia tra regolatore pubblico, regolatore privato ed utente, in cui agli

[60] V. ad esempio C. BUSCH, *op. cit.* 19.

[61] V. caso *Google Inc. v. Equustek Solutions Inc.* A livello dottrinale si rimanda a: I. PRETELLI, *op. cit.* 11, p. 42; J. DASKAL, *op. cit*. 36; C. ETTELDORF, *op. cit*. 36; M. DOUGLAS, *op. cit*. 36.

Stati rimarrebbe la determinazione dei principi generali cui la regolamentazione privata dovrebbe sottostare.

Tra i modi utilizzabili per stabilire questa collaborazione vi è l'imposizione in capo ai gestori di doveri di *accountability*, grazie a cui questi potrebbero in ogni momento dimostrare la propria conformità alle indicazioni degli attori pubblici nello svolgimento della propria funzione regolatoria, oltre che di trasparenza nei confronti degli utenti. Come vedremo, è questa la logica che già permea alcuni strumenti legislativi dell'Unione, tra cui il GDPR o il Regolamento (UE) 2019/1150, e su cui si fonda il nuovo Digital Services Act entrato in vigore nell'ottobre 2022.

Tali strumenti, seppur in misura differente, riconoscono infatti il potere regolatorio dei gestori delle piattaforme e cercano di contenerlo orientandolo al rispetto di determinati principi e regole stabilite a monte dal legislatore dell'Unione. Gli stessi strumenti, peraltro, pongono in capo ai gestori precisi obblighi di cooperazione nell'applicazione di alcune norme di diritto di fonte pubblica nell'ambito delle piattaforme stesse, specie in settori delicati come la protezione dei dati personali o il contrasto alla diffusione di contenuti illegali. A garantire la predominanza delle norme di fonte pubblica resta, come vedremo, lo strumento sanzionatorio, utilizzato con decisione sia dal GDPR che dal Digital Services Act con una funzione di «*market destroying measure*», come è stata descritta da attenta dottrina[62].

[62] D.J. SVANTESSON, *A "Layered Approach" to Extraterritoriality of Data Privacy Laws*, in International Data Privacy Law, Vol. 3, n. 4, pp. 278-286, 2013; D.J. SVANTESSON, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, 2013.

Capitolo 2 – Le piattaforme digitali nel diritto materiale dell'Unione europea

SOMMARIO: 1 L'affacciarsi di internet e delle piattaforme nel diritto dell'Unione europea: cenni. – 2 L'evoluzione dell'hosting *provider* nella disciplina dell'Unione: da soggetto irresponsabile a controllore «attivo» dei contenuti degli utenti. – 2.1 Il regime di *«safe harbour»* della Direttiva 2000/31/CE. – 2.2 Il progressivo superamento del *safe harbour* e la figura dell'*«hosting provider* attivo». – 2.3 Dall'irresponsabilità degli *hosting provider* verso un sistema basato sulla «*accountability*». L'esempio della Direttiva (UE) 2019/790. – 3 I nuovi paradigmi regolatori alla luce della Digital Single Market Strategy. – 3.1 Il Regolamento (UE) 2019/1150 e la tutela degli utenti commerciali delle piattaforme digitali. – …*Segue*: La dimensione istituzionale e la «responsabilizzazione» dei fornitori delle piattaforme nel Regolamento P2B. – 3.2 Altri strumenti rilevanti nell'ambito della Digital Single Market Strategy (cenni). – 4 Problemi qualificatori: i gestori delle piattaforme come *internet service provider* o come fornitori dei «servizi sottostanti»? – 4.1 La saga Uber e la qualifica di fornitore di «servizi nel settore dei trasporti». – 4.2 Una prima applicazione del «Metodo Uber»: il caso *Airbnb Ireland* e le conclusioni (apparentemente) opposte della Corte. – 4.3 Chiarimenti e questioni irrisolte alla luce delle sentenze *Uber Spain*, *Uber France* e *Airbnb Ireland*.

1 L'affacciarsi di internet e delle piattaforme nel diritto dell'Unione europea: cenni

A partire dagli anni '90, con la diffusione su larga scala di internet e del *world wide web*, l'Unione europea (all'epoca Comunità europea) ha iniziato ad occuparsi in maniera sempre più incisiva di diritto dell'informatica e della regolamentazione di alcune delle attività che si svolgono sulla rete.

La necessità di un intervento a livello europeo è apparsa, infatti, sin da subito ineludibile, data l'inevitabile dimensione transazionale del fenomeno di internet e il conseguente bisogno di stabilire, all'interno del Mercato Unico, almeno un quadro normativo di principi comuni tra i vari Stati membri, pur ammettendo le diverse sensibilità presenti sul tema[1].

L'attività del legislatore dell'Unione non si è, peraltro, concretizzata in una regolamentazione a 360 gradi di internet ma in strumenti legislativi settoriali che hanno riguardato diversi ambiti del diritto in cui il ruolo della rete è diventato sempre più preponderante. Senza pretese di esaustività, si pensi, ad esempio, alla tutela del *software*[2], alla protezione dei dati personali[3], alle firme

[1] V. *ex multis* S. RUSSO, R. SCAVIZZI, *Manuale di diritto dell'Unione dell'informatica*, Giuffrè, 2010.

[2] Con riferimento alla tutela del *software*, il primo strumento rilevante è la Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore – apparsa in *GU L 122 del 17.5.1991, pagg. 42–46*. La direttiva in questione è stata recepita in Italia con il D.lgs. 518/1992 e successivamente abrogata dalla Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore – apparsa in *GU L 111 del 5.5.2009, pagg. 16–22*.

[3] Si vedano a tal proposito: la 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 – apparsa in *GU L 281 del 23.11.1995, pagg. 31–50*; 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche) – apparsa in *GU L 201 del 31.7.2002, pagg. 37–47*. Il primo di tali strumenti è stato abrogato 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) – apparso in *GU L 119 del 4.5.2016, pagg. 1–88*.

elettroniche[4], alla protezione dei consumatori[5] ed al commercio elettronico[6]. Si è trattato prevalentemente di direttive, molte delle quali divenute rapidamente obsolete e negli anni sostituite, talvolta da regolamenti.

Non è questa la sede per approfondire nel dettaglio i diversi strumenti, peraltro sempre più numerosi, del diritto dell'Unione che hanno a che fare con internet. Nelle prossime pagine ci si concentrerà piuttosto su quelli che, direttamente o indirettamente, interessano più da vicino i profili di diritto materiale relativi alla regolamentazione delle piattaforme digitali.

2 L'evoluzione dell'*hosting provider* nella disciplina dell'Unione: da soggetto irresponsabile a controllore «attivo» dei contenuti degli utenti

Una delle materie paradigmatiche dell'approccio assunto dal legislatore dell'Unione nei confronti dei soggetti che agiscono sulla rete riguarda la disci-

[4] Si veda a tal proposito la Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro dell'Unione per le firme elettroniche – apparsa in *GU L 13 del 19.1.2000, pagg. 12–20.* La direttiva in questione è stata abrogata dal successivo Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE – apparso in *GU L 257 del 28.8.2014, pagg. 73–114*.

[5] Numerosi sono gli strumenti del diritto dell'Unione che hanno a che fare con la protezione dei consumatori, anche online. Con riferimento alla prima stagione regolatoria, si menzionano qui ad esempio: Direttiva 97/7/CE del Parlamento europeo e del Consiglio del 20 maggio 1997 riguardante la protezione dei consumatori in materia di contratti a distanza – apparsa in *GU L 144 del 4.6.1997, pagg. 19–27.* La direttiva è stata abrogata dalla successiva Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio – apparsa in *GU L 304 del 22.11.2011, pagg. 64–88*. Si veda inoltre: Direttiva 2002/65/CE del Parlamento europeo e del Consiglio, del 23 settembre 2002, concernente la commercializzazione a distanza di servizi finanziari ai consumatori e che modifica la direttiva 90/619/CEE del Consiglio e le direttive 97/7/CE e 98/27/CE. – apparsa in *GU L 271 del 9.10.2002, pagg. 16–24*.

[6] Lo strumento cardine del diritto dell'Unione in materia di commercio elettronico è tuttora 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») – apparsa in *GU L 178 del 17.7.2000, pagg. 1–16*.

plina della responsabilità dei prestatori di «servizi della società dell'informazione» («*internet service provider*») per le informazioni ed i contenuti illeciti condivisi dai propri utenti.

La disciplina in questione, così come l'evoluzione interpretativa e giurisprudenziale che l'ha contraddistinta, è rilevante ai nostri fini in quanto, al netto dei problemi qualificatori di cui si dirà *infra* (v. par. 4), tra gli *internet service provider* presi in considerazione dalla normativa europea sono state ricondotte anche gran parte delle piattaforme digitali[7].

Fonte principale della materia è 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 (da qui il nome di «direttiva sul commercio elettronico» o di «e-Commerce Directive» in inglese, più di frequente sostituito dalla crasi «Direttiva e-Commerce»). Essa continuerà a regolare la materia sino a quando i Digital Services Act non sarà pienamente applicabile (v. *infra*: Cap. 6, par. 1).

La Direttiva in questione, recepita in Italia con il D.lgs. 70/2003, ha stabilito un insieme di principi comuni relativi alla regolamentazione del commercio elettronico all'interno del Mercato Unico, allo scopo di garantire la libera circolazione dei «servizi della società dell'informazione» tra gli Stati membri (art. 1, par. 1). Ciò, in particolare, attraverso il ravvicinamento di alcune norme nazionali su tali servizi, lo stabilimento dei prestatori, le comunicazioni commerciali, i contratti per via elettronica, la responsabilità degli intermediari, i codici

[7] V. ad esempio: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Le piattaforme online e il mercato unico digitale – Opportunità e sfide per l'Europa*, COM(2016) 288 final, 25 maggio 2016; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Lotta ai contenuti illeciti online – Verso una maggiore responsabilizzazione delle piattaforme online*, COM(2017) 555 final, 28 settembre 2017.

di condotta, la composizione extragiudiziaria delle controversie, i ricorsi giurisdizionali e la cooperazione tra Stati membri (art. 1, par. 2).

La Direttiva, giova qui ricordarlo, non ha peraltro introdotto alcuna nuova norma di diritto internazionale privato né si è occupata di competenza giurisdizionale (art. 1, par. 3) (sul punto v. *infra*: Cap. 3, par. 4.3.2).

2.1 Il regime di «*safe harbour*» della Direttiva 2000/31/CE

Prima di addentrarci nell'analisi delle norme per noi rilevanti, occorre brevemente chiarire come per «servizio della società dell'informazione» si intenda, ai sensi dell'art. 2, lett. a) della Direttiva e-Commerce: «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi[8]». Il «prestatore» è, invece, la persona fisica o giuridica che fornisce tali servizi (art. 2, lett. b). Tra i prestatori di servizi della società dell'informazione rientrano diverse categorie di soggetti[9] che operano su internet, incluse come detto gran parte delle piattaforme digitali.

---

[8] L'art 2, lett. a) della Direttiva 2001/31/CE definisce in realtà «servizi della società dell'informazione» come «servizi ai sensi dell'articolo 1, punto 2, della direttiva 98/34/CE[8], come modificata dalla direttiva 98/48/CE». È quest'ultima disposizione che contiene la definizione richiamata. A tal riguardo, si chiarisce come, ai sensi dell'art. 1, punto 2, della direttiva 98/34/CE, come modificata dalla direttiva 98/48/CE, si intenda: (i) «a distanza»: un servizio fornito senza la presenza simultanea delle parti; (ii) «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici; (iii) «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale. Si aggiunge in ultimo come la direttiva 98/34/CE sia stata successivamente abrogata dalla Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (Testo rilevante ai fini del SEE) – apparsa in *GU L 241 del 17.9.2015, pagg. 1–15*. La menzionata direttiva del 2015, peraltro, riporta all'art. 1, lett. b) la medesima definizione di «servizio» di cui al precedente strumento abrogato.

[9] Si veda l'Allegato I della Direttiva (UE) 2015/1535 per un elenco di servizi non contemplati della definizione di «servizio della società dell'informazione» di cui all'art. 1, par. 1, lett. b) della medesima direttiva.

La Direttiva e-Commerce prevede (artt. 12-15) a favore degli *internet service provider* delle specifiche esenzioni di responsabilità (c.d. «*safe harbour provisions*») per le informazioni e i contenuti illeciti condivisi dai loro utenti (i «destinatari dei servizi[10]»). Le esenzioni in questione variano in base al tipo di prestatore di servizi preso in considerazione. Nello specifico, la direttiva individua tre categorie di *internet service provider*: prestatori di servizi di semplice trasporto di informazioni («*mere conduit*»), di memorizzazione temporanea («*caching*») e di memorizzazione duratura di informazioni («*hosting*»).

In breve, per i prestatori «*mere conduit*» è previsto (art. 12) il regime di esenzione più esteso, in quanto gli stessi non sono responsabili delle informazioni trasmesse a condizione che non diano origine alla trasmissione, non selezionino il destinatario della stessa e non selezionino né modifichino le informazioni trasmesse. Anche per i prestatori di servizi «*caching*» (art. 13) vige un generale regime di *safe harbour*, dal momento che essi vanno esenti da responsabilità a condizione che non modifichino le informazioni, si conformino alle condizioni di accesso ed alle norme di aggiornamento delle informazioni, non interferiscano con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni. Ai fini dell'esenzione, l'art. 13, par. 1, lett. e) richiede inoltre che il prestatore di servizi «*caching*» agisca prontamente per rimuovere le informazioni memorizzate, o per disabilitare l'accesso alle stesse, non appena venga a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete, che l'accesso alle informazioni è stato disabilitato oppure che

[10] Definizione fornita dall'art. 2, lett. d) della Direttiva 2000/31/CE, ai sensi del quale per «destinatario del servizio» si intende: «la persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili delle informazioni».

un organo giurisdizionale o un'autorità amministrativa ne abbia disposto la rimozione o la disabilitazione dell'accesso.

Più limitato è il regime di irresponsabilità dei prestatori di servizi di *hosting (*art. 15), le cui attività di memorizzazione finalizzate alla conservazione duratura implicano un'ingerenza maggiore nelle informazioni condivise dagli utenti. Per questi «*hosting provider*, tra cui si annoverano piattaforme digitali come *social network*, *marketplace* digitali o piattaforme di *crowdfounding*[11], l'esenzione opera a condizione che il prestatore non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene alle azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, ovvero che, non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. L'art. 15, par. 2, chiarisce peraltro come tali esenzioni non si applichino nel caso in cui il destinatario del servizio agisca sotto l'autorità o il controllo del prestatore.

Da quanto sopra emerge come la Direttiva e-Commerce sia in generale improntata sul principio dell'irresponsabilità degli *internet service provider*. Tale impostazione si basava sull'assunto, all'epoca generalmente valido, per cui i fornitori di servizi online siano dei meri intermediari che restano di regola estranei alle attività di selezione, organizzazione, produzione e aggiornamento dei contenuti condivisi sugli spazi da essi gestiti[12].

Per queste ragioni, l'art. 15 della direttiva esclude esplicitamente che vi sia in capo agli *internet service provider* un obbligo generale di sorveglianza[13] sulle

---

[11] V. COM(2017) 555 final, *supra* n. 7

[12] V. *ex multis*: O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in Percorsi Costituzionali, fasc. 1, pp. 45-74, 2014.

[13] V. a questo proposito: CGUE, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook Ireland Limited*, 3 ottobre 2019 – ECLI:EU:C:2019:821. Nella pronuncia in questione, in particolare, la Corte ha chiarito che l'art. 15, par. 1 della Direttiva e-Commerce non osta a che un giudice di uno Stato membro possa ordinare ad un *hosting provider* di: (i) rimuovere le informazioni da

informazioni che essi trasmettono o memorizzano né uno di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Agli Stati membri è lasciata soltanto la possibilità di stabilire in capo ai prestatori il dovere di informare le autorità competenti di presunte attività o informazioni illecite, inclusa la comunicazione di informazioni che consentano di identificare i destinatari dei servizi con cui essi hanno accordi di memorizzazione dei dati (art. 15, par. 1).

I doveri degli *internet service provider* di collaborazione con le autorità pubbliche sono peraltro ribaditi delle sopracitate norme che ne stabiliscono i regimi di irresponsabilità. In particolare, per tutte e tre le categorie è fatta salva la possibilità che gli organi giurisdizionali o le autorità amministrative degli Stati membri esigano che il prestatore impedisca o ponga fine ad una violazione[14]. Per gli *hosting provider* è fatta anche salva la possibilità che gli Stati membri definiscano procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime (art. 14, par. 3).

2.2 Il progressivo superamento del *safe harbour* e la figura dell'«*hosting provider* attivo»

esso memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, qualunque sia l'autore della richiesta di memorizzazione di siffatte informazioni; (ii) rimuovere le informazioni da esso memorizzate e il cui contenuto sia equivalente a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illeceità e che contiene gli elementi specificati nell'ingiunzione e le differenze nella formulazione di tale contenuto equivalente rispetto a quella che caratterizza l'informazione precedentemente dichiarata illecita non siano tali da costringere il prestatore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto; (iii) imuovere le informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime a livello mondiale, nell'ambito del diritto internazionale pertinente».

[14] Vedi in particolare le seguenti disposizioni della Direttiva 2000/31/CE: art. 12, par. 3 per quanto riguarda i prestatori di servizi di «*mere conduit*», art. 13, par. 2 per i «*caching*», art. 12, par. 3 per gli «*hosting*».

Come detto, il regime di irresponsabilità previsto dalla Direttiva e-Commerce si basava su un assunto che, se condivisibile all'epoca dell'approvazione dello strumento legislativo, è divenuto con gli anni sempre più superato, quanto meno per ciò che riguarda gli *hosting provider*.

Negli ultimi due decenni, infatti, si è assistito ad una poderosa crescita di *hosting provider* – tra cui le piattaforme digitali – che, lungi dallo svolgere attività meramente tecniche e passive, fondano i loro modelli di *business* proprio sull'utilizzo, l'elaborazione e l'organizzazione delle informazioni e dei contenuti forniti e caricati dai propri utenti, nonché dei loro dati personali. Questi dati e contenuti vengono infatti utilizzati in maniera attiva dai fornitori, anche grazie a sistemi di indicizzazione, categorizzazione e profilazione basati sui comportamenti degli utenti, allo scopo di trarne un profitto economico.

La sempre maggiore diffusione dei modelli di *business* brevemente descritti ha portato dottrina[15], istituzioni[16] e giurisprudenza[17] a mettere sempre più in dubbio la tenuta del principio di «neutralità» dei fornitori di servizi di *hosting* su cui si fondava il regime di irresponsabilità ai sensi dell'art. 15 della Direttiva *e-Commerce*. I dubbi in questione hanno condotto, in particolare, alla creazione per via giurisprudenziale di una nuova categoria di *hosting provider* definiti «attivi» in quanto, a differenza di quelli tradizionali che svolgono compiti meramente tecnici e passivi, intervengono attivamente sulle informazioni e sui contenuti caricati dagli utenti[18]. Per tali ragioni essi non ricadrebbero, quindi,

---

[15] V. *ex multis*: O. POLLICINO, *op. cit.* 12; R. BOCCHINI, *La responsabilità di facebook per la mancata rimozione di contenuti illeciti*, in Giur.it., fasc. 3, pp. 632-656, 2017; G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell'hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo*, in federalismi.it, n. 2, pp. 108-147, 2020. Accessibile online: https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=40904.

[16] V. ad esempio le comunicazioni della Commissione Europea citate *supra* n. 7.

[17] V. giurisprudenza citata *infra* n. 20

[18] COM(2017) 555 final, p. 11.

nel campo di applicazione del regime di «*safe harbour*» stabilito dalla direttiva[19].

La figura dell'*hosting provider* attivo è, come detto, di creazione giurisprudenziale e ha iniziato ad affacciarsi in alcune pronunce della Corte di Giustizia dell'Unione europea[20], per essere poi recepita anche a livello interno[21].

Rinviando ad altri autori[22] per un'analisi più completa dei profili strettamente civilisti relativi alla responsabilità di tali soggetti, è opportuno qui chiarire come la giurisprudenza dell'Unione non sia pervenuta ad una definizione

---

[19] A questo proposito si veda il considerando 42 della Direttiva 2000/31/CE, secondo cui: «Le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate».

[20] La creazione giurisprudenziale della figura dell'*hosting provider* attivo ha avuto inizio con il *leading case* CGUE, cause riunite da C-236/08 a C-238/08, *Google France SARL e Google Inc.* c. *Louis Vouitton Malletier SA*, *Google France SARL* c. *Viaticum SA e Luteciel SARL*, *Google France SARL* c. *Centre National de recherche en relations humaines (CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL*, 23 marzo 2010. Le indicazioni della Corte di Giustizia sono state ribadite e meglio specificate in alcune pronunce successive, tra cui: CGUE, causa C-324/09, *l'Oréal SA e altri*. c. *eBay International AG*, 12 luglio 2011; CGUE, C-291/13 *Sotiris Papasavvas* c. *O Fileleftheros Dimosia Etaireia Ltd, Takis Kounnafi, Giorgos Sertis*, 11 settembre 2014; CGUE, causa C-610/15, *Stichting Brein* c. *Ziggo BV*, *XS4ALL Internet BV*, 14 giugno 2018 – ECLI:EU:C:2017:456; CGUE, causa C-521/17, *Coöperatieve Vereniging SNB-React U.A*. c. *D.M.*, 7 agosto 2018. Per una panoramica si veda S. SICA, *Giurisprudenza nazionale ed europea e frammentazione legislativa della responsabilità civile del provider*, in A.M. MANCALEONI, E. POILLOT (a cura di), *National Judges and the Case Law of the Court of Justice of the European Union*, pp. 205-222, Roma Tre-Press, 2021.

[21] V. in particolare le sentenze Cass. Sez. I Civ. n. 7708, 19 marzo 2019 e Cass. Sez. I Civ. n. 7709, 19 marzo 2019. Per alcuni commenti sul punto vedi: G. D'ALFONSO, *op. cit.* n. 15; F. FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma la distinzione tra attivo e passivo*, in filodiritto.it, 18 aprile 2019, accessibile online: https://www.filodiritto.com/responsabilita-dellhosting-provider-la-cassazione-conferma-la-distinzione-tra-attivo-e-passivo.

[22] V. *ex multis*: O. POLLICINO, *op. cit.* 12; R. BOCCHINI, *op. cit.* 15; G.M. RICCIO, *La responsabilità civile degli internet service providers*, Giappichelli, 2002; G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service providers*, in S. SICA, P. STANZIONE (a cura di), *Commercio elettronico e categorie civilistiche*, pp. 368ss, Giuffrè, 2002; V. ZENO-ZENCOVICH, *Profili attivi e passivi della responsabilità dell'utente in Internet*, in A. PALAZZO, U. RUFFOLO (a cura di), *La tutela del navigatore in Internet*, pp. 137-144, Giuffrè, 2002; E. TOSI, *Responsabilità civile degli hosting*

generale di «*hosting provider* attivo». Al contrario, i Giudici di Lussemburgo hanno più volte ribadito[23] come occorra effettuare una valutazione caso per caso volta a determinare se il prestatore di servizi considerato svolga attività «di ordine meramente tecnico, automatico e passivo», non conoscendo né controllando le informazioni trasmesse o memorizzate dai propri utenti, ovvero abbia un «ruolo attivo» con riguardo a dette informazioni.

L'orientamento della Corte di Giustizia è stato di recente condiviso anche a livello interno dalla Corte di Cassazione[24] che, sulla scia di alcuni precedenti di merito[25], ha elencato, a livello esemplificativo, una serie di «indici di interferenza» idonei a delineare la figura dell'*hosting provider* attivo. Gli indici in questione, da accertare in concreto, altro non sono che «condotte che abbiano, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati». Tali condotte sono rappresentate dalle «attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione».

La presenza di tali «indici di interferenza» sarebbe quindi idonea, secondo la giurisprudenza ormai maggioritaria, ad escludere la qualifica di «passivo» in

---

provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilità ex post, in Il diritto degli affari, fasc. 1, 2020, pp. 1-24.

[23] V. giurisprudenza citata al precedente n. 20. Inoltre, si veda CGUE causa C-521/17, *Coöperatieve Vereniging SNB-REACT U.A.* c. *Deepak Mehta*, punti 44-50.

[24] V. giurisprudenza citata sub nota 21.

[25] V., nel medesimo filone della Cassazione citata, Tribunale di Milano, Sez. spec. prop. Industriale, R.G. 79619/2009, e intellettuale, sentenza del 9 settembre 2011, n. 10893. Per una panoramica sulla giurisprudenza di merito relativa all'*hosting provider* attivo si vedano: E. TOSI, *op. cit.* n. 22; E. TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in Rivista di Diritto Industriale, fasc. 1, 2017, pp. 3-122.

capo ad un *hosting provider*, privandolo di conseguenza dell'esenzione di responsabilità di cui all'art. 14 della Direttiva e-Commerce (cui corrisponde in Italia l'art. 16 D.lgs. 70/2003).

Non mancano peraltro in dottrina le critiche a tale evoluzione, in particolare da parte di chi, facendo leva sulla mancanza di una norma che riconosca esplicitamente la figura dell'*hosting provider* attivo nell'ordinamento dell'Unione, denuncia i rischi di una mancanza di certezza frutto di quella che viene definita come una «forzatura del dato legislativo[26]». Allo stesso modo, vi è chi sottolinea il rischio di una progressiva sostanziale erosione del regime di *safe harbour* per la maggior parte dei fornitori di servizi di memorizzazione[27]. Rischio che, da parte di certa dottrina italiana[28], viene ricollegato ad un'attività della giurisprudenza nazionale giudicata suscettibile di condurre ad una *interpretatio abrogans* della disciplina dell'Unione. Argomenta infatti tale dottrina che, considerando le attività concretamente svolte da tutti gli *hosting provider*, sarebbe quasi sempre possibile riscontrare quel *quid pluris* che dovrebbe, secondo l'indirizzo evolutivo appena poc'anzi esaminato, portare alla qualifica di *hosting provider* attivo.

2.3 Dall'irresponsabilità degli *hosting provider* verso un sistema basato sulla «*accountability*». L'esempio della Direttiva (UE) 2019/790

Dall'analisi appena svolta emerge una tendenza evolutiva dell'ordinamento dell'Unione europea – ma come si è visto anche di quello italiano – a considerare alcuni fornitori di servizi di *hosting* non più come soggetti irresponsabili ma come soggetti che, per via del loro sempre più crescente ruolo di controllo

[26] O. POLLICINO, *op. cit.* n. 12, p. 55.
[27] M. BASSINI, *La Cassazione e il simulacro del provider attivo: mala tempora currunt*, in Media Laws, n. 2, pp. 248-257, 2019, accessibile online: https://www.medialaws.eu/la-cassazione-e-il-simulacro-del-provider-attivo-mala-tempora-currunt/.
[28] V. R. BOCCHINI, *op. cit.* n. 15; M. BASSINI, *op. cit.* n. 27.

ed utilizzo dei contenuti e delle informazioni degli utenti, possano rispondere[29] della relativa illiceità.

La tendenza in questione si è concretizzata, oltre che nel consolidato orientamento giurisprudenziale di cui si è poc'anzi detto, anche in una serie di comunicazioni[30], raccomandazioni[31] e proposte[32] della Commissione europea volte a promuovere un regime basato sulla progressiva responsabilizzazione degli *hosting provider*, ed in particolare delle piattaforme, per quanto riguarda i contenuti illeciti condivisi dai propri utenti. Proposte che sono poi sfociate in strumenti normativi adottati dai colegislatori dell'Unione, come il RegolamentoP2B o il Digital Services Act, che fanno leva spesso sulla capacità di autoregolamentazione delle piattaforme e sulla collaborazione tra le stesse e gli Stati membri e dei quali si dirà meglio nel prosieguo (v. *infra*: par. 3; Cap. 6).

Innanzi tutto, esemplificativo di questa tendenza sembra essere quanto previsto dalla Direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale[33] in materia di responsabilità dei «prestatori di servizi di condivisione di contenuti online[34]» per la diffusione illecita di contenuti protetti dalle regole sul diritto d'autore.

---

[29] V. dottrina citata sub n. 22.

[30] V. comunicazioni citate sub. 7

[31] V. in particolare la Raccomandazione (UE) 2018/334 della Commissione, del 1° marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online, adottata a seguito della menzionata comunicazione COM(2017) 555 final del 28 settembre 2017.

[32] Vedi il Digital Services Act Package già citato al Cap. 1, par. 4.

[33] Nome completo: 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, apparsa in *GU L 130 del 17.5.2019, pagg. 92–125*.

[34] Definizione contenuta all'art. 2, n. 6) della Direttiva (UE) 2019/790, ai sensi della quale per «prestatore di servizi di condivisione di contenuti online»: si intende «un prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro. I prestatori di servizi quali le enciclopedie online senza scopo di lucro, i repertori didattici o scientifici senza scopo di lucro, le piattaforme di sviluppo di e condivisione di software open source, i fornitori di servizi di comunicazione elettronica ai sensi della direttiva (UE) 2018/1972, i mercati online, i servizi *cloud* da impresa a impresa e i servizi cloud che

La direttiva in questione, approvata al termine di un lungo negoziato politico e recepita in Italia con il D.lgs. 177/2021, contiene, infatti, delle disposizioni sul punto fortemente improntate alla «responsabilizzazione» dei suddetti fornitori («*online content-sharing service provider*» secondo la dicitura in inglese), tra cui si annoverano piattaforme come YouTube o Spotify.

La norma cardine su cui poggia il nuovo sistema di responsabilità è l'art. 17. Innanzi tutto, tale articolo dispone, al primo paragrafo, che un prestatore di spazi di condivisione *online* che voglia comunicare o mettere a disposizione del pubblico opere tutelate dal diritto d'autore o altri materiali protetti forniti dai propri utenti debba ottenere la previa autorizzazione dei titolari di tali diritti, ad esempio tramite accordi di licenza. L'autorizzazione in questione vale, ai sensi del par. 2, anche per gli utenti dello spazio da esso gestito (si pensi ancora una volta a YouTube), a condizione che questi non agiscano a fini commerciali o che la loro attività non generi ricavi significativi.

A tutela del predetto requisito, l'art. 17, par. 3 prevede espressamente che per i prestatori considerati dalla norma in commento non si applichi il regime di limitazione della responsabilità di cui all'art. 14 della Direttiva 2000/31/CE, cristallizzando con riguardo ad essi i principi stabiliti dalla giurisprudenza relativa alla figura dell'*hosting provider* attivo.

Di contro, il successivo art. 17, par. 4 sancisce esplicitamente come tali fornitori debbano essere considerati «responsabili» per la condivisione non autorizzata di materiale protetto dal diritto d'autore. La responsabilità in questione sussiste *ipso facto*[35], anche se un *provider* può andarne esente nel caso in cui dimostri congiuntamente di: (a) aver compiuto i massimi sforzi per ottenere un'autorizzazione; (b) aver compiuto, secondo «elevati standard di diligenza

consentono agli utenti di caricare contenuti per uso personale non sono prestatori di servizi di condivisione di contenuti online ai sensi della presente direttiva»

[35] G. D'ALFONSO, *op. cit.* n. 15, p. 139.

professionale di settore», i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso (c) aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai propri siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro, secondo quanto previsto dalla lettera b).

Le richiamate ipotesi di esenzione, definite da parte della dottrina[36] come uno specifico «*safe harbour*», appaiono sintomatiche di un nuovo approccio del legislatore dell'Unione basato sulla progressiva responsabilizzazione (o «*accountability*», come si è già avuto modo di preferire) degli *hosting provider* e delle piattaforme digitali.

Questo approccio, nel caso della nuova Direttiva Copyright, si basa innanzi tutto sull'obbligo dei fornitori di servizi di condivisione di contenuti online di fare quanto possibile per prevenire a monte una violazione del diritto d'autore attraverso un atteggiamento proattivo che si concretizzi negli sforzi e nei doveri diligenza di cui abbiamo appena dato conto. Come nel caso della Direttiva e-Commerce[37], non sono, peraltro, previsti degli obblighi generali di sorveglianza, al contrario esplicitamente esclusi dall'art. 17, par. 8.

Ai nostri fini, va segnalato inoltre come la direttiva del 2019 sembri perseguire l'obiettivo della «responsabilizzazione» dei *provider* anche facendo leva sulla loro «dimensione istituzionale».

---

[36] N.E. CURTO, *EU Directive on Copyright in the Digital Single Market and ISP Liability: What's Next at International Level?*, in Case Western Reserve Journal of Law, Technology and the Internet, Vol. 11, n. 3, pp.84-110, 2020, p. 91.

[37] Vedi in particolare il considerando 48 ed il già citato art. 15 della Direttiva 2000/31/CE

Ciò, in particolare, pare emergere dall'art. 17, par. 9, il quale stabilisce che i prestatori di servizi di condivisione di contenuti online debbano istituire «un meccanismo di reclamo e ricorso celere ed efficace che sia disponibile agli utenti dei loro servizi in caso di controversie in merito alla disabilitazione dell'accesso a, o alla rimozione di, specifiche opere o altri materiali da essi caricati». La norma continua quindi nel delineare le caratteristiche che tali meccanismi devono avere, tra cui si menzionano la celerità, l'effettività e le necessità di una verifica umana per qualsiasi decisione volta a disabilitare l'accesso o a rimuovere i contenuti forniti dagli utenti.

A parere di chi scrive, questa norma costituisce un esempio di tentativo del legislatore europeo di raggiungere i propri obiettivi stabilendo un regime di collaborazione con le piattaforme digitali. A queste ultime, infatti, la direttiva demanda in parte il compito di tutelare il diritto d'autore attraverso il controllo e la rimozione dei contenuti non autorizzati diffusi *online*. Attività che, per ragioni tecniche e di prossimità, le piattaforme risultano essere i soggetti più indicati a svolgere e che, peraltro, devono avvenire garantendo il rispetto dei diritti e delle libertà di espressione[38] degli utenti attraverso dei meccanismi di reclamo che assomigliano a dei sistemi di *alternative dispute resolution* interni alla piattaforma e che, come vedremo meglio nel prosieguo (v. *infra*: par. 3.1, Cap. 6, par. 4.3.1), vengono sempre più spesso previsti dal legislatore europeo.

La bontà di una simile ipotesi pare confermata dal terzo comma del medesimo art. 17, par. 9, che pone in capo ai prestatori di servizi di condivisione dei precisi obblighi di trasparenza. Questi hanno, infatti, il dovere di informare i propri utenti «della possibilità di utilizzare opere e altri materiali conformemente alle eccezioni o limitazioni al diritto d'autore e ai diritti connessi previste dal diritto dell'Unione». Il mezzo attraverso cui adempiere a tale obbligo

[38] Vedi a questo proposito il considerando 70 della Direttiva (UE) 2019/790

sono i «termini e condizioni» dei prestatori, che altro non sono che lo strumento contrattuale che regola il rapporto tra gli stessi ed i propri utenti.

Un simile approccio sembra implicare il riconoscimento, da parte del legislatore europeo, della dimensione istituzionale (o quanto meno di una forma rilevante di autonomia normativa) degli *online content-sharing service provider*, che paiono assurgere, con riguardo alla diffusione di contenuti tutelati dal diritto d'autore, a veri e propri arbitri degli spazi da essi gestiti.

Tale riconoscimento, peraltro, non significa affatto, nell'ottica del legislatore dell'Unione, una parificazione delle piattaforme ai tradizionali attori statali. Lo stesso art. 17, par. 9 è infatti chiaro nell'obbligare gli Stati membri a stabilire dei meccanismi stragiudiziali per la «risoluzione imparziale» delle controversie e a garantire agli utenti l'accesso alla tutela in via giudiziaria.

Preferibile sembra invece la tesi secondo cui il legislatore dell'Unione, riconoscendo la dimensione istituzionale delle piattaforme, cerchi di cooperare coi relativi gestori utilizzando la suddetta dimensione per il raggiungimento dei propri obiettivi e, in tale ottica, responsabilizzando sempre di più i gestori, anche allo scopo di contrastarne lo strapotere regolatorio all'interno dell'ambiente virtuale.

3 I nuovi paradigmi regolatori alla luce della Digital Single Market Strategy

Come accennato nel Capitolo I (v. *infra*: Cap. 1, par. 4), le piattaforme digitali rivestono un'importanza centrale nell'ambito della Digital Single Market Strategy, ossia la strategia politico-regolatoria intrapresa dalla Commissione europea per la valorizzazione del mercato digitale all'interno dell'Unione, che ha preso ufficialmente il via con una Comunicazione[39] del maggio 2015. Si tratta

[39] Si tratta della già citata Comunicazione della Commissione europea, COM(2015) 192 final, su cui v. nota sub Cap. 1 n. 52.

di un progetto ambizioso, la cui totale realizzazione, secondo le intenzioni della Commissione, all'epoca guidata da Jean-Claude Juncker, era stata stimata[40] in un aumento del Pil dell'Unione europea da 415 miliardi di euro.

Sin dalla prima comunicazione, infatti, la disciplina delle piattaforme – anche con riferimento al contrasto alla diffusione di contenuti illeciti su internet – è stata esplicitamente menzionata tra i temi di interesse del «secondo pilastro[41]» su cui si fonda la strategia, ossia la creazione di un «contesto favorevole affinché le reti e i servizi digitali possano svilupparsi». A tal riguardo, la Commissione ha anticipato lo svolgimento di una valutazione globale sul ruolo delle piattaforme nel mercato digitale, partendo da temi come la trasparenza, l'uso che le piattaforme fanno delle informazioni che raccolgono, le relazioni tra piattaforme e fornitori/prestatori, la capacità delle persone e delle imprese di lasciare una piattaforma a favore di un'altra e la ricerca di soluzioni per il contrasto alla diffusione di contenuti illeciti su internet.

[40] V. ivi a pag. 3 e, più nel dettaglio, l'allegato Commission Staff Working Document, *A Digital Single Market Strategy for Europe - Analysis and Evidence*, SWD(2015) 100 final, 6 maggio 2015, a pag. 5.

[41] I tre pilastri su cui si fonda la strategia sono: «(1) migliorare l'accesso online ai beni e servizi in tutta Europa per i consumatori e le imprese – questo implica l'eliminazione in tempi rapidi delle differenze fondamentali che separano il mondo online dal mondo offline al fine di abbattere le barriere che bloccano l'attività online attraverso le frontiere; (2) creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi – questo implica la disponibilità di infrastrutture e di servizi contenutistici ad alta velocità protetti e affidabili, sostenuti da condizioni regolamentari propizie all'innovazione, agli investimenti, alla concorrenza leale e alla parità di condizioni; (3) massimizzare il potenziale di crescita dell'economia digitale europea – questo implica investimenti nelle infrastrutture e tecnologie delle TIC, come le nuvole informatiche (*cloud computing*) e i megadati (*big data*), ricerca e innovazione per rafforzare la competitività industriale e miglioramento dei servizi pubblici, dell'inclusione e delle competenze» – v. COM(2015) 192 final, pag. 3.

In seguito, la Commissione ha emanato altre comunicazioni[42] più specifiche rivolte alle piattaforme. Tra queste va in particolare menzionata la Comunicazione[43] del 2016 sulle piattaforme online e il mercato unico digitale, in cui l'Esecutivo dell'Unione ha meglio delineato la propria strategia regolatoria nei confronti di tali soggetti. A tal proposito, è bene notare sin da ora come la Commissione abbia sottolineato la necessità di un quadro normativo più uniforme a livello di Unione, dal momento che «affinché l'Europa possa sfruttare appieno i vantaggi dell'economia delle piattaforme e stimolare la crescita delle *start-up* europee del settore, è evidente che in un mercato unico non possono esistere 28 diversi quadri normativi in materia di piattaforme online[44]». A parere della Commissione, infatti, «la presenza di norme differenti a livello nazionale (o addirittura locale) in materia di piattaforme online crea incertezza per gli operatori economici, limita la disponibilità dei servizi digitali e ingenera confusione negli utenti e nelle aziende». Di contro, l'Esecutivo ha sottolineato l'importanza di norme armonizzate a livello UE, come il GDPR.

In tale comunicazione la Commissione ha inoltre indicato esplicitamente i seguenti principi su cui si basa la sua strategia in materia di piattaforme: (1) pari condizioni concorrenziali per servizi digitali comparabili; (2) condotte responsabili da parte delle piattaforme online a tutela dei valori fondamentali; (3) trasparenza e correttezza per conservare la fiducia degli utenti e salvaguardare l'innovazione; (4) mercati aperti e non discriminatori nel quadro di un'economia fondata sui dati.

---

[42] V. Comunicazioni citate sub nota 7. V. altresì: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un'agenda europea per l'economia collaborativa*, COM(2016) 356 final, 2 giugno 2016.

[43] COM(2016) 288 final, *cit.* n. 7.

[44] V. ivi a pag. 5. Si chiarisce come, a seguito del recesso del Regno Unito dall'Unione Europea (c.d. Brexit) il riferimento a «28 quadri normativi diversi» vada ora inteso a 27.

A tutela del ruolo innovativo delle piattaforme, la Comunicazione ha poi chiarito come le misure normative future proposte a livello di UE dovranno trattare soltanto «problemi chiaramente circoscritti relativi a un tipo specifico di piattaforme online o a un'attività specifica che queste svolgono[45]», evitando quindi regolamentazioni generali.

Infine, come avremo modo di vedere meglio *infra* (v. Cap. 4, par. 3), la Commissione ha posto enfasi, oltre che sulla trasparenza e sulla *accountability*, sull'importanza sempre più crescente dell'auto-regolamentazione o della co-regolamentazione delle piattaforme[46], compresi gli strumenti del settore idonei a garantire l'applicazione dei requisiti legali, nonché gli adeguati meccanismi di monitoraggio. Tali meccanismi, in particolare, vengono considerati la chiave per far sì che le menzionate misure di *self-regulation* o *co-regulation* «possano conseguire il giusto equilibrio tra le esigenze di prevedibilità, flessibilità ed efficienza e la necessità di sviluppare soluzioni a prova di futuro[47]».

Enfasi sulla trasparenza e sulla responsabilizzazione delle piattaforme, oltre che sulla cooperazione tra le stesse e le autorità pubbliche, è stata posta anche nella già menzionata[48] comunicazione relativa al contrasto alla diffusione di contenuti illeciti su internet, così come nelle raccomandazioni[49] adottate a seguito della stessa. Anche su questo tema avremmo modo di tornare nel prosieguo del presente lavoro (v. *infra*: Cap. 5).

---

[45] COM(2016) 288 final, p. 5. Tra i settori viene citata anche l'economia collaborativa, su cui v. *infra*.

[46] Rinviando a *infra* (Cap. 4, par. 3) per un'analisi più compiuta sulla strategia regolatoria intrapresa dalla Commissione e sul ruolo assunto in essa dalla regolamentazione privata, si menzionano sin da ora le seguenti opere bibliografiche: M. CANTERO GAMITO, *op. cit.* Cap. 1, n. 19; M. FINCK, *Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy*, in LSE Law, Society and Economy Working Papers, n. 15, London School of Economics and Political Science Law Department, 2017. Disponibile online al seguente link: http://eprints.lse.ac.uk/87568/

[47] COM (2016) 288 final, p. 6.

[48] V. *supra* n. 30.

[49] V. *supra* n. 31

Allo stesso modo, torneremo in seguito (v. *infra*: Cap. 6), ad ideale conclusione di questo lavoro e con uno sguardo inevitabilmente proteso al futuro, sul Digital Services Act.

3.1 Il Regolamento (UE) 2019/1150 e la tutela degli utenti commerciali delle piattaforme digitali

Tra le iniziative legislative in materia di piattaforme assunte dalla Commissione europea nell'ambito della Digital Single Market Strategy va menzionata la proposta[50] del 2018 da cui è poi scaturito il Regolamento (UE) 2019/1150 del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (ribattezzato «Regolamento P2B», dove la «P» sta per «Platform» e la «B» sta per «Business»).

Si tratta del primo strumento[51], nell'ordinamento dell'Unione europea, specificamente rivolto alla disciplina delle piattaforme digitali, pur non essendo queste ultime incluse tra le definizioni[52] e preferendo invece il regolamento concentrarsi sulla nozione di «servizi di intermediazione online[53]». Questa

---

[50] Commissione europea, COM(2018) 238 final, *Proposta di Regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online*, 26 aprile 2018.

[51] P. FRANZINA, *Promoting Fairness and Transparency for Business Users of Online Platforms: The Role of Private International Law* in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 147-152, Schulthess, 2018; A. PALMIERI, *Profili giuridici delle piattaforme digitali – La tutela degli utenti commerciali e dei titolari di siti web aziendali*, Giappichelli, 2019; T. PRASTITOU-MERDI, *The Notion of "Online Intermediation Services" Found in the New EU Platform Regulation: Who Is Caught After All?*, in T. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU-MERDI (a cura di), *EU Internet Law in the Digital Single Market*, pp. 543-560, Springer, 2021.

[52] La parola «piattaforme» compare comunque per tredici volte all'interno del Regolamento P2B: undici nei considerando e due all'art. 18 (sulla revisione dello strumento normativo). Ogni volta appare all'interno della locuzione «economia delle piattaforme online».

[53] Ai sensi dell'art. 2, n. 2) del Regolamento P2B sono «servizi di intermediazione online»: «servizi che soddisfano tutti i seguenti requisiti: a) sono servizi della società dell'informazione ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio; b) consentono agli utenti commerciali di offrire beni o servizi ai consumatori, con l'obiettivo di facilitare l'avvio di transazioni dirette tra tali utenti commerciali e

scelta lascia peraltro irrisolti diversi problemi qualificatori relativi alla natura delle piattaforme stesse, di cui si dirà a breve (v. *infra*: par. 4).

Lo scopo del Regolamento P2B è, secondo quanto previsto dall'art. 1, par. 1, «garantire che gli utenti commerciali di servizi di intermediazione online e gli utenti titolari di siti web aziendali che siano in relazione con motori di ricerca online dispongano di un'adeguata trasparenza, di equità e di efficaci possibilità di ricorso». A tal fine esso stabilisce norme a tutela di soggetti professionali – «utenti commerciali[54]» e «titolari di siti web aziendali[55]» – che fanno ricorso ai «servizi di intermediazione online» o ai «motori di ricerca online» per offrire i propri beni o servizi ai consumatori attraverso internet (inclusa, secondo taluni[56], la semplice attività di pubblicità). Il Regolamento P2B, infatti, riconosce lo squilibrio esistente[57] nelle relazioni tra gestori di piattaforme ed utenti commerciali (per semplicità ci si riferirà nel prosieguo soltanto a queste sapendo che, ove non esplicitamente indicato, le considerazioni svolte valgono anche

---

i consumatori, a prescindere da dove sono concluse dette transazioni; c) sono forniti agli utenti commerciali in base a rapporti contrattuali tra il fornitore di tali servizi e gli utenti commerciali che offrono beni e servizi ai consumatori».

[54] L'art. 2, n. 1) del Regolamento P2B definisce «utente commerciale»: «un privato che agisce nell'ambito delle proprie attività commerciali o professionali o una persona giuridica che offre beni o servizi ai consumatori tramite servizi di intermediazione online per fini legati alla sua attività commerciale, imprenditoriale, artigianale o professionale».

[55] L'art. 2, n. 7) del Regolamento P2B definisce «utente titolare di sito web aziendale»: «persona fisica o giuridica che usa un'interfaccia online, vale a dire un software, inclusi un sito web o una parte di esso e applicazioni, incluse le applicazioni mobili, per offrire beni o servizi ai consumatori per fini legati alla sua attività commerciale, imprenditoriale, artigianale o professionale».

[56] C. TWIGG-FLESNER, *The EU's Proposals for Regulating B2B Relationships on online platforms – Transparency, Fairness and Beyond*, in Journal of European Consumer and Markets Law, Vol. 7, n. 6, pp. 222-233, 2018. Disponibile su SSRN: https://ssrn.com/abstract=3253115. V. in particolare a p. 225.

[57] Cfr. considerando 2: «[…] l'incremento delle intermediazioni delle transazioni attraverso i servizi di intermediazione online […] conduce a un aumento della dipendenza da tali servizi degli utenti commerciali […] per raggiungere i consumatori. Dato l'aumento della dipendenza, i fornitori di tali servizi spesso hanno un potere contrattuale superiore, che consente loro di agire di fatto unilateralmente in un modo che può essere iniquo e quindi dannoso per gli interessi legittimi dei loro utenti commerciali e, indirettamente, anche dei consumatori dell'Unione […]».

per i rapporti tra titolari di siti web aziendali e motori di ricerca) e tenta di porvi rimedio prendendo le difese delle parti deboli.

Rinviando ad altri autori[58] per un'analisi dettagliata delle disposizioni che compongono il Regolamento P2B, ci si soffermerà di seguito sugli aspetti dello stesso rilevanti per lo scopo della nostra indagine. Per quanto riguarda le implicazioni più squisitamente di diritto internazionale privato[59] si rimanda invece a *infra* (Cap. 3, par.5.2).

Ai nostri fini, occorre innanzi tutto segnalare come il Regolamento P2B, similmente alla Direttiva Copyright, fondi gran parte della propria strategia sulla conformazione dei «termini e condizioni» che regolano i rapporti contrattuali tra gli utenti commerciali e le piattaforme e che, indipendentemente da come sono nominati, hanno il loro elemento distintivo nell'essere determinati unilateralmente dalle piattaforme stesse. A tal fine, l'art. 3, par. 2 richiede – a pena di nullità (art. 3, par. 3) – che essi siano redatti con un linguaggio «chiaro, semplice e comprensibile» (lett. a)) e che siano facilmente reperibili dagli utenti commerciali per tutto il rapporto con la piattaforma (lett. b)). Sempre per ragioni di trasparenza, la norma prosegue nell'imporre che i «termini e condizioni» indichino le ragioni che possono giustificare la decisione del *provider* di una piattaforma di sospendere, cessare o limitare in altro modo, in tutto o in parte, la fornitura dei propri servizi agli utenti commerciali, escludendoli pertanto dalla piattaforma stessa.

Le disposizioni successive indicano ulteriori elementi che devono essere presenti nei «termini e condizioni» delle piattaforme. Tra essi vanno menzionati i

---

[58] V. in particolare: P. FRANZINA, *op. cit.* n. 51; A. PALMIERI, *op. cit.* n. 51; T. PRASTITOU-MERDI, *op. cit.* n. 51; C. TWIGG-FLESNER, *op. cit.* n. 56; C. BUSCH, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in A. DE FRANCESCHI, R. SCHULZE (a cura di) *Digital revolution - new challenges for law: data protection, artificial intelligence, smart products, blockchain technology and virtual currencies*, pp. 57-75, C.H. Beck-Nomos, 2019.

[59] Su questo tema si veda in modo particolare P. FRANZINA, *op. cit.* n. 51.

parametri che determinano il «posizionamento[60]» dei beni e dei servizi degli utenti commerciali all'interno della piattaforma o del motore di ricerca (art. 5), una descrizione del tipo di «prodotti o servizi accessori[61]» offerti dal *provider* di una piattaforma (o da terzi) attraverso il proprio servizio di intermediazione (art. 6) ed una in merito a qualunque trattamento differenziato che un *provider* riservi o possa riservare ai prodotti o ai servizi offerti dello stesso o da utenti commerciali da esso controllati (art. 7). L'art. 8 richiede invece che i fornitori non impongano (salvo eccezioni specificamente elencate) modifiche retroattive dei «termini e condizioni» ed inseriscano in questi delle informazioni sulle condizioni alle quali gli utenti commerciali possono risolvere la propria relazione contrattuale con essi, oltre che una descrizione relativa all'accesso tecnico e contrattuale alle informazioni fornite o generate dall'utente commerciale che questi conservino al termine del rapporto contrattuale. Sempre sull'accesso ai dati sono presenti degli specifici obblighi di trasparenza al successivo art. 9, con la precisazione che tale norma non pregiudica gli altri testi europei in materia di protezione dei dati personali[62]. L'art. 10, infine, richiede ai fornitori di indicare nei propri «termini e condizioni» le ragioni di eventuali limitazioni della capacità degli utenti commerciali di offrire i propri prodotti e servizi a condizioni differenti tramite mezzi diverse dalle piattaforme stesse.

---

[60] L'art. 2, n. 8) del Regolamento P2B definisce «posizionamento»: «la rilevanza relativa attribuita ai beni o ai servizi offerti mediante i servizi di intermediazione online, o l'importanza attribuita ai risultati della ricerca da motori di ricerca online, come illustrato, organizzato o comunicato, rispettivamente, dai fornitori di servizi di intermediazione online o dai fornitori di motori di ricerca online a prescindere dai mezzi tecnologici usati per tale presentazione, organizzazione o comunicazione».

[61] L'art. 2, n. 11) del Regolamento P2B definisce «prodotti e servizi accessori»: «prodotti e servizi offerti al consumatore prima del completamento di una transazione avviata sui servizi di intermediazione online, in aggiunta e in modo complementare rispetto al prodotto o servizio principale offerto dall'utente commerciale attraverso i servizi di intermediazione online»;

[62] L'art. 9, par. 3 fa esplicitamente salvi il Regolamento (UE) 2016/679, la Direttiva (UE) 2016/680 e la direttiva 2002/58/CE.

Altra tecnica utilizzata dal Regolamento P2B è quella della «proceduralizzazione[63]» di alcune condotte dei fornitori delle piattaforme. È un esempio di ciò l'art. 3 che, mentre non prevede alcun requisito di tipo sostanziale per le modifiche unilaterali dei «termini e condizioni», richiede il rispetto di un periodo di preavviso per la comunicazione delle stesse agli utenti commerciali, ai quali peraltro corrisponde un diritto di recesso (art. 3, par. 2). Ancora più marcato è a questo proposito l'art. 4, che stabilisce una serie di requisiti procedurali a cui i fornitori devono attenersi in materia di limitazione, sospensione e cessazione della fornitura dei propri servizi agli utenti commerciali. In particolare, è fatto obbligo ai *provider* di comunicare le proprie decisioni con un preavviso di trenta giorni e di fornire sempre una motivazione.

L'obbligo di motivazione, oltre che essere sorretto da ragioni di trasparenza, serve a garantire agli utenti la possibilità di «chiarire i fatti e le circostanze» a sostegno delle proprie ragioni nell'ambito di un sistema interno di gestione dei reclami che i fornitori delle piattaforme – ancora una volta analogamente a quanto previsto dall'art. 17 della Direttiva Copyright – sono obbligati a stabilire ai sensi del successivo art. 11.

Il meccanismo in questione è uno degli aspetti chiave del Regolamento P2B. Esso serve, in particolare, a permettere agli utenti di presentare ai fornitori delle piattaforme reclami in merito a questioni relative ad inadempimenti degli obblighi del Regolamento P2B, problemi tecnologici e misure o comportamenti adottati dai *provider* e direttamente connessi alla fornitura dei servizi di intermediazione online (art. 11, par. 2). L'art. 11 non stabilisce particolari requisiti sulla procedura per la gestione dei reclami ma si limita a sancire che i

[63] C. BUSCH, *The P2B Regulation (EU) 2019/1150: Towards a "procedural turn" in EU platform regulation?*, in Journal of European Consumer and Market Law, Vol. 9, n. 4, 2020, pp. 133-134.

sistemi in questione debbano basarsi sui principi della trasparenza e della parità di trattamento a parità di situazione, ponendo inoltre enfasi sulla rapidità delle decisioni e sull'attenzione che le piattaforme devono avere nella gestione e nella risoluzione dei reclami.

Va chiarito infine come i sistemi di gestione dei reclami appena descritti, pur rivestendo un'importanza decisiva nell'economia del regolamento, non esauriscono gli strumenti a tutela degli utenti commerciali. Accanto ad essi, infatti, l'art. 12 prevede che i fornitori delle piattaforme indichino – sempre nei propri «termini e condizioni» – due o più mediatori allo scopo di addivenire alla risoluzione stragiudiziale delle controversie insorte con gli utenti commerciali. A tutela di questi ultimi è inoltre previsto che i *provider* si facciano carico di «una parte ragionevole» dei costi della mediazione.

Tanto i reclami interni quanto la mediazione non pregiudicano, peraltro, il diritto degli utenti commerciali e dei fornitori di tutelare le proprie ragioni in sede giudiziaria (art.12, par. 5). A tal proposito, è opportuno aggiungere come l'art. 14 preveda una speciale legittimazione ad agire[64] in capo ad associazioni o organizzazioni rappresentative degli interessi degli utenti commerciali, così come ad organismi pubblici istituiti all'interno dei vari Stati membri.

[64] Secondo il considerando 44, tale legittimazione serve a garantire l'efficace applicazione del Regolamento P2B e la tutela degli utenti commerciali. Lo stesso considerando 44 afferma infatti che: «Vari fattori, come i mezzi finanziari limitati, il timore di ritorsioni e la scelta esclusiva del diritto e del foro imposta nei termini e nelle condizioni, possono limitare l'efficacia delle possibilità di ricorso giudiziale esistenti, particolarmente quelle che richiedono agli utenti commerciali o agli utenti titolari di siti web aziendali di agire individualmente e palesando la propria identità […]».

…*Segue*: La dimensione istituzionale e la «responsabilizzazione» dei fornitori delle piattaforme nel Regolamento P2B

L'analisi appena svolta ci permette di sviluppare alcune ulteriori considerazioni sulla dimensione istituzionale delle piattaforme e sulla più volte richiamata strategia di «responsabilizzazione» dei loro fornitori intrapresa dal legislatore dell'Unione.

Innanzi tutto, occorre rilevare come il fatto che il Regolamento P2B imponga ai fornitori di piattaforme di stabilire un sistema interno di gestione dei reclami degli utenti commerciali sembri riconoscere che questi agiscano, all'interno degli ambienti da essi gestiti, come dei veri e propri regolatori privati, assumendo su talune questioni anche delle funzioni di tipo para-giurisdizionale[65].

Questo ruolo appare peraltro valorizzato dal Regolamento P2B, in quanto i fornitori delle piattaforme vengono considerati come i soggetti più adatti a cui gli utenti possono rivolgersi per avere accesso a «possibilità di ricorso immediate, idonee ed efficaci[66]» a tutela dei propri diritti.

Il legislatore europeo sembra quindi legittimare – e per certi versi promuovere – la funzione regolatoria e para-giurisdizionale dei *provider*, cercando al tempo stesso di indirizzarla verso il rispetto dei propri principi.

A tal fine, il Regolamento P2B utilizza, innanzi tutto, i già esaminati vincoli procedurali e doveri di trasparenza posti in capo ai fornitori nella redazione dei propri «termini e condizioni». Significativa è anche la circostanza per cui il testo normativo faccia esplicitamente salvi la tutela giurisdizionale e uno strumento «tradizionale» di risoluzione alternativa delle controversie come la mediazione. Ciò ad ulteriore riprova della tesi per cui il regolatore pubblico,

---

[65] V. C. BUSCH *op. cit*. n. 63; R. VAN LOO, *Federal Rules of Platform Procedure*, in The University of Chicago Law Review, Vol. 88, n. 4, 2020, pp. 829-896.
[66] Cfr. considerando 37.

pur riconoscendo l'esistenza di una forma di potere regolatorio in capo ai fornitori delle piattaforme, non conferisca ad essi una delega in bianco ma si collochi sempre ad un livello superiore, mantenendo un ruolo di garanzia a tutela dei diritti degli utenti commerciali.

Sotto il profilo della responsabilizzazione va poi sottolineato come l'art. 11, par. 4, facendo leva sulla trasparenza, preveda che i fornitori delle piattaforme predispongano e mettano a disposizione del pubblico «informazioni sul funzionamento e l'efficacia[67]» dei loro sistemi interni di gestione dei reclami, «al fine di aiutare gli utenti commerciali a comprendere i principali tipi di problemi che possono insorgere nel contesto della fornitura dei differenti servizi di intermediazione online e la possibilità di raggiungere una veloce ed effettiva risoluzione bilaterale[68]». Le ragioni di «*accountability*» alla base di tale ulteriore obbligo informativo appaiono chiare se si considera che la norma richiede espressamente che i *provider*, assumendo un atteggiamento proattivo, verifichino «quanto meno annualmente» le informazioni e le aggiornino nel caso in cui siano necessarie modifiche significative.

La «responsabilizzazione» dei fornitori viene perseguita anche dall'art. 17 che, analogamente ad altri strumenti legislativi (v. *infra*: Cap. 4, par. 3.2.1; Cap. 6, par. 4.4), contiene l'incoraggiamento della Commissione europea affinché i fornitori di piattaforme e le organizzazioni e associazioni che li rappresentano (così come i *provider* di motori di ricerca ed i relativi rappresentanti) elaborino, assieme agli utenti commerciali ed alle relative organizzazioni di categoria, codici di condotta intesi a contribuire alla corretta applicazione del Regola-

[67] Ai sensi dell'art. 11, par. 4 del Regolamento P2B tra le informazioni da mettere a disposizione del pubblico figurano «il numero totale di reclami presentati, le principali tipologie di reclami, il tempo mediamente necessario per trattarli e dati aggregati relativi all'esito dei reclami».
[68] Cfr. considerando 37.

mento P2B. Allo stesso modo, la Commissione incoraggia i fornitori ad adottare e applicare codici di condotta settoriali, nel caso in cui esistano e siano ampiamente utilizzati.

La rilevanza di questi codici e di altri analoghi strumenti dal punto di vista della *private regulation* sarà esaminata più attentamente nel prosieguo (v. Cap. 4, par. 3.2.1, 3.2.2). Va tuttavia evidenziato sin da ora come essi costituiscano un deciso incoraggiamento all'auto-regolamentazione (ovvero alla co-regolamentazione) delle piattaforme digitali allo scopo di raggiungere gli obiettivi prefissati dal legislatore dell'Unione, a più riprese evocato nell'ambito della Digital Single Market Strategy.

Infine, è opportuno rilevare come l'art. 16 del Regolamento P2B preveda esplicitamente che la Commissione europea possa, ai fini del monitoraggio sull'impatto dello stesso, richiedere informazioni ai fornitori delle piattaforme, per i quali di conseguenza discendono dei doveri di collaborazione sul punto.

Da quanto sopra sembra emergere come la dimensione istituzionale delle piattaforme e il potere regolatorio dei relativi fornitori vengano considerati come un dato dal legislatore dell'Unione. Quest'ultimo, lungi dall'annientare tali fenomeni, pare piuttosto preoccuparsi di orientarli al rispetto dei principi che informano il Regolamento P2B, contribuendo a delineare un quadro normativo improntato sulla «responsabilizzazione» degli stessi fornitori.

Non mancano, peraltro, in dottrina delle voci critiche rispetto all'approccio alla base del Regolamento P2B. In particolare, occorre qui dar conto dell'opinione[69] di chi individua un limite di tale strumento nel suo essere focalizzato in maniera esclusiva sulla disciplina dei rapporti contrattuali tra i fornitori delle piattaforme ed i propri utenti commerciali, inerendo i vari obblighi previsti dallo stesso unicamente alla conformazione dei «termini e condizioni»

[69] C. TWIGG-FLESNER, *op. cit.* n. 56, p. 232.

che regolano le predette relazioni bilaterali. A parere della richiamata dottrina, infatti, il legislatore dell'Unione avrebbe dovuto concentrarsi in maniera più decisa sul ruolo di «*market-maker*» delle piattaforme e sviluppare norme adatte a regolare un intero ecosistema di mercato in cui agiscono *provider*, utenti commerciali e consumatori, piuttosto che migliaia di relazioni bilaterali tra i primi due.

Ad avviso di chi scrive le critiche mosse, pur rispondendo a preoccupazioni condivisibili, vanno in realtà ridimensionate per due ragioni. La prima è che, pur disciplinando unicamente le relazioni tra utenti commerciali e fornitori il Regolamento P2B contiene al proprio interno, soprattutto nei considerando, diversi riferimenti ai «consumatori[70]». Questi ultimi, in particolare, emergono come dei veri e propri «beneficiari indiretti[71]» del regolamento, con ciò dimostrando una visione del legislatore dell'Unione improntata in realtà alla tutela generale del mercato delle piattaforme e non alla mera disciplina di migliaia di rapporti bilaterali sconnessi l'uno dall'altro. La seconda ragione è che il Regolamento P2B non è uno strumento isolato ma si colloca, come si è visto, nel solco di una ampia strategia volta a valorizzare il mercato digitale all'interno dell'Unione e in cui la regolamentazione delle piattaforme, intese anche come «*market-maker*», assume una rilevanza centrale. In tale ottica, a fugare ogni ulteriore dubbio dovrebbe essere il già menzionato Digital Markets Act, che riguarda proprio la disciplina di alcune specifiche piattaforme che, per via del ruolo da esse assunte all'interno del mercato digitale, sono considerate come «*gatekeeper*» dal legislatore dell'Unione.

[70] Le parole consumatore/consumatori compaiono in tutto 68 volte nel Regolamento P2B, di cui 43 nei considerando.
[71] A. PALMIERI, *op. cit.* n. 51, pp. 126ss.

3.2 Altri strumenti rilevanti nell'ambito della Digital Single Market Strategy (cenni)

Il Regolamento P2B costituisce, ad oggi, uno dei principali strumenti normativi in materia di piattaforme digitali adottati nell'ambito della Digital Single Market Strategy. Ad esso vanno aggiunti la già analizzata Direttiva (UE) 2019/790 e i recentemente approvati Digital Markets Act e Digital Services Act (sui quali si dirà meglio *infra*: Cap. 6).

Non si tratta, peraltro, degli unici testi rilevanti per la disciplina delle piattaforme ed esemplificativi del nuovo corso intrapreso dalla Commissione europea. Al contrario, sono numerosi gli strumenti che lambiscono il mondo dei fornitori di servizi di intermediazione *online* e contribuiscono alla loro progressiva responsabilizzazione.

Non è questa la sede per una puntuale analisi di tutti gli strumenti legislativi in questione. Per i fini che qui interessano, basti menzionare testi come il già citato GDPR o il Regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali[72]. Entrambi, infatti, lasciano diverso spazio alla regolamentazione privata e, nel caso del GDPR, pongono enfasi sul principio di «*accountability*» dei «titolari del trattamento[73]» presi in considerazione dallo stesso.

Di importanza minore sono, ai nostri fini, strumenti come il Regolamento (UE) 2019/881 sulla cibersicurezza[74] o il Regolamento (UE) 2018/302 sul c.d.

---

[72] Nome completo: 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, apparso in *GU L 303, 28.11.2018, p. 59–68.*

[73] Ai sensi dell'art. 4, n. 7) GDPR «titolare del trattamento» è «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 […]».

[74] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (Testo rilevante ai fini del SEE), apparso in *GU L 151 del 7.6.2019, pagg. 15–69.*

«*geoblocking*[75]». Occorre infine anche ricordare la già menzionata Direttiva (UE) 2015/1535[76] che, all'art. 1, par. 1, lett. b), contiene la nuova definizione di «servizio della società dell'informazione» originariamente prevista dall'art. 1, punto 2, della direttiva 98/34/CE, come modificata dalla direttiva 98/48/CE.

4. Problemi qualificatori: i gestori delle piattaforme come *internet service provider* o come fornitori dei «servizi sottostanti»?

Svolta una pur sommaria analisi delle norme del diritto dell'Unione più rilevanti per le piattaforme digitali, occorre adesso soffermarsi su una importante questione qualificatoria relativa all'applicazione delle predette norme che ha sollevato e tuttora solleva diverse incertezze.

Come abbiamo visto, in particolare, il diritto dell'Unione non definisce né considera direttamente le «piattaforme» – la cosa, come vedremo, è destinata a cambiare con il Digital Services Act (v. *infra*: Cap. 6, par. 2.1) – ma altre figure a cui le stesse sono state ricondotte. La più importante di esse è il «prestatore di servizi della società dell'informazione» (art. 2, lett. b Direttiva e-Commerce), di cui la più recente figura di «prestatore di servizi di condivisione di contenuti online» (art. 2, n. 6 Direttiva 2019/790) costituisce una specificazione. A queste si è aggiunto anche il «fornitore di servizi di intermediazione online», previsto

[75] Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE (Testo rilevante ai fini del SEE), apparso in *GU L 60I del 2.3.2018, pagg. 1–15.*

[76] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (Testo rilevante ai fini del SEE), apparso in *GU L 241 del 17.9.2015, pagg. 1–15*.

dal Regolamento P2B e pensato proprio in funzione dell'economia delle piattaforme *online*[77].

La definizione di cui alla Direttiva *e-Commerce* è, come si è già avuto modo di constatare, figlia di un'epoca in cui il ruolo dell'*internet service provider* comportava in prevalenza lo svolgimento di attività di tipo meramente tecnico e passivo. Con l'avvento delle piattaforme il paradigma è però entrato in crisi, come si è già saggiato grazie alle considerazioni in merito alla figura di creazione giurisprudenziale dell'*hosting provider* attivo (v. *supra* par. 2.2).

Gli altri dubbi di cui ci si occupa ora riguardano la qualifica da assegnare a piattaforme che, per via dei loro modelli di *business* improntati sul favorire l'incontro tra domanda e offerta di utenti e fornitori di determinati servizi, appaiono svolgere attività ulteriori rispetto a quelle del mero intermediario di servizi della società dell'informazione. In particolare, si è posto il tema se queste piattaforme debbano essere considerate come fornitori dei servizi «sottostanti[78]» scambiati attraverso lo spazio virtuale da esse messo a disposizione, piuttosto che degli *internet service provider* o in aggiunta a ciò. È il caso, ad esempio, di Uber e di Airbnb, a proposito delle quali sono state discusse in giurisprudenza le possibili qualifiche di fornitori di «servizi nel settore dei trasporti» o di servizi di mediazione immobiliare.

La questione non è meramente teorica ma ha delle importanti ricadute pratiche, che riguardano in primo luogo le norme sulla concorrenza e sull'accesso ai mercati. Questo in quanto l'art. 4 della Direttiva *e-Commerce* stabilisce espressamente il «principio dell'assenza di autorizzazione preventiva», in base al quale l'accesso all'attività di *internet service provider* ed il suo esercizio

---

[77] V. C. TWIGG-FLESNER, *op. cit.* n. 56; P. FRANZINA, *op. cit.* n. 51; A. PALMIERI, *op. cit.* n. 51; T. PRASTITOU-MERDI, *op. cit.* n. 51; C. TWIGG-FLESNER, *op. cit.* n. 56; C. BUSCH, *op. cit.* n. 58.

[78] V. in particolare la Comunicazione della Commissione europea COM(2016) 356 final (cit. *supra* n. 42, pp. 6ss.

non possono essere soggetti ad autorizzazione preventiva o ad altri requisiti ad effetto equivalente (come una licenza). Viceversa, agli Stati membri è lasciato il potere di prevedere autorizzazioni o licenze per operare in mercati come quello relativo alla fornitura di servizi di trasporto (tra le altre cose esplicitamente escluso dal campo di applicazione della direttiva Bolkenstein[79]) o quello delle locazioni immobiliari brevi (su cui esistono differenze e barriere all'interno dei vari Stati membri).

Possibili ricadute potrebbero sorgere anche dal punto di vista della responsabilità in quanto, come si è visto, la mancata qualifica di «prestatore di servizi della società dell'informazione» implicherebbe, per quest'ultimo, la non applicabilità del già esaminato regime di «*safe harbour*» di cui agli artt. 12-14 della Direttiva *e-Commerce* (v. *supra* par. 2.1). Ancora, sempre dal punto di vista della responsabilità, secondo alcuni studiosi[80] qualificare una piattaforma come fornitore del «servizio sottostante» esporrebbe la stessa a forme di responsabilità nei confronti dei propri utenti, collegabili proprio alla fornitura del servizio in questione e che, al contrario, non sorgerebbero nel caso in cui la piattaforma fosse considerata un mero intermediario.

Il menzionato problema qualificatorio è stato affrontato per la prima volta in maniera esplicita dalla Commissione europea nella sua comunicazione[81] del 2016 relativa alla c.d. «economia collaborativa» («*collaborative economy*»). In tale occasione, l'Esecutivo dell'Unione ha sottolineato la necessità di una valuta-

[79] Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno, apparsa in *GU L 376 del 27.12.2006, pagg. 36–68*. Vedi in particolare considerando 17, 21 e art. 2, par. 2, lett. d).
[80] N. FILATOVA-BILOUS, *Once again platform liability: on the edge of the 'Uber' and 'Airbnb' cases*, in Internet Policy Review – Journal of Internet Regulation, Vol. 10, n. 2, 2020, pp. 2-27.
[81] COM(2016) 356 final.

zione «caso per caso» per stabilire se il gestore di una piattaforma possa effettivamente essere considerata – oltre o piuttosto che *internet service provider* – fornitore del servizio «sottostante».

A tal proposito, la Commissione ha suggerito di prendere in considerazione vari criteri fattuali e giuridici, chiarendo come il livello di controllo o di influenza che il gestore di una piattaforma può esercitare sui fornitori dei servizi sottostanti sia in genere il fattore determinante. Per misurare tale livello, la Commissione ha indicato i seguenti indici chiave: (i) il fatto che il gestore della piattaforma stabilisce il prezzo finale che dovrà essere pagato dagli utenti; (ii) il fatto che lo stesso gestore determina le altre condizioni contrattuali che disciplinano il rapporto tra utenti e fornitori dei servizi sottostanti; (iii) il fatto che questo sia proprietario dei beni essenziali usati per la fornitura dei servizi sottostanti.

Dal punto di vista della responsabilità va peraltro aggiunto come, a parere della Commissione, il gestore di una piattaforma considerato fornitore del servizio sottostante debba comunque essere qualificato anche come *internet service provider* e, di conseguenza, beneficiare del regime di *safe harbour* nel caso in cui sussistano le relative condizioni (*i.e.* se il fornitore non venga considerato un *hosting provider* attivo). Ai fini dell'esenzione per i contenuti illegali, quindi, il servizio «sottostante» non svuoterebbe di significato la qualifica di «prestatore di servizi della società dell'informazione» anche se, come chiarito dalla Commissione, tale esenzione varrebbe soltanto per i servizi di cui alla Direttiva e-Commerce e non si estenderebbe anche ai «sottostanti». Nella comunicazione dell'Esecutivo non manca, peraltro, un incoraggiamento[82] a che i ge-

[82] Ivi, p. 9.

stori delle piattaforme assumano a prescindere un «comportamento responsabile» nella forma di azioni volontarie, ad esempio per affrontare la questione delle recensioni finte.

4.1 La saga Uber e la qualifica di fornitore di «servizi nel settore dei trasporti»

Le indicazioni della Commissione sono state in seguito applicate – ed in parte superate – dalla Corte di Giustizia in due casi relativi ad Uber (sentenza *Uber Spain*[83] e *Uber France*[84]) e in uno successivo relativo ad Airbnb (sentenza *Airbnb Ireland*[85]). Le pronunce della Corte, su cui ci soffermeremo brevemente, non hanno tuttavia eliminato le incertezze sul punto, anche perché le conclusioni raggiunte sono state opposte.

Nei primi due casi la Corte di Giustizia ha affermato che un servizio di intermediazione, come quello offerto da Uber, avente ad oggetto la messa in contatto mediante un'applicazione per *smartphone*, dietro retribuzione, di conducenti non professionisti, che utilizzano il proprio veicolo, con persone che desiderano effettuare uno spostamento nell'area urbana, deve essere considerato indissolubilmente legato a un servizio di trasporto e rientrante, pertanto, nella qualificazione di «servizio nel settore dei trasporti», ai sensi del diritto dell'Unione (in particolare dell'art. 58 TFUE e della direttiva 2006/123/CE).

Per giungere a tale conclusione la Corte ha in primo luogo rilevato come il servizio di Uber sia più di un semplice servizio d'intermediazione *online*. Al contrario, infatti, ad avviso dei giudici di Lussemburgo Uber crea al contempo

---

[83] CGUE, causa C-434/15, *Asociación Profesional Elite Taxi* c. *Uber Systems Spain SL*, 20 dicembre 2017.

[84] CGUE, causa C-320/16, procedimento penale a carico di *Uber France SAS*, con l'intervento di: *Nabil Bensalem*, 10 aprile 2018.

[85] CGUE, causa C-390/18, procedimento penale a carico di *X*, con l'intervento di: *YA, Airbnb Ireland UC, Hôtelière Turenne SAS, Association pour un hébergement et un tourisme professionnels (AHTOP), Valhotel*, 19 dicembre 2019.

un'offerta di servizi di trasporto urbano che rende accessibile con strumenti informatici, come la sua app, e di cui organizza il funzionamento generale a favore degli utenti. A tal proposito, la Corte ha sottolineato come il servizio di Uber sia necessario sia per i conducenti sia per gli utenti che, in mancanza, non opererebbero sul mercato dei servizi di trasporti. Inoltre, è stato evidenziato come Uber abbia un'influenza determinante sulle condizioni a cui i conducenti possono fornire i propri servizi, ad esempio fissando il prezzo massimo della corsa, ed eserciti un determinato controllo sulla qualità dei veicoli e dei loro conducenti, nonché sul comportamento di questi ultimi, che può anche portare alla loro esclusione.

Pertanto, la Corte ha concluso affermando che il servizio d'intermediazione di Uber – pur presentando in linea di principio i criteri per essere qualificato «servizio della società dell'informazione» ai sensi della Direttiva *e-Commerce* – debba essere considerato parte integrante di un servizio complessivo in cui l'elemento principale è un servizio di trasporto e sia, di conseguenza, da qualificare non come «servizio della società dell'informazione» ma come «servizio nel settore dei trasporti[86]».

Come si può vedere, nel proprio ragionamento la Corte ha fatto applicazione delle indicazioni della Commissione europea, svolgendo un'analisi sul modello di business di Uber per qualificarne l'attività dal punto di vista del diritto dell'Unione. Peraltro, a differenza di quanto suggerito dall'Esecutivo, i Giudici di Lussemburgo non hanno considerato tra i criteri decisivi per qualificare Uber come fornitore di servizi di trasporto la proprietà dei beni essenziali (nel caso specifico i veicoli) ma hanno dato rilievo unicamente alla capacità della stessa di influenzare i termini dei rapporti contrattuali tra utenti e conducenti

[86] V. punto 40 sentenza *Uber Spain*. La definizione di «servizio nel settore dei trasporti» viene fornita dall'art. 2, par. 2, lett. d) 2006/123/CE.

ed al suo ruolo di «*market-maker*[87]», ossia di creatore di un mercato che, in sua assenza, non esisterebbe.

Inoltre, escludendo categoricamente l'applicazione della Direttiva e-Commerce, la Corte sembra sconfessare la Commissione anche a proposito dell'operatività del regime di «*safe harbour*» con riferimento alle piattaforme nelle quali il «servizio della società dell'informazione» sia accessorio ad un «servizio sottostante». Nell'ottica della Corte, infatti, soltanto quest'ultimo è il servizio rilevante per qualificare e di conseguenza disciplinare la piattaforma, rimanendo il servizio della società dell'informazione ed il relativo regime di esenzione dalla responsabilità assorbiti dalla qualifica dell'altro servizio che, da «sottostante», diventa quindi «principale[88]».

L'approccio assunto dalla Corte nelle sentenze Uber è, a parere di certa dottrina[89], da salutare con favore dal momento che viene ritenuto corretto, per valutare il ruolo contrattuale dei gestori delle piattaforme, porre enfasi sul livello di influenza degli stessi sulla formazione degli accordi conclusi attraverso la loro attività piuttosto che su elementi come la proprietà dei beni utilizzati per la fornitura dei loro servizi. Ancora, la dottrina favorevole ha sottolineato come, oltre a fornire un metodo per la qualificazione caso per caso delle piattaforme, l'approccio della Corte contribuirebbe all'obiettivo della progressiva responsabilizzazione dei loro gestori perseguito a livello dell'Unione.

Di contro, alcune voci critiche hanno sostenuto come la mancata qualificazione di piattaforme del tipo di Uber come «servizi della società dell'informa-

---

[87] V. a questo proposito: T. PRASTITOU-MERDI, *op. cit.* n. 51, pp. 551ss; T. RODRÍGUEZ DE LAS HERAS BALLELL, *op. cit.* Cap. 1, n. 9, p. 67; A. DE FRANCESCHI, *Uber Spain and the "Identity Crisis" of Online Platforms*, in Journal of European Consumer and Markets Law, Vol. 7, n. 1, 2018, pp. 1-4.

[88] CGUE, *Uber Spain*, punto 40.

[89] A. DE FRANCESCHI, *op. cit.* n. 87.

zione» sia invece suscettibile, da una parte, di acuire le incertezze esistenti relative all'applicazione della Direttiva e-Commerce e, dall'altra, di crearne in relazione al Regolamento P2B. A parere di tale dottrina, infatti, piattaforme di questo genere rimarrebbero inevitabilmente escluse dal campo di applicazione del nuovo strumento in quanto, non essendo «servizi della società dell'informazione», non potrebbero nemmeno qualificarsi come «servizi di intermediazione online» (art. 2, par. 2 Regolamento P2B). Ciò sconfesserebbe, peraltro, l'obiettivo della Commissione a che il nuovo regolamento si applichi a tutti gli attori del mercato delle piattaforme[90].

Va inoltre aggiunto come, a mente della stessa dottrina, le conclusioni della Corte risultino ingiustificate, anche perché la qualifica di *internet service provider* non avrebbe, secondo la tesi sostenuta, precluso l'applicazione delle norme nazionali in materia di accesso ai mercati dei servizi di trasporto, la cui preservazione viene considerata il vero motivo alla base delle decisioni dei Giudici di Lussemburgo.

4.2 Una prima applicazione del «Metodo Uber»: il caso *Airbnb Ireland* e le conclusioni (apparentemente) opposte della Corte

Dopo le sentenze *Uber Spain* ed *Uber France* la Corte di Giustizia ha avuto modo di pronunciarsi sulla qualifica di un'altra piattaforma molto popolare a livello mondiale, ossia Airbnb. L'occasione si è posta in particolare nel caso *Airbnb Ireland*, relativo ad un procedimento penale intentato in Francia per condotte consistenti nella gestione di fondi per attività di mediazione e gestione di immobili ed esercizi commerciali da parte di un soggetto sprovvisto di licenza per l'esercizio di tale professione e, pertanto, in violazione della *loi n° 70-9, du 2 janvier 1970* («Legge Hoguet»).

[90] T. PRASTITOU-MERDI, *op. cit.* n. 51, p. 553.

Come nel caso di Uber, nel procedere con la qualificazione la Corte ha, in primo luogo, rilevato come il servizio offerto da Airbnb Ireland costituisca, quanto meno in linea di principio, un «servizio della società dell'informazione» ai sensi della Direttiva *e-Commerce*, in quanto servizio prestato dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario dei servizi, come da requisiti previsti dall'art. 1, par. 1, lett. b) della Direttiva (UE) 2015/1535.

Successivamente, i Giudici di Lussemburgo hanno fatto applicazione dei criteri stabiliti nelle sentenze *Uber Spain* e *Uber France* per verificare se il servizio in questione costituisse, anche in questo caso, parte integrante di un servizio globale il cui elemento principale fosse un servizio a cui vada riconosciuta una diversa qualificazione giuridica, nello specifico un servizio nel settore immobiliare.

A tal fine, la Corte ha, innanzi tutto, rilevato come la «caratteristica essenziale» del servizio offerto da Airbnb non sia la realizzazione immediata di una prestazione di alloggio ma la creazione di un elenco strutturato degli alloggi disponibili sulla sua piattaforma, corrispondente ai criteri selezionati dalle persone che cercano una sistemazione di breve durata, a vantaggio sia di tali persone che degli albergatori. Sotto questo profilo, a differenza di quanto stabilito nelle due pronunce *Uber*, la Corte ha affermato come la creazione di tale elenco costituisca, per la sua importanza, un servizio che non può essere considerato come un semplice accessorio di un servizio globale al quale vada applicata una qualifica giuridica diversa, vale a dire una prestazione di alloggio.

In secondo luogo, analizzando il potenziale ruolo di «*market-maker*» di Airbnb, la Corte ha rilevato come il servizio da questa offerto non risulti «per nulla indispensabile alla realizzazione di prestazioni di alloggio sia dal punto di vista dei locatari che dei locatori che vi fanno ricorso, posto che entrambi dispongono di numerosi altri canali, alcuni disponibili da lungo tempo, come

le agenzie immobiliari, gli annunci in formato cartaceo o elettronico o ancora i siti Internet di locazioni immobiliari[91]». Sul punto la differenza con Uber è evidente e sostanziale in quanto, come si è visto, il servizio di quest'ultima è stato considerato imprescindibile per mettere in contatto utenti e conducenti tramite la popolare applicazione, senza la quale, a parere della Corte, il mercato di questi ultimi semplicemente non potrebbe esistere.

In ultimo, i Giudici di Lussemburgo hanno considerato l'aspetto dell'influenza di Airbnb sulla conformazione dei contratti di locazione conclusi attraverso la sua piattaforma. A tal riguardo, la Corte ha rilevato come Airbnb non stabilisca né fissi un limite all'importo che può essere preteso dai locatori e che, al massimo, «essa mette a loro disposizione uno strumento opzionale di stima del prezzo della loro locazione alla luce delle medie di mercato ricavate da detta piattaforma, lasciando unicamente al locatore la responsabilità di determinare l'importo della locazione». Pertanto, sottolineando anche come la stessa «non effettua nemmeno la selezione dei locatori o degli alloggi proposti in locazione sulla sua piattaforma[92]», la Corte ha affermato che Airbnb, a differenza di Uber, non esercita un'influenza decisiva sulle condizioni dei servizi di alloggio cui è collegato il proprio servizio.

Alla luce ciò la Corte ha concluso stabilendo che un servizio di mediazione come quello di Airbnb, pur se offerto attraverso una piattaforma che fornisce anche determinate «prestazioni accessorie[93]», debba essere qualificato come

---

[91] CGUE, *Airbnb Ireland*, punto 55.

[92] CGUE, *Airbnb Ireland*, punto 68.

[93] CGUE, *Airbnb Ireland*: «59. […] oltre alla sua attività consistente nel mettere in contatto locatori e i locatari tramite la piattaforma elettronica omonima, la Airbnb Ireland fornisce ai locatori uno schema che definisce il contenuto della loro offerta, un servizio opzionale di fotografia del bene posto in locazione nonché un sistema di valutazione dei locatori e dei locatari consultabile dai futuri locatori e locatari […]. 61 […] Airbnb Payments UK, società del gruppo Airbnb, si incarica della riscossione dell'importo delle locazioni presso i locatari per poi trasferirlo ai locatori, secondo le modalità ricordate nel punto 19 della presente sentenza. […]. 63. Infine, nemmeno la circostanza che la Airbnb Ireland offre ai locatori una garanzia contro

un «servizio della società dell'informazione», che non può essere considerato parte integrante di un servizio globale il cui elemento principale sarebbe una prestazione di alloggio.

4.3 Chiarimenti e questioni irrisolte alla luce delle sentenze *Uber Spain*, *Uber France* e *Airbnb Ireland*

Osservando in chiave sistematica le sentenze appena esaminate, occorre in primo luogo constatare come in esse, pur giungendo a conclusioni apparentemente opposte, la Corte di Giustizia abbia fatto applicazione dei medesimi criteri per addivenire alla qualificazione delle due piattaforme ai sensi del diritto dell'Unione. Da questo punto di vista metodologico l'approccio della Corte appare quindi da salutare con favore.

La giurisprudenza in commento non ha tuttavia risolto tutte le incertezze sul punto, come sottolineato da più parti in dottrina[94]. In particolare, è stato evidenziato come l'utilizzo di un approccio «*case-by-case*» del tipo indicato dalla Corte corra in più circostanze il rischio di risultare fallace e di acuire l'aleatorietà intorno al problema qualificatorio in discussione. Ciò anche perché la Corte – a differenza di quanto fatto dalla Commissione nella comunicazione sopra citata – non ha fornito alcuna indicazione in merito al grado di importanza da assegnare a ciascuno dei criteri dalla stessa presi in considerazione.

A tal proposito, diversi commentatori hanno criticato le distinzioni fatte dalla Corte in merito al ruolo di «*market-maker*» delle piattaforme considerate nelle proprie decisioni. Questo in quanto anche Uber, a giudizio di tale dottrina, non sarebbe tecnicamente «indispensabile» per la creazione del proprio mercato in quanto i conducenti potrebbero comunque entrare in contatto con gli

---

i danni nonché, in opzione, un'assicurazione per la responsabilità civile è tale da modificare la qualificazione giuridica del servizio di mediazione fornito da detta piattaforma».

[94] T. PRASTITOU-MERDI, *op. cit.* n. 51, pp. 555ss; T. RODRÍGUEZ DE LAS HERAS BALLELL, *op. cit.* Cap. 1, n. 9 p. 67; N. FILATOVA-BILOUS, n. 80.

utenti attraverso modalità più tradizionali e farraginose (es. telefonicamente). Viceversa, è stato notato come, se è vero che esistessero già diversi strumenti per offrire locazioni a breve termine, Airbnb abbia aperto il mercato a soggetti abitualmente esclusi da esso come proprietari o locatari di case «normali».

In via generale, il rischio segnalato è quello per cui, essendo di rado possibile qualificare un servizio come «indispensabile» in termini assoluti, l'utilizzo dell'approccio della Corte conduca più che altro a decisioni basate su incerte valutazioni circa il grado in cui una piattaforma espande o valorizza un mercato in realtà già esistente. Il risultato indesiderato sarebbe quello di creare asimmetrie applicative, soprattutto tra i vari Stati membri, con conseguenze negative in termini di certezza del diritto[95] che andrebbero ad intaccare diversi settori economici. Si pensi, ad esempio, al *food delivery*, in cui le piattaforme rivestono un'importanza decisiva nell'amplificare la visibilità di ristoranti e locali le cui attività, tuttavia, esistono indipendentemente dalle stesse.

A livello sistematico, altra dottrina[96] ha inoltre sottolineato come il porre enfasi sull'influenza di una piattaforma nella conformazione dei termini contrattuali che regolano i rapporti tra utenti e fornitori allo scopo di escluderne la qualifica di *internet service provider* rischi di minare l'effettiva importanza pratica di strumenti come il Regolamento P2B che, come abbiamo visto, si basano al contrario sulla premessa per cui i «fornitori di servizi di intermediazione online» abbiano un consistente potere regolatorio.

Si è già avuto modo di vedere, peraltro, come per parte della dottrina[97] la mancata qualificazione di una piattaforma come «servizio della società dell'informazione» ai sensi della Direttiva e-Commerce sia suscettibile di escluderla

[95] M. INGLESE, *Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland*, in Eurojus, fasc. 1, pp. 37-52, 2020.
[96] T. PRASTITOU-MERDI, *op. cit.* n. 51, pp. 552ss.
[97] T. PRASTITOU-MERDI, *op. cit.* n. 51, pp. 555ss.

in toto dall'ambito di applicazione dello stesso Regolamento P2B. Le conseguenze di ciò sarebbero notevoli in quanto gli utenti commerciali – ed indirettamente anche i consumatori – di piattaforme sempre più rilevanti nel mercato digitale si vedrebbero privati della tutela garantita dal nuovo strumento legislativo. Come abbiamo visto, peraltro, il Regolamento P2B è stato adottato con l'obiettivo ambizioso di applicarsi alla gran parte delle piattaforme attive sul mercato digitale ed un'eventuale esclusione di piattaforme come Uber rischierebbe di minare concretamente le intenzioni del legislatore dell'Unione. Simili considerazioni valgono, peraltro, anche per il Digital Services Act (su cui v. *infra*: Cap. 6, par. 2.1)

A parere di chi scrive, il ragionamento della Corte nelle sentenze in commento potrebbe in realtà, almeno in parte, smussare le predette preoccupazioni. In tutte e tre le pronunce, infatti, i Giudici di Lussemburgo sono partiti dalla constatazione per cui sia Uber che Airbnb offrano un servizio che, quanto meno in linea di principio, costituisce un «servizio della società dell'informazione», per poi valutare se lo stesso sia accessorio ad un differente servizio globale, rispettivamente di trasporto o di alloggio. Nel caso di Uber il carattere della accessorietà è stato quindi ritenuto decisivo per escludere l'applicazione della Direttiva e-Commerce ma non anche per eliminare l'assunto di base. Non è pertanto da escludere che tali servizi possano comunque essere ritenuti come «servizi della società dell'informazione» ai fini del Regolamento P2B, il quale, come si è visto, persegue finalità diverse dalla Direttiva e-Commerce e non dice nulla in merito ai requisiti di accesso ai diversi mercati su cui operano le piattaforme. Per chiarire le incertezze, vista anche l'assoluta novità del regolamento in questione, saranno senz'altro utili degli interventi giurisprudenziali, auspicabili in futuro anche a proposito del Digital Services Act, a maggior ragione considerando che questo si pone per molti aspetti in continuità con la stessa Direttiva e-Commerce.

Capitolo 3 – Le piattaforme digitali e il diritto internazionale privato dell'Unione europea

SOMMARIO: 1 Piattaforme digitali e diritto internazionale privato: criticità di fondo. – 1.1 Gli intrecci tra spazio fisico e virtuale nell'ambito delle piattaforme digitali. – 1.2 Piattaforme e limiti dell'impostazione stato-centrica del diritto internazionale privato dell'Unione. – 2 Le norme di diritto internazionale privato nei rapporti tra piattaforme e utenti. – 2.1 L'architettura contrattuale alla base dei rapporti piattaforma-utente. – 2.2 I tentativi di valorizzare il luogo di residenza o di domicilio dell'utente ai fini della competenza giurisdizionale. – 2.3 La protezione degli utenti «lavoratori» ai sensi del diritto internazionale privato. – 2.3.1 Problemi qualificatori: tra «lavoratori» subordinati e autonomi. – 2.3.2 Problematiche relative all'applicazione delle norme e dei criteri di collegamento di diritto internazionale privato. – 2.4 La protezione degli utenti «consumatori». – 2.4.1 Problemi qualificatori: tra «consumatori» e «professionisti». – 2.4.2 La qualifica di «consumatore» nell'ambito delle piattaforme digitali: indicazioni alla luce del caso *Schrems*. – 2.4.3 Il regime consumeristico in pratica: tra «*targeting approach*» e volontà delle parti. – A) Il «*targeting approach*» e le sue evoluzioni nel mercato digitale: il caso *Pammer*. – B) I limiti alla volontà delle parti come ulteriore tutela del consumatore. – 2.5 L'insufficienza dei regimi speciali e la necessità di proteggere gli utenti appartenenti ad altre categorie. – 3 Le norme di diritto internazionale privato nei rapporti tra utenti. – 3.1 La disciplina dei rapporti contrattuali tra utenti. – *…Segue*: L'applicazione dei regimi protettivi. – 3.2 La rilevanza delle regole delle piattaforme nei rapporti tra utenti. – 3.2.1 L'estensione della scelta di legge contenuta nelle condizioni della piattaforma. – 3.2.2 Le regole delle piattaforme come «dato di fatto» nei rapporti tra utenti. – 4 Gli illeciti civili: tra ubiquità, *favor laesi* e tutela del mercato. – 4.1 La lesione dei diritti della personalità e la «teoria del mosaico». – 4.2 La violazione dei diritti di proprietà intellettuale in rete e il caso *Wintersteiger*. – 4.3 Piattaforme e

norme di diritto internazionale privato in materia di concorrenza. – 4.3.1 Le questioni relative alla legge applicabile: tra «teoria del mosaico» e rapporti con la Direttiva e-Commerce. – 4.3.2 La competenza giurisdizionale: assenza di regimi specifici e problemi qualificatori. – 5 I «nuovi» paradigmi del diritto internazionale privato online: dal ritorno dell'unilateralismo al «*regulatory overreaching*». – 5.1 Il metodo unilateralista come tentativo di estendere la sovranità degli ordinamenti giuridici in rete. – 5.2 Il Regolamento P2B tra unilateralismo e assenza di norme sulla giurisdizione. – 5.3 Il «*regulatory overreaching*» e il bisogno strutturale della cooperazione delle piattaforme.

1 Piattaforme digitali e diritto internazionale privato: criticità di fondo

Dopo aver esaminato i profili rilevanti ai sensi del diritto materiale, in questo capitolo ci si concentrerà sulle problematiche relative all'applicazione delle norme di diritto internazionale privato dell'Unione europea nell'ambito delle piattaforme digitali.

L'importanza della questione risulta evidente se si considera che, come si è già avuto modo di constatare (v. *supra*: Cap. 1, par. 3), le piattaforme sono ambienti per loro natura transnazionali, in cui in ogni momento si costituiscono rapporti giuridici tra soggetti stabiliti in tutto il mondo. Questa capacità di facilitare le interazioni tra individui riducendo sensibilmente gli ostacoli derivanti dalle distanze spazio-temporali, oltre a portare significativi benefici per l'economia e per gli scambi commerciali, si traduce in diverse incertezze relative alle classiche questioni del diritto internazionale privato, in *primis* l'individuazione della legge applicabile e la disciplina sulla giurisdizione rispetto ai rapporti costituitisi nell'ambito delle piattaforme, oltre che l'efficacia delle decisioni delle autorità giudiziarie.

Gli interrogativi in questione, che vanno di pari passo con le problematiche qualificatorie affrontate nel precedente capitolo, sono soltanto in parte risolti

(o risolvibili) dalle norme di diritto internazionale privato attualmente in vigore nel sistema dell'Unione europea[1]. Queste, infatti, come si è già avuto modo di notare, si fondano in gran parte su logiche[2] basate sulla territorialità e sulla centralità degli ordinamenti statali. In particolare, le norme di diritto internazionale privato dell'Unione, sulla scorta del metodo bilaterale savignano, si basano principalmente sull'utilizzo di criteri di collegamento volti a localizzare una fattispecie nel territorio di un determinato Stato allo scopo, a seconda dei casi, di individuare la legge applicabile o risolvere le questioni relative alla disciplina sulla giurisdizione. Poco o nullo è invece lo spazio per gli ordinamenti e i diritti di fonte diversa[3].

Le anzidette logiche mal si attagliano ad ambienti virtuali, come le piattaforme, che presentano scarsi ancoraggi con i territori fisici e in cui, come si è già anticipato e si approfondirà meglio in seguito (v. *supra*: Cap. 1, par. 3; *infra*: Cap. 4, par. 3**)**, la regolamentazione privata assume un'importanza notevole, per certi versi superiore a quella degli Stati. Il risultato è la scarsa idoneità delle norme di diritto internazionale privato dell'Unione ad operare nell'ambito

[1] Per i fini che qui interessano si considerano, in particolare, gli seguenti strumenti normativi: Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I); Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II); Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012 , concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (Bruxelles I*bis*).

[2] Si vedano: J. BOMHOFF, A. MEUWESE, p. 149; O. KAHN-FREUND, entrambi *cit.* sub Cap. 1 n. 44. Nello specifico sulle piattaforme si veda: P. FRANZINA, *op. cit.* sub Cap. 2 n. 51; I. PRETELLI, *Protecting Digital Platform Users by Means of Private International Law*, in *Cuadernos de Derecho Transnacional,* Vol. 13, n. 1, pp. 574-585, 2021, disponibile su SSRN: https://ssrn.com/abstract=3784912.

[3] Sul tema si vedano, *inter alia*: A. BONOMI, *The Rome I Regulation on the Law Applicable to Contractual Obligations: Some General Remarks*, in Yearbook of Private International Law, Vol. X, pp. 165-176, 2008.

delle piattaforme digitali, con importanti conseguenze sia in termini di prevedibilità che di effettività delle soluzioni, vale a dire alcuni tra gli obiettivi cui mirano le stesse regole internazionalprivatistiche[4].

Su queste problematiche ci si soffermerà più nel dettaglio nelle prossime pagine, cercando di comprendere se ed in quale misura siano ipotizzabili nuovi paradigmi. Nelle analisi sul punto si prenderanno in considerazione sia le relazioni afferenti alla «dimensione verticale», sia quelle relative alla «dimensione orizzontale» delle piattaforme. Un focus specifico sarà dedicato alle norme di diritto internazionale privato in materia di illeciti, la cui disciplina interessa i rapporti afferenti ad entrambe le dimensioni.

1.1 Gli intrecci tra spazio fisico e virtuale nell'ambito delle piattaforme digitali

Per affrontare le tematiche descritte è utile partire da una classificazione operata in dottrina[5], che distingue tre tipi di piattaforme sulla base degli intrecci tra mondo digitale e spazio fisico che caratterizzano i rapporti giuridici da esse favoriti.

Il primo tipo, più tradizionale, è costituito dalle piattaforme che si limitano a mostrare annunci pubblicitari e a mettere a disposizione degli utenti i canali attraverso cui contattare il venditore dei prodotti o il fornitore dei servizi cui l'annuncio si riferisce. In questo caso, pertanto, pur essendo le parti entrate in contatto grazie alla piattaforma, l'eventuale rapporto giuridico tra le stesse ci costituisce e si esegue integralmente nel mondo fisico.

Piattaforme del secondo tipo sono invece quelle in cui le volontà degli utenti si incontrano nel mondo virtuale per costituire (spesso tramite «*click*») rapporti

[4] Si considerino, a tal proposito, le seguenti disposizioni tratti dai regolamenti dell'Unione: considerando 15 e 16 Regolamento Bruxelles I*bis*; considerando 6 e 16 Regolamento Roma I; considerando 6, 14, 16, 20 Regolamento Roma II.

[5] I. PRETELLI, *op. cit.* sub Cap. 1, n. 11.

che si eseguono, in tutto o nella maggior parte, nel mondo fisico. È questo, al netto dei problemi qualificatori cui si è detto in precedenza (v. *supra* Cap. 2, par. 4), il caso di piattaforme molto popolari come Airbnb, Uber o TaskRabbit, attraverso cui vengono offerti servizi concretamente fruiti dagli utenti nello spazio fisico. Appartengono a questa categoria anche le piattaforme di *e-commerce*.

Il terzo tipo è rappresentato dalle piattaforme in cui si costituiscono rapporti destinati ad eseguirsi integralmente nello spazio virtuale. È il caso dei *social network*, dei videogiochi *online*, delle piattaforme di *streaming* di contenuti digitali e, più in generale, di quelle attraverso cui vengono forniti servizi o venduti prodotti dei quali è possibile fruire o godere integralmente *online*. Importanti, anche in termini di ricadute sociali e di rischio di *dumping*[6], sono le piattaforme di «*crowdworking*», attraverso cui è possibile mettere a disposizione, in cambio di un compenso economico, prestazioni lavorative (come, ad esempio, servizi di traduzione, lezioni private, assistenza informatica) che possono essere svolte totalmente in rete e a distanza, senza alcun bisogno di incontri fisici tra l'utente prestatore e il committente/acquirente. Tra queste si possono menzionare le americane Upwork e Topcoder, l'israeliana Fiverr, e la tedesca Twago.

[6] Idem, p. 46. Si vedano anche, nello stesso volume: E. MOSTACCI, *Faut-il prévoir des règles impératives pour la protection des parties faibles dans les relations de travail? Quelques suggestions méthodologiques pour une réponse éclairée*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 243-254, Schulthess, 2018 (p. 251); A. MEIER, *Le futur dialogue social et du tripartisme dans le contexte de la digitalisation de l'économie*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 305-324, Schulthess, 2018 (p. 310).

Tenendo conto della predetta classificazione, si può preliminarmente affermare come il funzionamento delle norme di diritto internazionale privato risulti, tendenzialmente, meno complicato nell'ambito delle piattaforme dei primi due tipi. Questo in quanto i tradizionali criteri di collegamento basati sulla territorialità appaiono, in generale, più facilmente adattabili alle stesse. Così, ad esempio, parlando di piattaforme come Uber appare agevole determinare il «luogo [fisico] di esecuzione dell'obbligazione dedotta in giudizio[7]», così come quello in cui «l'immobile è situato[8]» in Airbnb.

Come vedremo meglio nelle prossime pagine, assai più complessa è l'applicazione dei criteri di collegamento internazionalprivatisti nell'ambito delle piattaforme del terzo tipo, dal momento che i legami delle stesse con il territorio sono minimi – anche se pur sempre esistenti, quanto meno se si considerano i luoghi (fisici) di residenza delle parti o quelli in cui si trovano le infrastrutture che ne permettono il funzionamento da un punto di vista tecnologico.

Nell'ambito di queste piattaforme la prevedibilità delle soluzioni circa la legge applicabile e la competenza giurisdizionale appare più a rischio che nelle altre. Ciò si è tradotto, quanto meno nella giurisprudenza della Corte di Giustizia europea relativa all'applicazione delle norme dei regolamenti Bruxelles I e Bruxelles I*bis* sulla competenza giurisdizionale in materia di fatti illeciti[9] commessi attraverso internet, in una sempre più estesa applicazione della teoria «dell'ubiquità» inaugurata con la sentenza *Mines de Potasse*[10] e oggi espres-

[7] V. art. 7, punto 1 Regolamento Bruxelles I*bis*.

[8] V. ad esempio: art. 4, par. 1, lett. c) Regolamento Roma I; art. 24, punto 1) Regolamento Bruxelles I*bis*.

[9] Il riferimento è all'art. 5, punto 3 del Regolamento CE n. 44/2001 (Bruxelles I), rifuso nel successivo art. 7, punto 2 del Regolamento UE n. 1215/2012 (Bruxelles I*bis*).

[10] CGUE, causa C-21/76, *Handelskwekerij G.J. Bier B. V.* c. *Mines de potasse d'Alsace S.A.*, 20 novembre 1976 – ECLI:EU:C:1976:166.

samente rifusa nell'art. 7, punto 2 del Regolamento Bruxelles I*bis*. Come vedremo meglio in seguito (v. *infra*: par. 4.1), nell'ambito di questa tendenza evolutiva si colloca la c.d. «teoria del mosaico», elaborata dalla Corte di Giustizia con la sentenza *Shevill*[11] in materia di violazione dei diritti della personalità e diffamazione, e successivamente ripresa ed estesa ulteriormente nella sentenza *e-Date*[12] a proposito degli illeciti commessi in rete.

1.2 Piattaforme e limiti dell'impostazione stato-centrica del diritto internazionale privato dell'Unione

Come già accennato, l'altra caratteristica delle norme del diritto internazionale privato dell'Unione europea che ne limita l'applicazione nell'ambito delle piattaforme digitali è la loro impostazione prevalentemente «stato-centrica». Tali norme, infatti, sono finalizzate essenzialmente alla risoluzione dei conflitti di legge o delle questioni relative alla giurisdizione sorte tra ordinamenti giuridici statali. Del tutto residuale è invece lo spazio per diritti di matrice diversa.

Nel Regolamento Roma I, ad esempio, il solo riferimento ai diritti non statali è contenuto nel considerando 13, in base al quale «il presente regolamento non impedisce che le parti includano nel loro contratto, mediante riferimento, un diritto non statale». La dottrina[13] ne ricava la conclusione per cui le parti possano utilizzare il diritto non statale soltanto per integrare il contenuto materiale del contratto (c.d. «autonomia materiale[14]»), essendo invece precluso individuare lo stesso quale norma regolatrice dell'intero negozio. L'art. 3 del

---

[11] CGUE, causa C-68/93, *Fiona Shevill e a.* c. *Presse Alliance SA*, 7 marzo 1995 – ECLI:EU:C:1995:61.

[12] CGUE, cause riunite C-509/09 e C-161/10, *eDate Advertising GmbH e a.* c. *X e Société MGN LIMITED*, 25 ottobre 2011 – ECLI:EU:C:2011:685.

[13] V. *ex multis*: P. FRANZINA, *op. cit*. 3; P. MANKOWSKI, *Article 3: Freedom of Choice* in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome I Regulation: Commentary*, pp. 87-263, Verlag Dr. Otto Schmidt, 2016; F. RAGNO, *Article 3 Freedom of Choice*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 59-87, Cambridge University Press, 2020.

[14] P. FRANZINA, *Introduzione al diritto internazionale privato*, Giappichelli, 2021 (p. 207)

medesimo regolamento, infatti, limita l'autonomia delle parti circa la scelta della legge applicabile all'intero contratto (c.d. «autonomia conflittuale[15]») soltanto ai diritti di fonte pubblica. In questo senso, peraltro, va ricordato come la proposta[16] originaria della Commissione europea contenesse, all'art. 3, par. 2, la possibilità per le parti di scegliere, come legge applicabile, anche «principi e norme di diritto sostanziale dei contratti, riconosciuti a livello internazionale o comunitario». La previsione, che si riferiva a corpi di norme come i principi Unidroit[17], è stata tuttavia accantonata nel corso del processo di adozione del regolamento, confermando quindi la tradizionale impostazione stato-centrica sottesa allo stesso.

Del tutto marginale è lo spazio per gli ordinamenti e i diritti non statali anche negli altri strumenti normativi. Come vedremo meglio in seguito, ad esempio, vi è in dottrina chi ha provato a teorizzarne la rilevanza quale norma di sicurezza e di condotta ai sensi dell'art. 17 del Regolamento Roma II (v. *infra*: par. 3.2.2).

Con l'avvento di internet prima e delle piattaforme digitali dopo, la dottrina[18] ha iniziato ad interrogarsi sulla necessità e sulla attuabilità di nuovi paradigmi che, distaccandosi almeno in parte da questa visione tradizionale, valorizzino

---

[15] Idem, p. 207.

[16] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio sulla legge applicabile alle obbligazioni contrattuali (Roma I)*, COM(2005) 650 def. –2005/0261 (COD), 15 dicembre 2005.

[17] È possibile reperire le varie versioni dei Principi Unidroit dei contratti commerciali internazionali (ultima delle quali del 2016) online al seguente link: https://www.unidroit.org/instruments/commercial-contracts/.

[18] V. *inter alia*: L. LESSIG, *op. cit.* sub Cap. 1, n. 32; J. GOLDSMITH-T. WU, *op. cit.* sub Cap. 1, n. 46; D.J. SVANTESSON, *op. cit.* sub Cap. 1, n. 46; I. PRETELLI, *op. cit.* sub Cap. 1, n. 11; T. LUTZI, *op. cit.* sub Cap. 1, n. 37; L. BYGRAVE, *Internet Governance by Contract*, Oxford Scholarship Online, 2015 (pp. 28-30, 44-46).

il fenomeno auto-regolatorio tipico della rete anche a fini internazionalprivatisti. I paradigmi in questione si fondano, in particolare, sull'idea[19] già richiamata (v. *supra*: Cap. 1, par. 5) per cui le piattaforme possano essere considerate alla stregua di ordinamenti giuridici autonomi, con delle proprie regole e, soprattutto, la capacità di applicarle senza bisogno di forze coercitive esterne.

Conseguenza di questa visione, secondo la prospettazione dottrinale in commento, sarebbe quella per cui le regole delle piattaforme possano essere individuate dalle norme di conflitto come «legge applicabile» alle fattispecie relative al mondo virtuale. Ciò, in particolare, potrebbe avvenire assimilando le piattaforme ai «luoghi» fisici considerati dai criteri di collegamento internazionalprivatistici, in modo da localizzare a tal fine una fattispecie all'interno dell'ambiente virtuale, risolvendo così le difficoltà illustrate nel precedente paragrafo 1.1. Allo stesso modo, si è sostenuto come alle piattaforme – o ad organi indipendenti riconducibili ad esse – possa essere assegnata, se non una vera e propria «competenza giurisdizionale», una sorta di funzione «para-giurisdizionale». Soluzione che, come abbiamo visto (v. *supra*: Cap. 2, par. 2.3, 3.1), è già stata fatta propria da diversi strumenti comunitari, come il Regolamento P2B, la Direttiva Copyright ed il Digital Services Act, è che risulta apprezzabile anche alla luce del principio generale di «prossimità[20]».

Queste soluzioni, che valorizzano in maniera decisiva la «dimensione istituzionale» delle piattaforme, si scontrano tuttavia con l'impostazione di fondo delle norme del diritto internazionale privato dell'Unione. Quest'ultimo, infatti, nonostante la recente svolta unilateralista di cui si dirà più avanti (v. *infra*: par. 5) e il riconoscimento di funzioni «para-giurisdizionali» operato da strumenti di diritto materiale di settore, come il già menzionato Regolamento P2B

[19] V. dottrina *cit.* sub Cap. 1, n. 19.
[20] V. dottrina *cit.* sub Cap. 2, n. 63.

o il Digital Services Act (v. *supra*: Cap. 2, par. 3.1; *infra*: Cap. 6, par. 4.2, 4.3.1), resta sempre poco incline nei confronti delle norme non statali. I limiti dell'attuale sistema sono palesati anche dalla giurisprudenza richiamata nelle prossime pagine, in cui si coglie soprattutto lo sforzo di estendere e adattare i tradizionali criteri di collegamento al mondo virtuale allo scopo di trovare soluzioni di diritto positivo senza affrontare il tema del potere regolatorio dei soggetti privati che agiscono su internet.

Non si tratta, peraltro, di un'impostazione isolata, posto che anche in altri sistemi[21] di diritto internazionale privato lo spazio per le norme di fonti diverse da quelle pubbliche, e in particolare di quelle di fonte privata, appare limitato[22].

2 Le norme di diritto internazionale privato nei rapporti tra piattaforme e utenti

Concentrando la nostra analisi sulle norme di diritto internazionale privato dell'Unione europea, ci occupiamo in primo luogo della loro applicazione nei rapporti tra le piattaforme e i loro utenti, afferenti alla «dimensione verticale».

[21] V. ad esempio i Principi dell'Aja sulla scelta della legge applicabile ai contratti commerciali internazionali del 2015, il cui art. 3 sembra ammettere la possibilità che le parti scelgano una fonte di diritto non statale come «legge» applicabile ad un proprio contratto. A riguardo, si veda, *ex multis*: R. MICHAELS, *Non-State Law in the Hague Principles on Choice of Law in International Commercial Contracts*, in K. PURNHAGEN, P. ROTT (a cura di), *Varieties of European Economic Law and Regulation: Liber Amicorum for Hans Micklitz*, pp. 43-69, Springer, 2014.
I principi, assieme al relativo commentario, possono essere consultati a partire dal seguente link: https://www.hcch.net/en/instruments/conventions/specialised-sections/choice-of-law-principles

[22] Si rimanda al successivo capitolo III per un'analisi più completa sugli intrecci tra diritto di fonte pubblica e *private regulation* e sul ruolo che può giocare il diritto internazionale privato sul punto, rimanendo il focus di questa sezione sul *corpus* normativo dell'Unione.

2.1 L'architettura contrattuale alla base dei rapporti piattaforma-utente

Come si è già avuto modo di saggiare, i rapporti che animano la «dimensione verticale» delle piattaforme si fondano, innanzi tutto, su dei contratti conclusi tra i gestori di queste e i propri utenti.

A tal proposito, va innanzi tutto ricordato come si tratti di contratti segnati da un naturale squilibrio tra le parti, posto che le regole li governano – i «termini e condizioni», per richiamare il linguaggio del Regolamento P2B – sono predisposte unilateralmente dai gestori delle piattaforme e sostanzialmente non negoziabili dagli utenti. Essi si atteggiano, inoltre, a contratti a causa e oggetto[23] multiformi. Ad esempio, i problemi qualificatori descritti nella precedente sezione mostrano come i rapporti tra utenti e *provider* possano, a seconda delle circostanze, essere inquadrati, ai sensi del diritto dell'Unione, nello schema della prestazione di «servizi della società d'informazione» o in quello della fornitura dei c.d. «servizi sottostanti» (v. *supra*: Cap. 2, par. 4).

La conformazione di tali contratti – così come la disciplina ad essi eventualmente applicabile – è strettamente correlata alla qualifica dell'utente. Non di rado, ad esempio, risulta a tal fine decisivo il carattere di «consumatore» ovvero di «professionista» dell'utente della piattaforma (v. *infra* par. 2.4.1). Allo stesso modo, vi sono casi, come quelli eclatanti delle piattaforme della c.d. «*gig economy*[24]», in cui è determinate stabilire se un utente possa o meno essere considerato un «lavoratore» ai sensi del diritto dell'Unione (v. *infra* par. 2.3.1).

---

[23] L'utilizzo di queste categorie di diritto civile interno, sconosciute al diritto dell'Unione, risponde a finalità prettamente descrittive.

[24] Per una completa illustrazione del concetto di «*gig economy*» e delle sue cadute a livello di diritto del lavoro su scala internazionale si vedano, *ex multis*: V. DE STEFANO, *The Rise of the "Just-in-time Workforce": On-Demand Work, Crowdwork and Labour Protection in the "Gig-Economy"*, Organizzazione Internazionale del lavoro, Condizioni di lavoro e occupazione, n. 71, 2016; M.A. CHERRY, *Regulatory Options for Conflicts of Law and Jurisdictional Issues in the On-Demand Economy*, Organizzazione Internazionale del lavoro, Condizioni di lavoro e occupazione, n. 106, 2019.

L'attribuzione di una di queste qualifiche ha delle ricadute significative anche ai sensi del diritto internazionale privato dell'Unione. Infatti, tanto il Regolamento Roma I quanto il Regolamento Bruxelles I*bis* prevedono dei regimi speciali a favore sia dei «lavoratori[25]» (subordinati) che dei «consumatori[26]», considerati le parti deboli dei rispettivi rapporti giuridici. Un simile regime, meno rilevante nell'ambito delle piattaforme digitali, è previsto anche a protezione degli assicurati[27].

2.2 I tentativi di valorizzare il luogo di residenza o di domicilio dell'utente ai fini della competenza giurisdizionale

Rimandando soltanto di poco l'approfondimento su questi aspetti cruciali (v. *infra* par. 2.4.1 e par. 2.3.1), dal punto di vista del diritto internazionale privato va subito rilevato come dal carattere – prevalentemente ma non esclusivamente – contrattuale dei rapporti utenti-piattaforme discenda l'applicazione del Regolamento Roma I a proposito della legge applicabile e delle pertinenti disposizioni del Regolamento Bruxelles I*bis* (in particolare l'art. 7, punto 1) circa la competenza giurisdizionale.

Le riflessioni su quest'ultima norma, in particolare, hanno portato parte della dottrina[28] a teorizzare l'utilizzo del criterio del domicilio (o della residenza) dell'utente quale «luogo di esecuzione» del contratto ai fini della giurisdi-

[25] Si vedano, rispettivamente, l'art. 8 Regolamento Roma I per la legge applicabile e gli artt. 20-23 (Capo I, Sezione 5) Regolamento Bruxelles I*bis* per quanto riguarda la competenza giurisdizionale.

[26] Si vedano, rispettivamente, l'art. 6 Regolamento Roma I per la legge applicabile e gli artt. 17-19 (Capo I, Sezione 4) Regolamento Bruxelles I*bis* per quanto riguarda la competenza giurisdizionale.

[27] Si vedano, rispettivamente, l'art. 7 Regolamento Roma I per la legge applicabile e gli artt. 10-16 (Capo I, Sezione 3) Regolamento Bruxelles I*bis* per quanto riguarda la competenza giurisdizionale.

[28] I. PRETELLI, *op. cit.* sub Cap. 1, n. 11 p. 30.

zione. Tale criterio non è peraltro previsto esplicitamente da nessuna disposizione del Regolamento Bruxelles I*bis*[29]. A livello di diritto positivo, una valorizzazione della residenza dell'utente («abbonato») si ha invece nel Regolamento UE 2017/1128 relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno. In particolare, l'art. 3 di tale strumento prende come riferimento le condizioni di abbonamento di cui un abbonato beneficia nel proprio «paese di residenza» per garantirne il diritto alla portabilità dei contenuti digitali[30].

Obiettivo dell'impostazione richiamata sarebbe quello di favorire la prevedibilità della giurisdizione nell'ambiente virtuale cercando di trovare un ancoraggio facilmente individuabile con il territorio fisico. L'assunto alla base della stessa è quello per cui, spesso, sarebbe proprio «a casa» dell'attore (ossia presso la sua residenza o il suo domicilio) che si eseguirebbero le prestazioni che connotano il contratto tra utente e piattaforma: dal *download* di contenuti digitali alla ricezione di merci attraverso le piattaforme *e-commerce*. Analogamente, il domicilio (o la residenza) dell'utente può presumibilmente essere considerato il luogo attraverso cui l'utente accede alla piattaforma per fruire dei servizi offerti da essa.

I limiti di queste tesi sono in realtà facili da cogliere e si ricollegano alle analisi poc'anzi svolte sugli intrecci tra mondo virtuale e spazio fisico nell'ambito delle piattaforme (v. *supra*: par. 1.1). Così, ad esempio, se nel caso della spedi-

[29] Il domicilio dell'utente potrebbe peraltro rilevare nel caso in cui questi sia il convenuto, quale foro generale ai sensi dell'art. 4 Regolamento Bruxelles I*bis*.

[30] «1. Il fornitore di un servizio di contenuti online prestato dietro pagamento di un corrispettivo in denaro consente a un abbonato che sia temporaneamente presente in uno Stato membro di accedere al servizio di contenuti online e di fruirne con le stesse modalità del servizio offerto nello Stato membro di residenza, anche assicurando l'accesso agli stessi contenuti su dispositivi identici per numero e categoria, per lo stesso numero di utenti e con la medesima gamma di funzionalità […]» (art. 3, par. 1 Regolamento UE 2017/1128).

zione di merci acquistate attraverso una piattaforma *e-commerce* è agevole individuare il luogo fisico di esecuzione del contratto, è anche vero che questo potrebbe non corrispondere al domicilio dell'utente ma ad un altro indirizzo. Ancora più incerto è l'utilizzo di tale impostazione nell'ambito delle piattaforme da cui si originano rapporti destinati ad esaurirsi nello spazio virtuale. Eclatanti sono i casi dei *social network* o delle piattaforme di *streaming*, a cui un utente potrebbe accedere da tanti luoghi diversi da quello di residenza o domicilio e lì effettuare il *download* di un contenuto digitale.

A livello interno, di recente[31] la Corte di Cassazione ha utilizzato il criterio del domicilio dell'attore per risolvere una questione di competenza giurisdizionale relativa all'applicazione dell'art. 33 della Convenzione di Montreal del 1999 sul trasporto aereo internazionale[32]. La pronuncia in questione, pur non riguardando il diritto internazionale privato dell'Unione, è comunque interessante ai nostri fini in quanto conferma l'attività creativa della giurisprudenza quando si tratta di interpretare i criteri di collegamento internazionalprivatisti e applicarli alle fattispecie relative a internet.

La controversia all'attenzione della Suprema Corte riguardava un'azione risarcitoria intentata da dei passeggeri domiciliati in Italia nei confronti di una compagnia aerea extraeuropea a seguito della contrattazione e dell'acquisto di alcuni biglietti aerei, avvenuti interamente *online*. I Giudici di legittimità hanno quindi affermato che, in tali casi, la giurisdizione possa essere incardinata presso il domicilio dell'acquirente, individuato dalla Cassazione come il

[31] Cass., sez. un. civ., ordinanza 8 luglio 2019, n. 18257 – ECLI:IT:CASS:2019:19453CIV.

[32] Nome completo: Convenzione per l'unificazione di alcune norme relative al trasporto aereo internazionale (Convenzione di Montreal), approvata per conto della Comunità europea con Decisione 2001/539/CE – Decisione del Consiglio, del 5 aprile 2001, relativa alla conclusione da parte della Comunità europea della convenzione per l'unificazione di alcune norme relative al trasporto aereo (convenzione di Montreal).

luogo dello «stabilimento a cura del quale il contratto è stato concluso», rilevante ai sensi dell'art. 33, par. 1 della Convenzione.

Nel motivare la propria decisione, la Corte ha fatto più volte riferimento ai principi del diritto internazionale privato dell'Unione, pur non essendo – come detto – quest'ultimo applicabile. In particolare, i giudici di legittimità si sono soffermati sui principi di prevedibilità e prossimità sottesi al Regolamento Bruxelles I*bis* e sulla loro tutela nel mondo virtuale. Alla luce dei predetti principi, è stata quindi esclusa la rilevanza, ai fini della competenza giurisdizionale, di elementi come lo stabilimento della compagnia aerea o la localizzazione dei server. Quest'ultimo, in particolare, è previsto in materia penale dalla Convenzione di Budapest[33] ma era già stato rigettato dalla Corte di Giustizia dell'Unione europea[34] nell'ambito di una controversia in materia di lesioni di diritti di proprietà intellettuale attraverso internet (v. *infra*: par. 4.2). Enfasi è stata posta dalla Cassazione anche sui regimi speciali a tutela delle parti deboli previsti dallo stesso Regolamento Bruxelles I*bis*, in particolare con riferimento ai consumatori.

Il ragionamento della Corte, pur apprezzabile nell'intento di proteggere le parti deboli del contratto, solleva tuttavia più di una perplessità[35] in quanto il riferimento al diritto dell'Unione appare poco conferente nell'ambito di una decisione relativa ad una convenzione internazionale che, anche se conclusa direttamente dalla Comunità europea (oggi Unione), deve essere interpretata in maniera autonoma secondo quanto previsto dalla Convenzione di Vienna

[33] Convenzione sulla criminalità informatica (STE no. 185), adottata in seno al Consiglio d'Europa il 23 novembre 2001 ed eseguita in Italia con legge 18 marzo 2008, n. 48.
[34] CGUE, causa C-523/10, *Wintersteiger AG* c. *Products 4U Sondermaschinenbau GmbH*, 19 aprile 2012 – ECLI:EU:C:2012:220 (v. in particolare punto 36).
[35] Per un commento sulla decisione si veda: G. MONGA, *Italian Supreme Court Rules on Jurisdiction under the Montreal Convention*, apparso su Eapil.blog, 9 aprile 2020, disponibile online: https://eapil.org/2020/04/09/italian-supreme-court-rules-on-jurisdiction-over-passengers-claims-to-damages-under-the-montreal-convention/

sul diritto dei trattati del 1969[36]. Peraltro, se si considera lo stesso Regolamento Bruxelles I*bis*, si constata come il criterio del domicilio dell'acquirente sia in realtà ad esso pressoché sconosciuto, potendo rilevare al più soltanto in materia consumeristica oltre che, eventualmente, quale foro del convenuto secondo la regola generale di cui all'art. 4.

2.3 La protezione degli utenti «lavoratori» ai sensi del diritto internazionale privato

Spostando la nostra attenzione sui regimi a protezione delle parti deboli, si inizia, per ragioni espositive, da quelli a tutela dei «lavoratori», per poi soffermarsi su quelle a protezione dei consumatori, seguendo quindi un ordine inverso rispetto a quello dei pertinenti strumenti del diritto dell'Unione.

In particolare, le norme che stabiliscono regimi a tutela dei «lavoratori» sono l'art. 8 del Regolamento Roma I per quanto riguarda la legge applicabile e gli artt. 20-23 (Capo II, Sezione 5) del Regolamento Bruxelles I*bis* a proposito della competenza giurisdizionale. Si tratta di disposizioni da leggere in stretta correlazione, in quanto l'obiettivo del legislatore dell'Unione è quello della coerenza tra i due strumenti di diritto internazionale privato e le soluzioni da essi fornite[37].

2.3.1 Problemi qualificatori: tra «lavoratori» subordinati e autonomi

L'applicazione dei regimi internazionalprivatistici a tutela dei lavoratori nell'ambito delle piattaforme solleva, innanzi tutto, diversi problemi qualificatori, che si intrecciano con le riflessioni già svolte a proposito della natura

[36] Convenzione di Vienna sul diritto dei trattati, conclusa a Vienna il 23 maggio 1969, eseguita in Italia con legge 12 febbraio 1974, n. 112. Si veda in particolare la Sezione 3 (artt. 31-33) sull'Interpretazione dei Trattati.

[37] V. considerando 7 Regolamento Roma I. Per approfondire: C. SCHMON, *The Interconnection of the EU Regulations Brussels I Recast and Rome I*, Springer, 2020.

stessa dalle piattaforme ai sensi del diritto dell'Unione (v. *supra*: Cap. 2, par. 4).

I problemi in questione sorgono, in *primis*, nell'ambito delle piattaforme relative alla c.d. «*gig economy*», ed in particolare di quelle di «*crowdworking*», attraverso cui delle persone offrono – dietro accordo con la piattaforma stessa – dei servizi o delle prestazioni lavorative a favore di altri utenti. Con riguardo a tali soggetti, si è posta a più riprese la questione se essi debbano essere considerati come lavoratori autonomi, eventualmente fornitori dei servizi «sottostanti» alla piattaforma, oppure come dei veri e propri «lavoratori[38]» ad essa subordinati. Si tratta di una questione molto dibattuta, che ha avuto e ha tuttora diverso risalto mediatico per via delle ricadute sociali e le tutele di tipo giuslavoristico[39] che quest'ultima qualifica porta con sé. Si pensi, ad esempio, a piattaforme come Uber Eats, Deliveroo o Glovo, la cui rapida diffusione è stata facilitata dalla «zona grigia[40]» che, specialmente all'inizio, contraddistingueva i rapporti tra esse ed i propri *rider*, sospesi tra la qualifica di lavoratori autonomi e quella di dipendenti.

Il tema è risultato divisivo tanto a livello di Unione europea quanto a livello di Stati membri. In Italia, ad esempio, al culmine di una dibattuta vicenda giudiziaria, la Corte di Cassazione ha confermato, nel 2020, come ai *rider* delle piattaforme di *delivery*, i quali svolgono di mansioni di fattorino normalmente

---

[38] V. considerando 14 Regolamento Bruxelles I*bis*.

[39] Vedi *ex multis*: V. DE STEFANO, *op. cit.* 24; M.A. CHERRY, *op. cit.* 24; M.A. CHERRY, V. DE STEFANO, *Reflecting on the Roundtable: Online Worker's Rights and Conflicts of Law*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 213-224, Schulthess, 2018.

[40] Si tratta di un'espressione usata testualmente dalla Corte di Cassazione nella sentenza Cass. Sez. Lav. n. 1660, 24 gennaio 2020 (v. in particolare par. 27).

inquadrati in base a contratti di collaborazione coordinata e continuativa, vadano riconosciute le tutele dei lavoratori subordinati[41]. Al contrario, la Corte di Appello di Parigi ne ha a più riprese sancito la natura di lavoratori autonomi[42] ai sensi del diritto francese, similmente a quanto fatto, ai sensi del diritto belga, dal Tribunale del Lavoro di Bruxelles nel dicembre 2021[43]. Contrasti sono sorti anche negli Stati Uniti[44], ove hanno sede alcune tra le maggiori piattaforme di «*crowdworking*» del mondo.

Rimandando a più puntuali e completi approfondimenti sul punto[45], ai nostri fini occorre constatare come, a livello di diritto dell'Unione, non siano sinora state raggiunte soluzioni comuni.

Negli anni, peraltro, la Corte di Giustizia ha elaborato una nozione di «lavoratore[46]» (dipendente) ai sensi del diritto dell'Unione. Secondo tale giurisprudenza, in particolare: «La caratteristica essenziale del rapporto di lavoro è la circostanza che una persona fornisca, per un certo periodo di tempo, a favore di un'altra e sotto la direzione di quest'ultima, prestazioni in contropartita

---

[41] Idem, per approfondire si veda, *ex multis*: AA.VV., *Massimario della giurisprudenza del lavoro*, numero speciale, giugno 2020.

[42] V. ad esempio: Cour d'appel de Paris, Pôle 6, Chambre 2, *YZ* v. *Deliveroo France*, n. 16/12875, 9 novembre 2017. Disponibile su: https://www.doctrine.fr/d/CA/Paris/2017/C125532D4. Per un commento si rimanda a M.A. CHERRY, V. DE STEFANO, *op. cit.* sub nota 39, p. 217.
Più di recente si veda: Cour d'appel de Paris, Pôle 6, Chambre 4, n. 18/028467, aprile 2021. Disponibile su: https://www.doctrine.fr/d/CA/Paris/2021/C222796DD80DCC4BA87B3.

[43] V. *Commission Administrative de règlement de la relation de travail* (CRT), n. 116-FR- 20180209, 23 febbraio 2018. Per un commento v. M.A. CHERRY, V. DE STEFANO, *op. cit.* sub nota 39, p. 217.

[44] Idem, p. 216.

[45] V. dottrina *cit.* sub nota 39.

[46] V. in particolare: CGUE, causa C-53/81, *D.M. Levin* c. *Segretario di Stato per la giustizia*, 23 marzo 1982 – ECLI:EU:C:1982:105; CGUE, causa C-66/85, *Deborah Lawrie-Blum* c. *Land Baden-Wurttemberg*, 3 luglio 1986 – ECLI:EU:C:1986:284; CGUE, causa C-85/96, *María Martínez Sala* c. *Freistaat Bayern*, 12 maggio 1998 – ECLI:EU:C:1998:217; CGUE, causa C-337/97, *C.P.M. Meeusen* c. *Hoofddirectie van de Informatie Beheer Groep*, 8 giugno 1999 – ECLI:EU:C:1999:284; CGUE, causa C-138/02, *Brian Francis Collins* c. *Secretary of State for Work and Pensions*, 23 marzo 2004 – ECLI:EU:C:2004:172.

delle quali riceva una retribuzione[47]». Gli insegnamenti della Corte devono essere utilizzati per tutte le norme dell'Unione in cui rilevi la nozione di «lavoratore», inclusi gli strumenti di diritto internazionale privato.

Nell'ambito delle piattaforme digitali, tuttavia, l'applicazione di tali principi risulta ancora problematica. Alcune indicazioni sono state fornite dalla Commissione europea nella già menzionata Comunicazione sull'economia collaborativa[48]. In tale documento, in particolare, l'Esecutivo europeo ha affermato che per stabilire se l'utente-prestatore dei «servizi sottostanti» possa o meno essere considerato come un lavoratore subordinato della piattaforma, occorre effettuare una valutazione caso per caso basata su tre criteri, discendenti dalla richiamata giurisprudenza della Corte. Il primo di essi è l'esistenza di un rapporto di subordinazione che, a parere dell'Esecutivo, si ha nel caso in cui il prestatore agisca sotto la direzione della piattaforma, la quale determina la scelta dell'attività e dei servizi da prestare, la retribuzione e le condizioni di lavoro.

Il secondo criterio è la natura del lavoro, ossia che il prestatore del servizio sottostante deve svolgere un'attività avente valore economico reale ed effettivo, escluse le attività talmente modeste da potersi definire puramente marginali ed accessorie. Si tratta di un punto delicato, come peraltro suggerisce la stessa espressione «*gig economy*» (letteralmente «economia dei lavoretti»). Come ricorda la stessa Commissione, infatti, nel contesto dell'economia collaborativa diversi prestatori forniscono effettivamente servizi che possono essere considerati come «puramente marginali ed accessori», il che porterebbe ad escluderne la qualifica di lavoratori. D'altro canto, l'Esecutivo dell'Unione avverte come la breve durata, l'orario di lavoro ridotto, il lavoro discontinuo

[47] V: CGUE, *Lawrie-Blum*, punti 16-17; CGUE, *Martinez Sala*, punto 32; CGUE, *Meeusen*, punto 13; CGUE, *Collins*, punto 26.
[48] V. COM(2016) 356 final, 2 giugno 2016, *cit.* sub Cap. 2, nota n. 42.

o la bassa produttività non possano di per sé escludere l'esistenza di un rapporto di lavoro e ricorda come l'effettiva definizione dello *status* dipenda da un esame globale di tutti e tre i criteri.

Il terzo ed ultimo criterio è quello della retribuzione, che viene usato principalmente per distinguere un volontario da un lavoratore. Esso non sarebbe quindi soddisfatto nel caso in cui il prestatore non ricevesse alcuna retribuzione, o ricevesse unicamente un rimborso dei costi sostenuti per lo svolgimento delle sue attività.

Le indicazioni della Commissione non hanno tuttavia eliminato le incertezze sul punto. Nel tentativo di cercare una soluzione, un'interessante dottrina[49] ha provato a far discendere la qualifica di «lavoratore» subordinato di una piattaforma dai medesimi parametri considerati dalla Corte di Giustizia UE nelle sentenze *Uber* – e prima ancora dalla Commissione nella poc'anzi richiamata comunicazione sull'economia collaborativa – per qualificare una piattaforma come fornitore di «servizi della società dell'informazione» ovvero del «servizio sottostante» ad essa (v. *supra*: Cap. 2, par. 4). In particolare, a parere di tale dottrina, la circostanza che una piattaforma, come nel caso di Uber, eserciti un'influenza determinante sui servizi sottostanti offerti dai propri utenti-prestatori farebbe sì che questi ultimi possano essere qualificati come «lavoratori» subordinati della medesima piattaforma ai sensi del diritto dell'Unione.

Una sistemazione definitiva della questione potrebbe arrivare, *de jure condendo*, dall'approvazione della proposta di direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali presentata dalla Commissione europea nel dicembre 2021[50]. L'obiettivo della proposta è

[49] V. I. PRETELLI, *op. cit.* sub Cap. 1, n. 11, p. 31. Della stessa autrice si veda anche I. PRETELLI, *op. cit.* n. 2, p. 9.

[50] Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali*, COM(2021) 762 fi-

quello di «migliorare le condizioni di lavoro e i diritti sociali delle persone che lavorano mediante piattaforme digitali, anche al fine di sostenere le condizioni per una crescita sostenibile delle piattaforme di lavoro digitali nell'Unione europea».

Senza pretese di esaustività circa i contenuti di tale proposta e le sue ricadute giuslavoristiche, ai nostri fini, è importante rilevare come essa fornisca sia una definizione di «persona che svolge un lavoro mediante piattaforme digitali[51]» sia una di «lavoratore delle piattaforme digitali[52]». Le due figure sono poste in un rapporto genere-specie. In particolare, la prima categoria racchiude tutti coloro che lavorano mediante le piattaforme digitali, indipendentemente dalla qualificazione contrattuale dei loro rapporti con la piattaforma. La seconda indica invece «qualsiasi persona che svolge un lavoro mediante piattaforme digitali e ha un contratto di lavoro o un rapporto di lavoro quali definiti dal diritto, dai contratti collettivi o dalle prassi in vigore negli Stati membri, tenuto conto della giurisprudenza della Corte di giustizia», riferendosi pertanto ai lavoratori subordinati in senso proprio.

---

nal, 9 dicembre 2021. Per approfondire v. M. BARBIERI, *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in Labour & Law Issues, Vol. 7, n. 2, 2021, disponibile online: https://labourlaw.unibo.it/article/view/14110.

[51] Ai sensi dell'art. 2, par. 1, n. 1) della proposta, si definisce «persona che svolge un lavoro mediante piattaforme digitali»: «qualsiasi persona fisica che svolge un lavoro mediante piattaforme digitali, indipendentemente dalla qualificazione contrattuale, da parte delle parti interessate, del rapporto tra tale persona e la piattaforma di lavoro digitale». L'art. 2, par. 1, n. 2) definisce invece «lavoro mediante piattaforme digitali»: «qualsiasi lavoro organizzato tramite una piattaforma di lavoro digitale e svolto nell'Unione da persone fisiche sulla base di un rapporto contrattuale tra la piattaforma di lavoro digitale e la persona fisica, indipendentemente dal fatto che esista o no un rapporto contrattuale tra tale persona e il destinatario del servizio».

[52] Ai sensi dell'art. 2, par. 1, n. 3) della proposta, si definisce «persona che svolge un lavoro mediante piattaforme digitali»: «qualsiasi persona fisica che svolge un lavoro mediante piattaforme digitali, indipendentemente dalla qualificazione contrattuale, da parte delle parti interessate, del rapporto tra tale persona e la piattaforma di lavoro digitale».

La proposta stabilisce inoltre una presunzione legale a tutela della parte debole, in quanto, ai sensi dell'art. 4, par. 1: «Si presume che il rapporto contrattuale tra una piattaforma di lavoro digitale che controlla, ai sensi del paragrafo 2[53], l'esecuzione del lavoro e una persona che svolge un lavoro mediante tale piattaforma sia un rapporto di lavoro». Le disposizioni successive specificano meglio il carattere di tale presunzione e le possibilità per confutarla (art. 5).

Va infine segnalato come l'approvazione della proposta, al netto della necessità di un recepimento da parte di ciascuno Stato membro, consentirebbe una generale attribuzione della qualifica di «lavoratore» alle persone che lavorano mediante piattaforme digitali anche ai sensi del diritto internazionale privato dell'Unione, rendendo quindi possibile l'applicazione a favore di essi dei regimi speciali ivi previsti.

2.3.2 Problematiche relative all'applicazione delle norme e dei criteri di collegamento di diritto internazionale privato

Detto delle questioni qualificatorie ancora rimaste senza soluzione, problematiche ed incertezze derivano anche dall'effettiva applicabilità, nell'ambito delle piattaforme digitali, dei regimi speciali previsti dal diritto internazionale privato dell'Unione a favore dei lavoratori.

Ricordando brevemente quanto disposto dalle norme e cominciando dalla competenza giurisdizionale, l'art. 21 del Regolamento Bruxelles I*bis* consente

[53] Ai sensi del citato art. 4, par. 2 della proposta: «Il controllo dell'esecuzione del lavoro ai sensi del paragrafo 1 è inteso come caratterizzato dalla presenza di almeno due dei seguenti elementi: a) determinazione effettiva del livello della retribuzione o fissazione dei limiti massimi per tale livello; b) obbligo, per la persona che svolge un lavoro mediante piattaforme digitali, di rispettare regole vincolanti specifiche per quanto riguarda l'aspetto esteriore, il comportamento nei confronti del destinatario del servizio o l'esecuzione del lavoro; c) supervisione dell'esecuzione del lavoro o verifica della qualità dei risultati del lavoro, anche con mezzi elettronici; d) effettiva limitazione, anche mediante sanzioni, della libertà di organizzare il proprio lavoro, in particolare della facoltà di scegliere l'orario di lavoro o i periodi di assenza, di accettare o rifiutare incarichi o di ricorrere a subappaltatori o sostituti; e) effettiva limitazione della possibilità di costruire una propria clientela o di svolgere lavori per terzi.

al lavoratore domiciliato in uno Stato membro di convenire il datore di lavoro, a propria scelta, davanti all'autorità giudiziaria dello Stato presso cui egli ha il suo domicilio oppure del luogo in cui o a partire dal quale svolge o svolgeva il proprio lavoro (nel caso di più paesi, davanti al giudice dello Stato in cui è situata la sede d'attività presso cui il lavoratore è stato assunto). Il datore di lavoro può, di contro, convenire il lavoratore soltanto nel luogo in cui quest'ultimo è domiciliato (art. 22). Ulteriore tutela a favore del lavoratore è la (parziale) limitazione dell'autonomia delle parti prevista dall'art. 23, in base al quale è possibile derogare alle disposizioni di cui agli artt. 21 e 22 soltanto con un accordo posteriore al sorgere della controversia o che consenta al lavoratore di adire un'autorità giurisdizionale diversa da quelle indicate in tali norme. Il regime appena descritto è un regime tendenzialmente esaustivo ed autosufficiente che generalmente disciplina in maniera esclusiva tutte le fattispecie relative ai lavoratori[54].

Per quanto riguarda la legge applicabile, la norma di riferimento è l'art. 8 del Regolamento Roma I. La stessa prevede, al par. 1, che un «contratto individuale di lavoro[55]» sia di regola disciplinato dalla legge scelta dalle parti (ai sensi dell'art. 3 del medesimo regolamento). Alla luce delle finalità di tutela della parte debole perseguite della norma, tale scelta non può, peraltro, privare il lavoratore della protezione assicuratagli dalle disposizioni alle quali

[54] V. P. FRANZINA, *op. cit.* 14, p. 115.

[55] Secondo la giurisprudenza della Corte di Giustizia: «I contratti di lavoro, come altri contratti in fatto di lavoro subordinato, hanno, rispetto agli altri contratti, anche quando questi riguardano prestazioni di servizi, determinate particolarità, in quanto creano un nesso durevole che inserisce il lavoratore nell' ambito di una determinata organizzazione dell'attività dell'impresa o del datore di lavoro e in quanto si ricollegano al luogo dell'esercizio dell'attività, il quale determina l'applicazione di norme imperative e di contratti collettivi». Si vedano a questo proposito: CGUE, causa C-266/85, *Hassan Shenavai* c. *Klaus Kreischer*, 15 gennaio 1987 – ECLI:EU:C:1987:11 (punto 16); CGUE, causa C-32/88, *Six Constructions Ltd* c. *Paul Humbert*, 15 febbraio 1989 – ECLI:EU:C:1989:68 (punto 10).

non è permesso derogare convenzionalmente in base alla legge che sarebbe stata applicabile in mancanza di scelta.

A tal proposito, sono i paragrafi successivi che dettano una serie di criteri «a cascata» per individuare la legge applicabile in assenza di scelta. L'art. 8, par. 2 richiama in primo luogo la legge del «paese nel quale, o in mancanza a partire dal quale, il lavoratore, in esecuzione del contratto, svolge abitualmente il suo lavoro». Per il caso in cui sia non sia possibile applicare tale criterio, «il contratto è disciplinato dalla legge del paese nel quale si trova la sede che ha proceduto ad assumere il lavoratore» (art. 8, par. 3). L'art. 8, par. 4 contiene infine una clausola di salvaguardia, a mente della quale nel caso in cui il contratto presenti un collegamento più stretto con un paese diverso da quello indicato nei paragrafi 2 e 3, si applica la legge di tale paese.

Le questioni poste dall'utilizzo delle norme appena richiamate nell'ambito delle piattaforme digitali sono di due tipi. Il primo, prettamente internazionalprivatistico, attiene ai già richiamati problemi di prevedibilità e di effettività delle soluzioni di diritto internazionale privato. Il secondo coinvolge invece considerazioni di natura materiale, che hanno a che fare con fenomeni di *dumping* sociale e di «*race to the bottom*».

A proposito dei problemi del primo tipo, il cuore di essi attiene all'individuazione del luogo in cui o a partire da cui il lavoratore svolge il proprio lavoro, allo scopo di localizzare la fattispecie. L'operazione in questione risulta agevole nell'ambito di piattaforme, come Uber o Deliveroo, in cui l'esecuzione delle mansioni di parte del lavoratore (al netto delle problematiche qualificatorie di cui si è appena detto) avviene integralmente in un luogo fisico. Totalmente diverso è invece il caso delle piattaforme di *crowdworking* (come Amazon Mechanical Turk) in cui le prestazioni lavorative vengono assegnate ed eseguite integralmente *online*.

A tal riguardo, similmente a quanto fatto in materia di contratti, parte della dottrina[56] ha tentato di valorizzare il criterio della residenza abituale (ovvero del domicilio per quanto attiene al Regolamento Bruxelles I*bis*) quale «luogo» a partire dal quale il lavoratore accederebbe alla piattaforma di *crowdworking* per svolgere il proprio lavoro. Tale approccio, pur se condivisibile anche alla luce dell'obiettivo perseguito dalle norme di proteggere il lavoratore garantendo al contempo la prevedibilità delle soluzioni internazionalprivatistiche, non appare tuttavia idoneo a risolvere tutte le incertezze connaturate alla natura delle piattaforme in esame, le quali permettono ad un utente di accedere da qualsiasi luogo ed ivi svolgere le proprie prestazioni.

Le problematiche del secondo tipo si collocano a valle dell'operazione di localizzazione della fattispecie e riguardano gli standard giuslavoristici del diritto materiale richiamato dalle norme di conflitto del Regolamento Roma I. Quest'ultimo, nella maggior parte dei casi e al netto delle incertezze appena ricordate, coinciderà, peraltro, con quello del foro competente individuato ai sensi del Regolamento Bruxelles I*bis*, alla luce dell'obiettivo di coerenza tra gli strumenti di diritto internazionale privato perseguito dal legislatore dell'Unione[57]. L'ordinamento giuridico in questione sarà spesso quello dello Stato in cui (o a partire da cui) il lavoratore svolge le proprie mansioni, le cui regole inderogabili a protezione del lavoratore troveranno applicazione nonostante scelte di legge in senso contrario, come previsto dall'art. 8, par. 1.

Come rilevato da più parti in dottrina[58], questa soluzione va tendenzialmente salutata con favore nell'ambito di piattaforme in cui il lavoratore esegue le proprie prestazioni in uno spazio fisico, in quanto consente allo stesso di beneficiare dei medesimi standard di protezione dei propri concorrenti che non

[56] I. PRETELLI, *op. cit.* 2, p. 8.
[57] I. PRETELLI, *op. cit*. sub Cap. 1, n. 11, p. 31.
[58] Idem. p. 33.

lavorano attraverso le piattaforme. Viceversa, per quanto riguarda le piattaforme di «*crowdworking*», in cui il luogo di esecuzione del lavoro va ricercato potenzialmente a livello globale, il rischio rilevato dalla dottrina[59] attiene alla diffusione di fenomeni di concorrenza sleale, *dumping* sociale e «*race to the bottom*», con un progressivo abbassamento degli standard giuslavoristici previsti dai vari ordinamenti nazionali allo scopo di attrarre (o assecondare) la diffusione di tali piattaforme. Tale rischio, se si considera il carattere universale[60] del Regolamento Roma I, può peraltro coinvolgere anche ordinamenti di Stati terzi, i cui standard in materia di diritto del lavoro possono essere assai più bassi di quelli dell'Unione europea. Per contrastare i suddetti fenomeni, si è da più parti invocata l'adozione di standard comuni a livello internazionale[61], anche nella forma di strumenti di *soft law*. Non è questa la sede per ulteriori approfondimenti sul punto: basti ai nostri fini ribadire come una possibile soluzione, quanto meno a livello di Unione europea, potrebbe discendere dall'adozione della già menzionata proposta di direttiva del dicembre 2021.

2.4 La protezione degli utenti «consumatori»

Un'altra categoria di soggetti «deboli» tutelati dal diritto internazionale privato dell'Unione e la cui protezione risulta assai rilevante nell'ambito delle piattaforme digitali sono i consumatori. Le disposizioni a tutela degli stessi sono, rispettivamente, l'art. 6 del Regolamento Roma I per quanto riguarda la

---

[59] Idem. p. 33. V. anche: M.A. CHERRY, V. DE STEFANO, *op. cit.* sub nota 39; M.A. CHERRY, *op. cit.* sub nota 24.

[60] V. art. 2 Regolamento Roma I: «La legge designata dal presente regolamento si applica anche ove non sia quella di uno Stato membro». Per approfondire: F. RAGNO, *Article 2 Universal Application*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 55-57, Cambridge University Press, 2020.

[61] Si veda a questo proposito: M.A. CHERRY , *op. cit.* 24 (pp. 28, 33-37). L'autrice in particolare afferma: «*Corporate social responsibility and corporate codes of conduct can set best practices and standards for computer crowdwork; these forms of "soft law" cross borders and can be influential*». V. anche: I. PRETELLI, *op. cit*. Cap. 1, n. 11, p. 46; M.A. CHERRY, V. DE STEFANO, *op. cit.* sub nota 39, p. 222.

legge applicabile e gli artt. 17-19 (Capo II, Sezione 5) del Regolamento Bruxelles I*bis* in relazione alla competenza giurisdizionale.

2.4.1 Problemi qualificatori: tra «consumatori» e «professionisti»

Analogamente a quanto accade per i lavoratori, anche l'applicazione delle norme di diritto internazionale privato a tutela dei consumatori solleva, in primo luogo, diverse questioni di tipo qualificatorio. Tali questioni, su cui esiste peraltro copiosa giurisprudenza, sono state abbondantemente affrontate dalla dottrina – anche a prescindere dalle piattaforme digitali – e sono di seguito trattate in breve per quanto funzionale ai fini del presente lavoro, rimandando ad altre sedi[62] per specifici ed ulteriori approfondimenti attinenti alla materia consumeristica.

Nell'affrontare le suddette tematiche, occorre in primo luogo rilevare come il diritto dell'Unione europea fornisca da più parti[63] delle definizioni di «consumatore». Salvo piccole differenze testuali[64], questa figura è ovunque individuata come una «persona fisica» che, ai sensi dello strumento normativo di

---

[62] V. *ex multis*: P. FRANZINA, *Norme di conflitto comunitarie in materia di contratti con consumatori e corretto funzionamento del mercato interno*, in Rivista di diritto internazionale, Vol. 92, fasc. 1, pp. 122-129, 2009; F. RAGNO, *The Law Applicable to Consumer Contracts under the Rome I Regulation*, in F. FERRARI, S. LEIBLE (a cura di), *Rome I – The Law Applicable to Contractual Obligations in Europe,* pp.129-170, Sellier European Law Publishers, 2009; Z. S. TANG, *Electronic Consumer Contracts in the Conflict of Laws*, Hart Publishing, 2018; F. RAGNO, *Article 6 Consumer Contracts*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 161-162, Cambridge University Press, 2020.

[63] Per le definizioni di «consumatore» nell'ordinamento dell'Unione si vedano, *ex multis*: Art. 2, lett. b) Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori; Art. 2, punto 1 Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011 , sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio.

[64] Per i rischi relativi alle parziali differenze definitorie si veda Commissione europea, *Libro verde – Revisione dell'acquis relativo ai consumatori*, COM (2006) 744 definitivo, 8 febbraio 2007 (in particolare p. 16).

volta in volta considerato, agisce per un fine che può essere considerato «estraneo alla sua attività commerciale o professionale». La figura del «consumatore», definita in questi termini tanto dal Regolamento Roma I (art. 6, par. 1) che dal Regolamento Bruxelles I*bis* (art. 17, par. 1), si contrappone a quella del «professionista», vale a dire qualsiasi «persona [fisica o giuridica] che agisce nell'esercizio della sua attività commerciale o professionale[65]». Quest'ultimo è considerato dal legislatore come la «parte forte» del rapporto.

Sin dagli anni '70, la giurisprudenza della Corte di Giustizia[66] ha elaborato una serie di criteri per stabilire, in concreto, se un soggetto ricada in una delle due categorie ai sensi del diritto internazionale privato dell'Unione. In particolare, secondo le ultime indicazioni dei giudici di Lussemburgo, la nozione di «consumatore», ai fini internazionalprivatistici:

> *«Deve essere interpretata in maniera restrittiva, facendo riferimento alla posizione di tale persona in un determinato contratto, in relazione alla natura ed alla finalità di quest'ultimo, e non invece alla situazione soggettiva di quella stessa persona, potendo un solo e medesimo soggetto essere considerato un consumatore nell'ambito di determinate operazioni ed un operatore economico nell'ambito di altre[67]».*

L'approdo in questione chiarisce dunque come la qualifica del consumatore non dipenda da caratteri intrinseci propri del soggetto considerato ma sia da

---

[65] Tale definizione, coerente ad altre previste all'interno del diritto dell'Unione, è contenuta all'art. 6, par. 1 del Regolamento Roma I. La specifica tra parentesi quadra, per cui il professionista può essere sia persona fisica che giuridica, è pacificamente consolidata e sancita testualmente da altri strumenti normativi del diritto dell'Unione, quali la Direttiva 2011/83/UE (v. art. 2, n. 2).

[66] V. CGUE, causa C-150/77, *Bertrand* c. *Paul Ott KG.*, 21 giugno 1978 – ECLI:EU:C:1978:137 (punto 21).

[67] V. in particolare: CGUE, causa C-269/95, *Francesco Benincasa* c. *Dentalkit Srl*, 3 luglio 1997 – ECLI:EU:C:1997:337 (punto 16); CGUE, causa C-464/01, *Johann Gruber* c. *Bay Wa AG*, 20 gennaio 2005 – ECLI:EU:C:2005:32 (punto 36); CGUE, causa C-498/2016, *Maximilian Schrems* c. *Facebook Ireland Limited*, 25 gennaio 2018 (punto 29).

ricollegare allo specifico contratto da questi concluso. Infatti, un consumatore può – e nella pratica è sovente così – essere un soggetto che nella vita svolge un'attività di tipo professionale, anche imprenditoriale, ma che nello specifico contratto agisce per uno scopo estraneo alla sua professione. La qualifica di consumatore assume in questo modo le sembianze di «una qualità contingente e momentanea rivestita in relazione ad un atto o ad un contratto[68]».

Da quanto sopra si intuisce come la valutazione del carattere di «consumatore» o di «professionista» sia di per sé un'operazione tutt'altro che agevole, soprattutto se si considerano i casi, assai frequenti, in cui un soggetto agisce per scopi ibridi ovvero concluda contratti «promiscui», che possano sia essere funzionali alla sua attività professionale sia esserne estranei.

Di questi ultimi contratti la Corte si è occupata nella sentenza *Gruber*, nella quale, confermando l'interpretazione restrittiva della nozione di «consumatore», ha chiarito «come un soggetto che ha stipulato un contratto relativo ad un bene destinato ad un uso in parte professionale ed in parte estraneo alla sua attività professionale» non possa invocare a proprio favore il regime speciale sulla competenza giurisdizionale previsto dagli artt. 17-19 del Regolamento Bruxelles I*bis* (corrispondenti agli artt. 13-15 della Convenzione di Bruxelles vigente *ratione temporis*) «a meno che l'uso professionale sia talmente marginale da avere un ruolo trascurabile nel contesto globale dell'operazione di cui trattasi, essendo irrilevante a tale riguardo il fatto che predomini l'aspetto extraprofessionale[69]».

---

[68] E. GABRIELLI, *Il consumatore e il professionista*, in E. GABRIELLI, E. MINERVINI (a cura di), *I contratti del consumatore*, UTET, 2005.

[69] CGUE, *Gruber*, punto 54; CGUE, *Schrems*, punto 32. A livello dottrinale si veda, *ex multis*: F. RAGNO, *op. cit.* n. 62.

La distinzione tra consumatore e professionista presenta inoltre dei caratteri dinamici, in quanto un soggetto potrebbe aver concluso un contratto nelle vesti di consumatore salvo poi decidere di fruire dello stesso in qualità di professionista (si pensi ad esempio all'acquisto di un computer personale in seguito adibito a strumento di lavoro).

Anche questi aspetti sono stati affrontati in diverse occasioni dalla Corte di Giustizia. Importante sul punto è la sentenza *Benincasa*[70], relativa ad una controversia tra la società Dentalkit s.r.l. ed il Sig. Benincasa in ordine alla validità di un contratto di *franchising* per la futura apertura ed esercizio di un negozio a Monaco. In tale pronuncia, in particolare, i Giudici di Lussemburgo hanno rigettato la tesi del Sig. Benincasa, il quale si considerava consumatore ed aveva invocato la speciale tutela prevista dagli artt. 13, par. 1 e 14, par. 1 della Convenzione di Bruxelles (applicabile *ratione temporis*) facendo leva sul fatto che l'attività professionale non fosse ancora iniziata al momento della stipula del contratto. Al contrario, la Corte ha affermato il principio per cui un soggetto che abbia stipulato un contratto per l'esercizio di un'attività professionale non attuale, ma futura, non possa essere considerato un «consumatore» ai sensi del diritto internazionale privato europeo, dato che il carattere futuro di un'attività nulla toglie alla sua natura professionale.

2.4.2 La qualifica di «consumatore» nell'ambito delle piattaforme digitali: indicazioni alla luce del caso *Schrems*

L'operazione qualificatoria risulta ancora più complicata nell'ambito delle piattaforme digitali, in cui la distinzione tra «consumatore» e «professionista» si fa più sfumata ed è molto frequente che un soggetto possa agire, in momenti diversi, assumendo entrambe le vesti. Si pensi, ad esempio, a casi come e-Bay

[70] CGUE, *Benincasa*.

o Airbnb, in cui le persone possono vendere o acquistare merce così come offrire o prendere in locazione appartamenti agendo indifferentemente per scopi estranei o attinenti alla propria professione. Ciò, peraltro, senza che la propria controparte ne possa essere *ex ante* consapevole e a nulla rilevando eventuali qualificazioni contenute nei «termini e condizioni» della piattaforma.

La distinzione si fa ancora più sottile nell'ambito di piattaforme per la condivisione di contenuti e di *social network*, ove sovente si intrecciano la vita personale e professionale di una persona. Si pensi ad esempio al caso di un *influencer* che invii messaggi di auguri o di amore a parenti, amici o partner attraverso il proprio profilo, solitamente utilizzato per scopi professionali. Si pensi ancora al caso della persona che decida di trasformare il proprio profilo di *social network*, sino a quel momento utilizzato soltanto a fini personali, in un canale attraverso cui vendere libri, raccogliere fondi o comunque diffondere contenuti rilevanti per la propria attività professionale.

Proprio su questi aspetti, importanti chiarimenti sono stati forniti dalla Corte di Giustizia nella sentenza *Schrems*[71], recentemente ripresa e confermata dalla decisione sul caso *Personal Exchange International Limited*[72]. La pronuncia in questione è parte di un filone giudiziario che vede contrapposto l'attivista austriaco per la *privacy* Maximillian Schrems a Facebook, resa famosa da due importanti pronunce[73] in materia di trasferimenti dei dati personali verso gli Stati Uniti d'America.

---

[71] CGUE, *Schrems* (2018).

[72] CGUE, causa C-774/19, *A. B. e B. B.* c. *Personal Exchange International Limited*, 20 dicembre 2020 – ECLI:EU:C:2020:1015 (punto 42).

[73] Si tratta delle due pronunce relative al trasferimento dei dati personali a partire dall'Unione europea verso gli Stati Uniti d'America con cui la Corte di Giustizia ha dichiarato l'invalidità delle decisioni con cui la Commissione europea aveva considerato adeguato, ai sensi dell'art. 26 direttiva 95/46/CE, il livello di protezione dei dati personali garantito, rispettivamente, dai meccanismi noti come *Safe Harbour* e *EU-US Privacy Shield.* Per le relative decisioni: 2000/520/CE: Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai

Nella decisione in commento, invece, i giudici di Lussemburgo sono stati chiamati a pronunciarsi sulla possibilità di qualificare «consumatore», ai sensi delle pertinenti disposizioni del Regolamento Bruxelles I (vigente *ratione temporis*), lo stesso Sig. Schrems nell'ambito del proprio rapporto contrattuale con la nota piattaforma di *social network*. Il rapporto in questione aveva infatti conosciuto un'evoluzione dinamica simile a quelle descritte in precedenza. Nello specifico, Schrems aveva aperto un account Facebook nel 2008 per esclusivi scopi privati ma, dal 2011, aveva iniziato ad utilizzare una nuova pagina appositamente creata per informare gli utenti delle azioni giudiziarie intraprese contro la piattaforma e delle altre iniziative a tutela della *privacy* da egli portate avanti, oltre che per ottenere delle donazioni e pubblicizzare i suoi libri[74]. Se, pertanto, non vi erano dubbi che dal 2008 sino al 2011 Schrems avesse utilizzato i servizi di Facebook agendo come «consumatore», altrettanto non poteva dirsi a seguito dell'apertura della nuova pagina.

Nel pronunciarsi sulla questione, i Giudici di Lussemburgo hanno innanzi tutto ricordato come, ai fini qualificatori, occorra tenere conto, nell'ambito dei servizi di *social network* digitali che hanno tendenza ad essere utilizzati su un lungo periodo, dell'evoluzione dell'uso che viene fatto di tali servizi nel tempo. In particolare, secondo la Corte, un utente può invocare la qualità di consumatore soltanto se, avendo originariamente concluso un contratto per un uso essenzialmente non professionale di tali servizi, non abbia in seguito iniziato a farne un uso di carattere essenzialmente professionale.

---

principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti; Decisione di Esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy). Per quanto riguarda le due sentenze: CGUE, causa C-362/2014, *Maximillian Schrems* c. *Data Protection Commissioner*, 6 ottobre 2015 – ECLI:EU:C:2015:650 (*Schrems I*); CGUE, causa C-311/18, *Data Protection Commissioner* c. *Facebook Ireland Limited e Maximillian Schrems*, 16 luglio 2020 – ECLI:EU:C:2020:559 (*Schrems II*).

[74] CGUE, *Schrems* (2018), punto 10.

A tal riguardo, la Corte ha ricordato come la nozione di «consumatore» si contrapponga a quella di operatore economico e prescinda dalle conoscenze o dalle informazioni di cui una persona realmente dispone, né le competenze che l'interessato possa acquisire nel settore nel cui ambito rientrano tali servizi, né il suo impegno ai fini della rappresentanza dei diritti e degli interessi degli utilizzatori di tali servizi valgono a privarla della qualità di «consumatore» ai sensi dell'art. 15 del Regolamento Bruxelles I (vigente *ratione temporis*). A parere della Corte, un'interpretazione della nozione di «consumatore» che escludesse tali attività si risolverebbe, infatti, nell'impedire una tutela effettiva dei diritti di cui i consumatori dispongono nei confronti delle loro controparti professionali e sarebbe in contrasto con l'obiettivo enunciato dall'art. 169, par. 1 TFUE[75] di promuovere il loro diritto all'organizzazione per la salvaguardia dei propri interessi.

Pertanto, la Corte ha concluso affermando il principio per cui l'utente di un account Facebook aperto per scopi privati non perde la qualità di «consumatore» ai sensi del Regolamento Bruxelles I (applicabile *ratione temporis*) nel caso in cui pubblichi libri, tenga conferenze, gestisca siti Internet, raccolga donazioni e si faccia cedere i diritti da numerosi consumatori al fine di far valere in giudizio tali diritti.

---

[75] V. art 169 TFUE: «1. Al fine di promuovere gli interessi dei consumatori ed assicurare un livello elevato di protezione dei consumatori, l'Unione contribuisce a tutelare la salute, la sicurezza e gli interessi economici dei consumatori nonché a promuovere il loro diritto all'informazione, all'educazione e all'organizzazione per la salvaguardia dei propri interessi. 2. L'Unione contribuisce al conseguimento degli obiettivi di cui al paragrafo 1 mediante: a) misure adottate a norma dell'articolo 114 nel quadro della realizzazione del mercato interno; b) misure di sostegno, di integrazione e di controllo della politica svolta dagli Stati membri. 3. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale, adottano le misure di cui al paragrafo 2, lettera b). 4. Le misure adottate a norma del paragrafo 3 non impediscono ai singoli Stati membri di mantenere o di introdurre misure di protezione più rigorose. Tali misure devono essere compatibili con i trattati. Esse sono notificate alla Commissione».

La pronuncia in questione è interessante in quanto in essa si scorge l'intento di assicurare e garantire l'effettiva tutela dei diritti dei consumatori, ponendoli per certi versi al riparo dalle evoluzioni dinamiche che possono conoscere le loro relazioni con le piattaforme digitali. Ciò non significa, peraltro, una cristallizzazione della qualifica iniziale di «consumatore» ai sensi del diritto internazionale privato. Al contrario, la Corte ha infatti ribadito l'obbligo di interpretare restrittivamente la nozione ai fini internazionalprivatistici per tutta la durata del rapporto. L'insegnamento dei Giudici di Lussemburgo è piuttosto quello per cui l'evoluzione dinamica delle attività svolte dal «consumatore» nell'ambito di una piattaforma digitale possano portare alla perdita della qualifica soltanto nel caso in cui egli inizi a comportarsi come un vero e proprio operatore economico e non, invece, ad organizzarsi, promuovere azioni e diffondere contenuti a tutela dei diritti propri e della sua categoria. Di conseguenza, l'interprete che voglia qualificare, a fini internazionalprivatistici, l'utente di un *social network* è chiamato di volta in volta a verificare in questi termini l'evoluzione delle sue attività nell'ambito della piattaforma.

2.4.3 Il regime consumeristico in pratica: tra «*targeting approach*» e volontà delle parti

Venendo all'analisi delle norme di diritto internazionale privato dell'Unione dedicate ai consumatori e della loro applicazione nell'ambito delle piattaforme digitali, occorre innanzi tutto chiarire come l'obiettivo delle stesse sia quello di infondere fiducia nei consumatori in modo da incentivarne la presenza sul mercato unico[76]. A tal fine, il legislatore dell'Unione ha concepito un regime volto a garantire un accesso agevole alla giustizia da parte del consumatore e a far sì che ai contratti conclusi da quest'ultimo si applichi, tendenzialmente, un diritto a lui familiare.

[76] P. FRANZINA, *op. cit.* n. 14, p. 226; F. RAGNO, *op. cit.* n. 62.

Così, a proposito della competenza giurisdizionale, è di regola previsto il ricorso al foro del consumatore, sia nei casi in cui sia questi ad agire in giudizio sia in quelli in cui l'azione sia promossa dall'altra parte (il professionista). In particolare, il consumatore può scegliere di agire nello Stato membro in cui l'altra parte è domiciliata oppure, indipendentemente dal domicilio di quest'ultima, nel luogo in cui egli stesso è domiciliato (art. 18, par. 1). Viceversa, al professionista è consentito proporre un'azione soltanto davanti alle autorità giurisdizionali dello Stato membro in cui è domiciliato il consumatore (art 18, par. 2). A livello di legge applicabile è invece previsto che, in mancanza di scelta di legge[77], il contratto tra il consumatore e il professionista sia di regola disciplinato dalla legge del paese in cui il consumatore ha la propria residenza abituale (art. 6, par. 1 Regolamento Roma I).

A) Il «*targeting approach*» e le sue evoluzioni nel mercato digitale: il caso *Pammer*

L'applicazione dei regimi appena richiamati non è tuttavia automatica ma soggiace ad una medesima limitazione, figlia dell'utilizzo della tecnica legislativa del c.d. «*targeting approach*[78]», già usata in diverse situazioni dal legislatore dell'Unione e conosciuta anche da altri ordinamenti giuridici (v. *infra* par. 5.1). In particolare, tanto l'art. 17 del Regolamento Bruxelles I*bis*[79] quanto l'art. 6,

---

[77] Ai sensi dell'art. 6, par. 2 Regolamento Roma I, peraltro, la facoltà delle parti di scegliere la legge applicabile al contratto non è illimitata ma: «[…] tale scelta non vale a privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è premesso derogare convenzionalmente ai sensi della legge che, in mancanza di scelta, sarebbe stata applicabile a norma del paragrafo 1».

[78] Per l'espressione, utilizzata a proposito della normativa in materia di protezione dei dati personali su cui si dirà *infra*, v. D.J. SVANTESSON, *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation*, in International Data Privacy Law, Vol. 5, n. 4, pp. 226-234, 2015.

[79] L'art. 17 Regolamento Bruxelles I*bis*, nello stabilire le condizioni di applicazione delle disposizioni relative ai consumatori, esenta dal c.d. «*targeting test*» i contratti di «vendita a rate di beni mobili materiali» (art. 17, par. 1, lett. a) Regolamento Bruxelles I*bis*) e i contratti di «prestito con rimborso rateizzato o di un'altra operazione di credito, connessi con il finanziamento

par. 1 del Regolamento Roma I[80] dispongono che le norme a tutela dei consumatori previste da entrambi gli strumenti si applichino soltanto a condizione che il professionista svolga le sue attività commerciali o professionali nel paese in cui il consumatore ha la residenza abituale (o è domiciliato, secondo la dicitura del Regolamento Bruxelles I*bis*) o diriga tali attività «con qualsiasi mezzo» verso tale paese o vari paesi tra cui quest'ultimo.

Il «*targeting approach*» di cui fa uso il legislatore dell'Unione permette di conciliare l'obiettivo di tutela del consumatore con quello generale della prevedibilità delle soluzioni circa la giurisdizione e la legge applicabile, costituendo, da questo punto di vista, un beneficio anche per il professionista. Questi, infatti, sin dal momento in cui sceglie di dirigere le proprie attività verso uno Stato membro è consapevole che la legge di tale paese disciplinerà i contratti conclusi con i consumatori ivi residenti, così come della possibilità di essere convenuto di fronte alle autorità del medesimo Stato dai consumatori ivi domiciliati. Va chiarito, peraltro, come soltanto questi ultimi (o quelli abitualmente residenti, ai sensi del Regolamento Roma I) possano invocare la tutela

di una vendita di tali beni» (art. 17, par. 1, lett. b) Regolamento Bruxelles I*bis*). Il par. 3 stabilisce inoltre che il regime di favore non si applichi «ai contratti di trasporto che non prevedono prestazioni combinate di trasporto e di alloggio per un prezzo globale».

[80] L'art. 6, par. 4 Regolamento Roma I esclude inoltre dall'ambito di applicazione del regime speciale a tutela dei consumatori i seguenti tipi di contratti: «[…] a) contratti di fornitura di servizi quando i servizi dovuti al consumatore devono essere forniti esclusivamente in un paese diverso da quello in cui egli risiede abitualmente; b) […] contratti di trasporto diversi dai contratti riguardanti un viaggio «tutto compreso» ai sensi della direttiva 90/314/CEE del Consiglio, del 13 giugno 1990, concernente i viaggi, le vacanze ed i circuiti «tutto compreso»; c) […] contratti aventi per oggetto un diritto reale immobiliare o la locazione di un immobile diversi dai contratti riguardanti un diritto di godimento a tempo parziale ai sensi della direttiva 94/47/CE; d) ai diritti e obblighi che costituiscono uno strumento finanziario e ai diritti e obblighi costitutivi delle clausole e condizioni che disciplinano l'emissione o l'offerta al pubblico e le offerte pubbliche di acquisizione di valori mobiliari, e alla sottoscrizione e al riacquisto di quote di organismi di investimento collettivo, nella misura in cui tali attività non costituiscono prestazione di un servizio finanziario; e) […] contratti conclusi nell'ambito del tipo di sistema che rientra nel campo di applicazione dell'articolo 4, paragrafo 1, lettera h)».

dei regimi protettivi, essendo gli stessi di contro preclusi ai consumatori stabiliti in paesi diversi, anche se comunque entrati in contatto con il professionista.

L'applicazione del «*targeting approach*» appena delineato è stata messa a dura prova dallo sviluppo del commercio elettronico e delle piattaforme digitali. Infatti, se è agevole stabilire quando un professionista che opera sul mercato fisico sta dirigendo le proprie attività verso un determinato Stato – essendo a tal fine rilevanti attività di pubblicità «classica», specificamente rivolte agli abitanti di tale paese – non lo è nel mercato *online*, che ha per sua natura portata globale. Un sito internet è infatti accessibile, quanto meno potenzialmente, in ogni momento e da qualsiasi parte del mondo, il che rende più complicato valutare verso quali Stati stia «dirigendo» le proprie attività il professionista che offre prodotti o servizi attraverso lo stesso.

Alcuni chiarimenti sul punto sono stati forniti dalla Corte di Giustizia nella sentenza *Pammer*[81], relativa all'applicazione dell'art. 15 del Regolamento Bruxelles I (vigente *ratione temporis* e corrispondente all'attuale art. 17 Regolamento Bruxelles I*bis*).

Nell'occasione, in particolare, i Giudici di Lussemburgo hanno escluso che la semplice accessibilità del sito web del professionista dallo Stato del domicilio del consumatore valga a qualificare le attività del professionista come «dirette» verso lo stesso. Al contrario, a parere della Corte occorre verificare se effettivamente il professionista intendesse commerciare e concludere contratti con consumatori domiciliati in uno o più Stati membri, tra i quali quello di domicilio del consumatore stesso. La Corte ha quindi fornito un elenco non esaustivo di elementi utili per effettuare la verifica in questione (c.d. «*targeting*

[81] CGUE, cause riunite C-585/08 e C-144/09, *Peter Pammer* c. *Reederei Karl Schlüter GmbH & Co. KG* e *Hotel Alpenhof GesmbH* c. *Oliver Heller*, 7 dicembre 2010 – ECLI:EU:C:2010:740.

test[82]»), tra cui si annoverano la natura internazionale dell'attività, l'indicazione di itinerari a partire da altri Stati membri per recarsi presso il luogo in cui il professionista è stabilito, l'uso di una lingua o di una moneta diverse da quelle abitualmente utilizzate nello Stato membro in cui il professionista è stabilito con la possibilità di prenotare e confermare la prenotazione in tale diversa lingua, l'indicazione di recapiti telefonici unitamente ad un prefisso internazionale, il dispiego di risorse finanziarie per un servizio di posizionamento su Internet al fine di facilitare ai consumatori domiciliati in altri Stati membri l'accesso al sito del professionista ovvero a quello del suo intermediario, l'utilizzazione di un nome di dominio di primo livello diverso da quello dello Stato membro in cui il professionista è stabilito e la menzione di una clientela internazionale composta da clienti domiciliati in Stati membri differenti[83].

L'utilizzo dei criteri indicati nella sentenza *Pammer* dovrebbe facilitare l'individuazione dello Stato «*target*», tanto ai sensi dell'art. 17 del Bruxelles I*bis* quanto ai sensi dell'art. 6 Regolamento Roma I, data la necessità di interpretare in maniera coerente le medesime nozioni fornite dall'ordinamento dell'Unione.

Con lo sviluppo del Mercato Unico Digitale, tra i cui obiettivi vi è quello di ridurre sempre di più gli ostacoli al commercio elettronico all'interno dell'Unione[84], l'operazione di «*targeting test*» ha assunto e assumerà un'importanza sempre più crescente per la ricerca di soluzioni internazionalprivatisti-

---

[82] Si veda *ex multis*: F. RAGNO, *op. cit* n. 62. Per una recente proposta relativa ad un c.d. «*distargeting test*» si veda inoltre: Z. CHEN, *Internet, Consumer Contracts and Private International Law: What Constitutes Targeting Activity Test?* in Information & Communications Technology Law, pubblicato il 21 dicembre 2021. Liberamente accessibile al seguente link: https://doi.org/10.1080/13600834.2021.2018760

[83] CGUE, *Pammer e Alpenhof*, punto 93.

[84] V. Commissione Europea, COM(2015) 192 final.

che in materia di consumatori. Lo stesso legislatore dell'Unione sembra esserne consapevole nel momento in cui ha previsto, all'art. 1, par. 6 del Regolamento sul c.d. «*geoblocking*[85]», che il rispetto di quest'ultimo non implica che il professionista stia dirigendo le proprie attività verso lo Stato membro della residenza abituale o del domicilio del consumatore ai sensi dell'art. 6, par. 1, lett. b) Regolamento Roma I e dell'art. 17, par. 1, lett. c) del Regolamento Bruxelles I*bis*[86]. Si tratta di una specifica importante, visto che lo scopo del regolamento è quello di «impedire blocchi geografici ingiustificati e altre forme di discriminazione basate, direttamente o indirettamente, sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti[87]». Obiettivo che il

[85] Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE.

[86] V. art. 1, par. 6 Regolamento (UE) 2018/301: «Il presente regolamento fa salvo il diritto dell'Unione riguardante la cooperazione giudiziaria in materia civile. La conformità al presente regolamento non implica che un professionista diriga le attività verso lo Stato membro della residenza abituale o del domicilio del consumatore ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento (CE) n. 593/2008 e dell'articolo 17, paragrafo 1, lettera c), del 1regolamento (UE) n. 1215/2012. In particolare, non si considera che un professionista diriga le attività verso lo Stato membro in cui il consumatore ha la residenza abituale o il domicilio per il solo fatto che, agendo a norma degli articoli 3, 4 e 5 del presente regolamento, non blocchi né limiti l'accesso dei consumatori a un'interfaccia online, non reindirizzi i consumatori, sulla base della loro nazionalità o del loro luogo di residenza, a una versione di un'interfaccia online diversa da quella cui i consumatori desideravano accedere inizialmente, non applichi condizioni generali di accesso diverse al momento della vendita di beni o della prestazione di servizi nelle situazioni di cui al presente regolamento oppure accetti strumenti di pagamento emessi in un altro Stato membro su base non discriminatoria. Inoltre, non si considera che un professionista, per le sole ragioni sopra indicate, diriga le attività verso lo Stato membro in cui il consumatore ha la residenza abituale o il domicilio, qualora il professionista fornisca informazioni e assistenza al consumatore dopo che il contratto è stato stipulato in conformità agli obblighi che incombono sul professionista in virtù del presente regolamento». Si veda anche il considerando 13 del medesimo regolamento.

[87] Art. 1, par. 1 Regolamento (UE) 2018/301.

legislatore mira a raggiungere, tra le altre cose, limitando in maniera sostanziale la possibilità, per i professionisti, di impedire l'accesso[88] ai propri siti internet da clienti cittadini o stabiliti in alti Stati membri e di proporre condizioni generali diverse a seconda della provenienza del cliente[89]. È chiaro quindi che, in assenza di tale previsione, il regolamento sul «*geoblocking*» avrebbe notevolmente complicato, se non reso del tutto impossibile, la già non semplice operazione di «*targeting test*».

B) I limiti alla volontà delle parti come ulteriore tutela del consumatore

Come nel caso dei lavoratori, un'ulteriore tutela predisposta dal legislatore dell'Unione a vantaggio dei consumatori è costituita dalla parziale limitazione della volontà delle parti in relazione alla possibilità di derogare alle speciali norme protettive dal Regolamento Bruxelles I*bis* e di scegliere la legge applicabile ai contratti da essi conclusi.

In particolare, con riguardo alla giurisdizione la deroga è ammissibile soltanto se effettuata tramite una convenzione posteriore al sorgere della controversia, che consenta al consumatore di adire una autorità giudiziaria diversa da quelle indicata dalle norme produttive o che, stipulata tra il consumatore e la sua controparte aventi entrambi il domicilio o la residenza abituale nel medesimo Stato membro al momento della conclusione del contratto, conferisca la competenza alle autorità giurisdizionali di tale Stato membro, sempre che la legge di quest'ultimo non vieti siffatte convenzioni (art. 19 Regolamento Bruxelles I*bis*).

Con riferimento alla legge applicabile, invece, la scelta è tendenzialmente libera ma la stessa non può privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente ai

[88] Art. 3 Regolamento (UE) 2018/301.
[89] Art. 4 Regolamento (UE) 2018/301.

sensi della legge che sarebbe stata applicabile in mancanza di scelta, vale a dire la legge dello Stato in cui il consumatore è domiciliato, in cui il professionista svolge o verso cui dirige la propria attività (art. 6, par. 2 Regolamento Roma I[90]). Ciò significa che anche nel caso in cui il contratto – concretamente rappresentato dalle condizioni generali[91] di una piattaforma digitale, determinate *ex ante* dal professionista e sostanzialmente non negoziabili dalla controparte – contenga una clausola di scelta di una legge diversa, il consumatore potrà comunque beneficiare della protezione garantita delle «norme imperative» della «sua» legge.

A tal proposito, va rilevato come la Corte di Giustizia abbia avuto modo di pronunciarsi[92] in merito alla natura abusiva, ai sensi dell'art. 3, par. 1 direttiva 93/13/CEE[93], di una clausola di scelta di legge applicabile contenuta nelle condizioni generali disciplinanti il contratto stipulato mediante commercio elettronico tra un professionista (nel caso concreto la Amazon EU Sarl, società di diritto lussemburghese principale entità del colosso *e-commerce* in Europa) e un consumatore. In particolare, a tutela della parte debole, la Corte ha nell'occasione chiarito che una simile clausola è da considerarsi abusiva nel caso in cui individui soltanto la legge dello Stato in cui è stabilito il professionista come applicabile, senza informare il consumatore della protezione ad egli garantita dalle «norme imperative[94]» del paese in cui è domiciliato ai sensi dell'art. 6, par. 2 Regolamento Roma I.

Dal punto di vista internazionalprivatistico occorre aggiungere come la Corte, nella medesima sentenza, si sia incidentalmente soffermata anche su

---

[90] T. LUTZI, *op. cit.* sub Cap. 1, n. 37, p. 137.
[91] I «termini e condizioni» per riprendere la dicitura utilizzata dal Regolamento P2B.
[92] CGUE, causa C-191/15, *Verein für Konsumenteninformation* c. *Amazon EU Sàrl*, 28 luglio 2016 – ECLI:EU:C:2016:612.
[93] Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori, apparsa in *GU L 95 del 21.4.1993, pagg. 29–34*.
[94] CGUE, *VKI* c. *Amazon*, punti 59, 69-71.

un'altra questione dibattuta in dottrina[95], ossia se la scelta di legge contenuta nelle condizioni generali di un professionista possa estendersi anche alle obbligazioni non contrattuali sorte tra lo stesso e il consumatore. Tale possibilità veniva, in particolare, teorizzata a partire della clausola di salvaguardia di cui all'art. 4, par. 3 Regolamento Roma II, il quale recita:

> «*Se dal complesso delle circostanze del caso risulta chiaramente che il fatto illecito presenta collegamenti manifestamente più stretti con un paese diverso da quello di cui ai paragrafi 1 o 2*[96]*, si applica la legge di quest'altro paese. Un collegamento manifestamente più stretto con un altro paese potrebbe fondarsi segnatamente su una relazione preesistente tra le parti, quale un contratto, che presenti uno stretto collegamento con il fatto illecito in questione*».

Da questa ultima specifica si è sviluppata la teoria per cui la clausola di scelta di legge contenuta nelle condizioni generali di un professionista potesse valere come un «collegamento manifestamente più stretto» nell'ambito di tali rapporti. Simili suggestioni sono tuttavia state respinte, seppur *obiter dictum*[97], della Corte di Giustizia. A parere dei Giudici di Lussemburgo, infatti, l'accoglimento di una simile teoria consentirebbe infatti ad un professionista come Amazon EU di scegliere, di fatto, la legge cui assoggettare un'obbligazione extracontrattuale, eludendo le condizioni previste a tal riguardo dall'art. 14,

---

[95] T. LUTZI, *op. cit.* sub Cap. 1, n. 37, p. 138.

[96] I paragrafi 1 e 2 dell'art. 4 Regolamento Roma II forniscono i criteri generali per individuare la legge applicabile alle obbligazioni non contrattuali. In particolare, gli stessi prevedono: «1. Salvo se diversamente previsto nel presente regolamento, la legge applicabile alle obbligazioni extracontrattuali che derivano da un fatto illecito è quella del paese in cui il danno si verifica, indipendentemente dal paese nel quale è avvenuto il fatto che ha dato origine al danno e a prescindere dal paese o dai paesi in cui si verificano le conseguenze indirette di tale fatto. 2. Tuttavia, qualora il presunto responsabile e la parte lesa risiedano abitualmente nello stesso paese nel momento in cui il danno si verifica, si applica la legge di tale paese».

[97] CGUE, *VKI* c. *Amazon*, punti 44-47.

par. 1, primo comma, lett. a) del Regolamento Roma II[98] (sul punto v. nel dettaglio *infra* par. 3.2.1).

2.5 L'insufficienza dei regimi speciali e la necessità di proteggere gli utenti appartenenti ad altre categorie

Lo sviluppo del commercio elettronico e delle piattaforme digitali, oltre ad aver messo a dura prova l'applicazione dei regimi speciali a favore di lavoratori e consumatori nei termini appena esaminati, ha fatto sorgere da più parti[99] l'interrogativo relativo alla necessità di proteggere altri soggetti che, pur non appartenendo alle predette categorie, si trovano in una posizione di evidente squilibrio nei confronti delle piattaforme.

È il caso, in particolare, degli utenti commerciali che, analogamente a quanto accade ai consumatori e ai lavoratori, si trovano sovente in una posizione di dipendenza nei confronti dei gestori delle piattaforme e sottostanno a condizioni generali decise unilateralmente da questi ultimi, che spesso contengono al proprio interno clausole di scelta della legge applicabile e del foro competente e che sono sostanzialmente non negoziabili dalla controparte. Lo squilibrio che interessa tali rapporti ha delle importanti ricadute anche dal punto di vista della concorrenza e della tenuta del mercato, dal momento che la dipendenza di molti utenti commerciali nei confronti delle piattaforme è diventata negli anni sempre più marcata, specie in settori chiave come il turismo o i trasporti.

Il legislatore dell'Unione si è dimostrato consapevole di questi fenomeni ed infatti, come si è già avuto modo di vedere (v. *supra*: Cap. 1, par. 4; Cap. 2, par.

---

[98] «1. Le parti possono convenire di sottoporre l'obbligazione extracontrattuale ad una legge di loro scelta: a) con un accordo posteriore al verificarsi del fatto che ha determinato il danno […]» (art. 14, par. 1, primo comma, lett. a), del Regolamento Roma II).

[99] V. P. FRANZINA, *op. cit.* sub Cap. 2, n. 51, p. 160; I. PRETELLI, *op. cit*. sub Cap. 1, n. 11, p. 31; I. PRETELLI, *op. cit*. 2, p. 9.

3.1), negli ultimi anni è intervenuto in più occasioni approntando a favore degli utenti commerciali delle tutele di diritto sostanziale, ad esempio con l'approvazione del Regolamento P2B e in seguito con il Digital Markets Act. Al contrario, a livello di diritto internazionale privato manca tuttora un regime protettivo dedicato a tali soggetti, dal momento che le norme sopra illustrate si riferiscono unicamente ai rapporti di lavoro o a quelli tra professionisti e consumatori (rapporti «B2C»), ignorando invece quelli stabiliti soltanto tra professionisti (rapporti «B2B»), che restano quindi soggetti alla disciplina generale.

La tutela degli utenti commerciali economicamente dipendenti dalle piattaforme digitali è stata in parte affrontata, dal punto di vista del diritto internazionale privato, dalla Corte di Giustizia nella sentenza *Booking.com*[100], sulla quale ci soffermeremo meglio nel prosieguo quando tratteremo i regimi in materia di concorrenza (v. *infra*: par. 4.3). Tale pronuncia, pur se favorevole nell'esito alla parte debole, non ha tuttavia sancito – né per la verità trattato – la possibilità di applicare la dottrina del *favor leasi* interpretando determinate norme di diritto internazionale privato in senso favorevole agli utenti commerciali delle piattaforme digitali. La Corte ha piuttosto basato la propria decisione facendo leva sugli obiettivi di prossimità e di buona amministrazione della giustizia perseguiti dal Regolamento Bruxelles I*bis*, ritenendo il giudice del mercato interessato dal presunto comportamento anticoncorrenziale quello più idoneo a pronunciarsi circa la natura dello stesso[101]. Ad ulteriore conferma di come, ad oggi, la tutela di parti deboli diverse rispetto a quelle

[100] CGUE, causa C-59/19, *Wikingerhof GmbH & Co. KG* c. *Booking.com BV*, 24 novembre 2020 – ECLI:EU:C:2020:950. Per dei commenti vedi: I. PRETELLI, *op. cit*. 2; P. FAVROD-COUNE, *The Legal Position of the Weaker Party in B2B Relationships with Online Platforms in the European Union, an Analysis of Dispute Resolution Mechanisms in Regulation (EU) 2019/1150*, in Yearbook of Private International Law, Vol. XXI, pp. 523- 548, 2021.

[101] CGUE, *Booking.com*, punto 37.

elencate nei regolamenti presi in considerazione non rientri ancora tra gli obiettivi del diritto internazionale privato dell'Unione europea.

3 Le norme di diritto internazionale privato nei rapporti tra utenti

Analizzati i profili internazionalprivatistici attinenti ai rapporti relativi alla «dimensione verticale» delle piattaforme digitali, il focus si sposta adesso su quelli tra utenti, che animano la c.d. «dimensione orizzontale». I rapporti in questione possono essere tanto di tipo contrattuale quanto non contrattuale e con riguardo ad entrambi emergono diverse problematiche di diritto internazionale privato. Quelle relative ai rapporti contrattuali saranno affrontate nelle prossime pagine, mentre quelle afferenti ai rapporti non contrattuali saranno trattate nel successivo par. 4, nell'ambito di un ragionamento valevole anche per i rapporti di cui alla «dimensione verticale».

3.1 La disciplina dei rapporti contrattuali tra utenti

Cominciando, quindi, dai rapporti contrattuali, occorre innanzi tutto premettere che gli stessi possono stabilirsi sia tra utenti considerati di «pari» livello dal diritto internazionale privato che tra soggetti tra cui è possibile individuare la parte «forte» e quella «debole». Il primo è il caso dei rapporti B2B ma anche di quelli che legano soggetti che si scambiano beni e servizi agendo al di fuori della propria attività professionale (c.d. «rapporti C2C»), come può accadere nell'ambito di piattaforme come eBay o Viagogo (dedicata alla vendita e allo scambio di biglietti per eventi dal vivo). Il secondo è, invece, il caso classico dei rapporti tra professionisti e consumatori e dei contratti di lavoro, con annessi i problemi qualificatori già trattati a proposito della «dimensione verticale» (v. *supra* par. 2.3.1, 2.4.1).

Dal punto di vista del diritto internazionale privato, per entrambi i tipi di rapporti valgono, *mutatis mutandis*, le medesime considerazioni svolte riguardo alla «dimensione verticale» e, più in generale, a proposito dell'utilizzo

nel mondo virtuale dei criteri di collegamento previsti in materia contrattuale dal Regolamento Roma I e dal Regolamento Bruxelles I*bis* (v. *supra*, par. 1.1, 2.1 e 2.2).

Per quest'ultimo, in particolare, si riscontrano le stesse difficoltà relative all'individuazione del «luogo di esecuzione» dell'obbligazione dedotta in giudizio (art. 7, punto 1). Anche nei rapporti tra utenti, infatti, la localizzazione della fattispecie appare agevole se si discorre di contratti da eseguirsi nel mondo fisico (ad esempio una compravendita di merci da consegnare all'utente) mentre risulta più problematica a proposito dei contratti che si concludono ed eseguono integralmente nell'ambito delle piattaforme[102]. Per ragioni di prevedibilità, anche in questo caso in dottrina[103] è stato proposto di dare rilievo al foro di residenza (o di domicilio) dell'utente, con tutte le criticità già rilevate in occasione degli approfondimenti sulla «dimensione verticale» (v. *supra* par. 2.2).

…*Segue*: L'applicazione dei regimi protettivi

Analoghe sono anche le considerazioni relative all'applicazione dei regimi protettivi dedicati a consumatori e lavoratori quando si tratta di proteggere la parti deboli dei rapporti relativi alla «dimensione orizzontale». A tal riguardo, peraltro, nella sentenza *Pammer* la Corte di Giustizia ha chiarito, seppur *obiter tantum*, come i principi ivi stabiliti a proposito dell'utilizzo del «*targeting approach*» nell'ambito del commercio elettronico valgano sia nel caso in cui un commerciante promuova la propria attività attraverso il suo sito Internet – quindi con l'obiettivo di stabilire rapporti «verticali» con gli utenti – sia

[102] I. PRETELLI, *op. cit*. sub Cap. 1, n. 11 p. 27 e *op. cit.* 2, p. 3.
[103] Idem, rispettivamente a p. 30 e p. 8.

nell'ipotesi in cui lo faccia attraverso il sito di una società intermediaria[104], come accade con piattaforme come Booking, Airbnb o Amazon.

Rimanendo sui regimi protettivi, nell'ambito della «dimensione orizzontale» si pongono ovviamente anche le questioni qualificatorie sopra esaminate (v. *supra* 2.3.1, 2.4.1). Peraltro, posto che le attività degli utenti – e di conseguenza i rapporti tra essi stabiliti – sono per natura più dinamiche e soggette ad evoluzione rispetto a quelle di una piattaforma, l'operazione qualificatoria presenta, rispetto a quanto succede con la «dimensione verticale», delle difficoltà pratiche maggiori. Come si è detto, inoltre, i rapporti afferenti alla «dimensione orizzontale» possono intercorrere anche soltanto tra due o più consumatori e non coinvolgere utenti professionisti (rapporti «C2C»), il che esclude, in questi ultimi casi, l'applicazione dei regimi protettivi di cui all'art. 6 Regolamento Roma I e agli artt. 17-19 Regolamento Bruxelles I*bis*.

Da sottolineare, infine, come in dottrina[105] sia stata messa in dubbio la stessa necessità di applicare i regimi protettivi a tutela dei consumatori nei casi di rapporti «orizzontali» con professionisti che non dispongano di una forza particolarmente maggiore rispetto alle proprie controparti. È il caso, ad esempio, di piccole imprese o di altri soggetti professionali che offrono i propri beni o servizi su base occasionale attraverso piattaforme come e-Bay. Una simile differenziazione tra professionisti, pur emersa nella giurisprudenza statunitense[106], non appare tuttavia attuabile ai fini dell'applicazione dei regimi a protezione dei consumatori previsti dal diritto internazionale privato dell'Unione. Questo nonostante il legislatore dell'Unione abbia, negli ultimi anni, adottato

---

[104] CGUE, *Pammer* e *Alpenhof*, punto 89.

[105] I. PRETELLI, *op. cit.* sub Cap. 1, n. 11, p. 38 e *op. cit.* n. 2, p. 11.

[106] Vedi in particolare la sentenza della Corte d'Appello del nono circuito statunitense: *Boschetto* v. *Hansing*, 539 F.3d 1011 (9th Cir. 2008). In tale pronuncia, in particolare, la Corte ha considerato la differenza tra soggetti che fanno un uso «*regular and systemic*» della piattaforma e-Bay per finalità commerciali e soggetti che ne fanno invece un utilizzo occasionale.

diversi strumenti a tutela anche dei professionisti utenti commerciali nei rapporti con le piattaforme (v. *supra*: Cap. 2, par. 3.1; Cap. 3, par. 2.5).

3.2 La rilevanza delle regole delle piattaforme nei rapporti tra utenti

Una questione discussa in dottrina è quella della rilevanza delle regole che disciplinano i rapporti contrattuali tra utenti e gestori delle piattaforme (i «termini e condizioni» secondo il linguaggio del Regolamento P2B) ai fini della risoluzione delle questioni internazionalprivatiste relative alla «dimensione orizzontale».

Si è già visto, in particolare, come i gestori delle piattaforme siano in grado di plasmare il contenuto materiale dei rapporti tra i propri utenti (v. *supra*: Cap. 1, par. 2.2). Nella prospettiva internazionalprivatista, si è avuto invece modo di constatare come i regolamenti dell'Unione siano tuttora ancorati ad una concezione fortemente «stato-centrica», in cui vi è uno spazio limitato per i diritti non statali (v. *supra*: par. 1.2). Escluso, quindi, che le regole di una piattaforma possano essere individuate come «legge applicabile» ai rapporti tra utenti, è stato sostenuto in dottrina[107] come esse possano comunque influenzare il giurista nell'applicazione delle norme di conflitto per quanto riguarda i suddetti rapporti. Questa possibilità è stata promossa, in particolare, in quanto favorirebbe la prevedibilità circa la legge applicabile e rispetterebbe una presunta aspettativa degli utenti per cui i comportamenti sulla piattaforma sarebbero, in primo luogo, disciplinati dalle regole della stessa.

3.2.1 L'estensione della scelta di legge contenuta nelle condizioni della piattaforma

La prima forma di influenza teorizzata dalla dottrina[108] riguarda la possibilità di estendere l'efficacia delle clausole di scelta di legge sovente incluse nelle

[107] T. LUTZI, *op. cit.* sub Cap. 1, n. 37, pp. 139ss.
[108] Idem, p. 139.

condizioni generali delle piattaforme – e quindi oggetto di accordo tra i gestori e gli utenti – anche ai rapporti afferenti alla «dimensione orizzontale».

A tal fine, viene innanzi tutto considerata la tesi per cui la scelta in questione riguarderebbe, implicitamente, anche i rapporti tra utenti. Ai sensi del diritto dell'Unione, sia l'art. 3, par. 1 Regolamento Roma I che l'art. 14, par. 1 Regolamento Roma II ammettono la possibilità di una scelta di legge implicita ma entrambi richiedono che questa risulti «chiaramente» (Roma I) o «in modo non equivoco» (Roma II) dal contratto o dalle circostanze del caso. L'art. 14 Regolamento Roma II contiene, peraltro, ulteriori limitazioni, *in primis* quella per cui, ad eccezione dei rapporti B2B, l'accordo debba essere posteriore al fatto che ha causato il danno. Pertanto, al di là delle supposte aspettative degli utenti, nessuna delle due norme appare realmente utile per lo scopo richiamato.

Un'altra via per giungere alla predetta estensione, considerata più efficace dalla dottrina[109] in commento, è rappresentata dalle clausole di salvaguardia contenute, rispettivamente, nell'art. 4, par. 3 Regolamento Roma I e nell'art. 4, par. 3 Regolamento Roma II.

Cominciando dai rapporti contrattuali, l'art. 4, par. 3 Regolamento Roma I dispone che nell'ipotesi in cui dal «complesso delle circostanze del caso» risulti chiaramente che il contratto presenta «collegamenti manifestamente più stretti» con un paese diverso da quello individuato attraverso l'applicazione dei criteri generali previsti dai paragrafi 1 o 2, si applichi la legge di tale diverso paese. La tesi sostenuta in dottrina è quella, già accennata (v. *supra* par. 2.4.3, sez. B)), per cui la clausola di scelta di legge contenuta nei «termini e condizioni» di una piattaforma, precedentemente accettati da entrambi gli

[109] Idem, p. 139ss.

utenti, valga a creare un tale collegamento tra la legge oggetto della stessa ed il contratto tra gli utenti.

Tale affermazione si basa, innanzi tutto, su quanto previsto dal considerando 20 Regolamento Roma I[110], ai sensi del quale per determinare il paese con il collegamento più stretto si dovrebbe considerare, tra l'altro, se il contratto di cui si discorre – in questo caso quello tra due o più utenti – sia strettamente collegato a un altro contratto o ad altri contratti, rappresentati nel caso in esame da quelli conclusi tra gli utenti e la piattaforma e le relative clausole di scelta di legge. La tesi fa inoltre leva sul principio di prossimità[111], che è poi alla base dello stesso art. 4, par. 3 Regolamento Roma I. In particolare, argomenta la dottrina, dato che nel mondo virtuale un utente raramente ha un'idea precisa su dove si trovi la «residenza abituale» della controparte tenuta alla «prestazione caratteristica[112]» del contratto, l'applicazione degli artt. 4, par. 1 e 2 si fonderebbe su un collegamento nei fatti molto più debole rispetto a quello con il paese la cui legge è oggetto della scelta contenuta nei «termini e condizioni» della piattaforma.

La tesi appena richiamata appare in parte condivisibile, soprattutto per quanto riguarda i riferimenti alla prossimità ma, dal momento che coinvolge una clausola di salvaguardia, è soggetta alla volubilità delle valutazioni caso per caso e non permette di individuare dei paradigmi generali. Peraltro, l'applicazione della stessa è in ogni caso limitata dai regimi speciali a protezione di «lavoratori» e «consumatori», che prevalgono sulle disposizioni di cui

---

110 «Qualora il contratto presenti manifestamente un collegamento più stretto con un paese diverso da quello indicato all'articolo 4, paragrafi 1 o 2, una clausola di salvaguardia dovrebbe prevedere che si debba applicare la legge di tale diverso paese. Per determinare tale paese si dovrebbe considerare, tra l'altro, se il contratto in questione sia strettamente collegato a un altro contratto o ad altri contratti» (considerando 20 Regolamento Roma I).

111 V. *ex multis*: U. MAGNUS, *Article 4*, in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome I Regulation: Commentary*, Verlag Dr. Otto Schmidt, 2016.

112 V. Artt. 4 par. 1 e par. 2 Regolamento Roma I.

all'art. 4, riducendo di molto il potenziale effetto espansivo della scelta di legge contenuta nei «termini e condizioni».

Simili considerazioni valgono per i rapporti non contrattuali. A tal proposito, si è peraltro già visto come la Corte di Giustizia abbia escluso la rilevanza dell'art. 4, par. 3 Regolamento Roma II per quanto riguarda gli illeciti commessi da un utente nei confronti del gestore di una piattaforma le cui condizioni generali contengono un accordo di scelta di legge, essendo quest'ultimo rilevante soltanto per il contratto (v. *supra* par. 2.4.3, B)). Per quanto riguarda i rapporti tra utenti, invece, la stessa configurazione della clausola di salvaguardia, che fa riferimento a «relazion[i] preesistent[i] tra le parti[113]», ne complica l'applicazione, dal momento che il rapporto preesistente non intercorre tra di essi ma tra ciascun utente e il gestore della piattaforma. La stessa dottrina[114] ne deduce quindi una rilevanza, all'atto pratico, assai ridotta.

3.2.2 Le regole delle piattaforme come «dato di fatto» nei rapporti tra utenti

Un'altra strada tentata in dottrina[115] è quella di considerare le regole della piattaforma come «dato di fatto» nei rapporti tra utenti. Ciò vale, in particolare, per le obbligazioni non contrattuali e discende dall'art. 17 Regolamento Roma II. Tale disposizione prevede infatti che, nel valutare il comportamento del presunto responsabile del danno, si tenga conto: «Quale dato di fatto e ove opportuno, delle norme di sicurezza e di condotta in vigore nel luogo e nel momento in cui si verifica il fatto che determina la responsabilità».

---

[113] V. art. 4, par. 3 Regolamento Roma II, il quale fa riferimento ad una «relazione preesistente» (usando quindi il singolare) tra le parti.
[114] T. LUTZI, *op. cit.* sub Cap. 1, n. 37, p. 141.
[115] Idem, pp. 141ss.

L'art. 17 agisce a prescindere dalla legge applicabile individuata attraverso le norme di conflitto contenute nello stesso regolamento e ammette che l'interprete possa non applicare una legge diversa ma prendere in considerazione, come mero dato di fatto[116], parametri valutativi pertinenti alla situazione in ragione della sua localizzazione obiettiva. La presa in considerazione delle norme del luogo della condotta permette di bilanciare la regola generale di cui all'art. 4, par. 1 Roma II, che dà invece esclusiva rilevanza al luogo dell'evento dannoso e presenta, secondo la menzionata dottrina[117], uno squilibrio a favore dell'attore parte lesa. Essa consentirebbe, infatti, di tutelare l'aspettativa del convenuto per cui gli illeciti da egli commessi in un determinato luogo dovrebbero essere valutati secondo gli *standard* ivi in vigore.

Per i fini che qui interessano, occorre chiedersi se le regole di una piattaforma possano essere considerate come «norma di sicurezza e di condotta» in vigore nel luogo (virtuale) del danno. A questo proposito, come sottolineato in dottrina[118], l'art. 17 non sembra riferirsi soltanto a norme statali o comunque di regolatori pubblici ma pare al contrario lasciare aperta la strada anche a regole di matrice diversa. Ciò anche alla luce di quanto previsto dal considerando 34, che parla genericamente di «tutte le disposizioni che presentano un collegamento con la sicurezza e la condotta», indicando solo esemplificativamente le norme relative alla sicurezza stradale in caso di incidente.

---

[116] Sul significato della disposizione si veda *ex multis*: F. MARONGIU BONAIUTI, *Le obbligazioni non contrattuali nel diritto internazionale privato,* Giuffré, 2013 (in particolare pp. 166ss).

[117] T. LUTZI, *op. cit.* sub Cap. 1, n. 37, p. 141. L'autore fa in particolare leva sul considerando 34 Regolamento Roma II, il quale recita: «Al fine di raggiungere un equilibrio ragionevole fra le parti, occorre tener conto, ove appropriato, delle norme di sicurezza e di condotta in vigore nel paese in cui il fatto dannoso è stato commesso, anche ove l'obbligazione extracontrattuale sia disciplinata dalla legge di un altro paese. Il concetto di «norme di sicurezza e di condotta» dovrebbe essere interpretato come riferito a tutte le disposizioni che presentano un collegamento con la sicurezza e la condotta, comprese per esempio le norme relative alla sicurezza stradale in caso di incidente».

[118] Idem, p. 142.

Da quanto sopra si ricava, pertanto, come nulla sembri ostare a che l'interprete prenda in considerazione, per valutare le responsabilità di un utente ai sensi dell'art. 17 Regolamento Roma II, le regole della piattaforma che governano le interazioni e i comportamenti degli utenti nello spazio virtuale. Si tratta, assieme al già citato considerando 13 del Regolamento Roma I (v. *infra* par. 1.2), dell'unico addentellato normativo nel sistema di diritto internazionale privato dell'Unione che sembra riconoscere una forma di rilevanza, peraltro limitata alla presa in considerazione come mero dato di fatto, alle norme di fonte statale, ed in particolare, per i fini che qui interessano, a quelle di matrice privata. Per il resto, non si rivengono in tale sistema altre disposizioni che permettano di valorizzare – o anche solo considerare allo scopo di limitarlo – il potere regolatorio dei gestori delle piattaforme.

4 Gli illeciti civili: tra ubiquità, *favor laesi* e tutela del mercato

Le interazioni degli utenti, sia tra di loro che con i gestori delle piattaforme, possono dare vita, oltre che a contratti, anche a rapporti giuridici di tipo extracontrattuale, derivanti da illeciti civili commessi nel mondo virtuale. È il caso, molto comune, della violazione dei diritti della personalità o di proprietà intellettuale, materie che hanno trovato terreno fertile nella rete e nel flusso di informazioni costante, e spesso incontrollabile se non *ex post*, che la caratterizza. Ancora, è il caso degli illeciti derivanti da violazione di norme in materia di concorrenza. Si tratta di rapporti che, come detto, possono afferire sia alla dimensione verticale che a quella orizzontale delle piattaforme, con la conseguenza che i ragionamenti che ci apprestiamo a svolgere nelle prossime pagine risulteranno validi – pur se con i dovuti distinguo – per entrambe.

Non interessa in questa sede approfondire da un punto di vista del diritto materiale tutta la galassia normativa, dottrinale e giurisprudenziale relativa a

tali materie. Compito per il cui assolvimento, peraltro, non si potrebbe prescindere dall'analisi dettagliata di strumenti complessi come il GDPR (per quanto riguarda i diritti della personalità) o lo stesso Digital Markets Act (a proposito della concorrenza). Rimandando quindi a sedi[119] più opportune per le doverose considerazioni sul punto, ci si soffermerà nelle prossime pagine soltanto sulle questioni attinenti al diritto internazionale privato dell'Unione.

4.1 La lesione dei diritti della personalità e la «teoria del mosaico»

Da un punto di vista internazionalprivatista, si è già avuto modo di anticipare (v. *supra* par. 1.1) come l'applicazione delle norme e dei criteri di collegamento in materia di illeciti civili nel mondo virtuale abbia dato vita ad un sempre maggiore utilizzo della teoria dell'ubiquità, cristallizzata oggi, per quanto riguarda la competenza giurisdizionale, nell'art. 7, punto 2 Regolamento Bruxelles I*bis*. In particolare, l'applicazione della stessa si è tradotta, in materia di diritti della personalità, nella formulazione della c.d. «teoria del mosaico» («*mosaic theory*» in inglese), inaugurata con la sentenza *Shevill*[120] per quanto riguarda il mondo analogico (diffamazione a mezzo di carta stampata) e trasposta in quello virtuale dalla successiva *e-Date*[121].

In questo filone giurisprudenziale, la Corte di Giustizia ha sancito il principio per cui una potenziale vittima possa agire, per la totalità del danno subito, o

---

[119] Per approfondire i profili di diritto sostanziale si vedano, *ex multis*: J. CARRASCOSA GONZALEZ, *The Internet – Privacy and Rights Relating to Personality*, in Collected Courses of The Hague Academy of International Law – Recueil des cours de l'Academie de droit international, Vol. 378, pp. 261-486, Brill Nijhoff, 2016; G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina Editore, 2016; O. POLLICINO, R. FRANZOSI, G. CAMPUS (a cura di), *Internet and Copyright protection in the European perspective, The Digital Single Market Copyrig*ht, Aracne, 2016; G. DELLA MORTE, *op. cit.* sub Cap. 1, n. 47; O. POLLICINO, M. BASSINI, G.M. RICCIO (a cura di), *Copyright versus (other) Fundamental Rights in the Digital Age. A Comparative Analysis in Search of a Common Constitutional Ground*, Edward Elgar, 2020; G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Collana di studi sull'integrazione europea, Cacucci, 2021. Per quanto riguarda la concorrenza si vedano le opere citate alla nota n. 57 di cui al Cap. 1.

[120] CGUE, *Shevill*, punto 33.

[121] CGUE, *e-Date*, punto 52.

dinanzi ai giudici dello Stato membro del luogo di stabilimento del soggetto che ha condiviso i contenuti da cui sono scaturiti i danni – considerato come il luogo della condotta – o a quelli dello Stato membro in cui si trova il proprio «centro d'interessi[122]». Quest'ultimo, in particolare, costituisce un criterio di collegamento creato appositamente[123] dalla Corte allo scopo di individuare il luogo dell'evento dannoso rilevante ai sensi dell'art. 7, punto 2 Regolamento Bruxelles I*bis* (corrispondente, all'epoca di *e-Date*, all'art. 5, punto 3 del Regolamento Bruxelles I). Per illustrarlo, i Giudici di Lussemburgo hanno chiarito come il luogo in cui una persona ha il proprio centro di interessi corrisponda, in via generale, alla sua residenza abituale, aggiungendo come, tuttavia, una persona possa avere il proprio centro di interessi anche in uno Stato membro diverso, ove altri indizi, quali l'esercizio di un'attività professionale, possano dimostrare l'esistenza di un collegamento particolarmente stretto con tale Stato[124]. In alternativa, la parte lesa può agire davanti ai giudici di ciascuno Stato membro sul cui territorio un'informazione messa in rete sia accessibile oppure lo sia stata: questi ultimi sono tuttavia competenti a conoscere del solo danno cagionato sul territorio del loro Stato.

La «teoria del mosaico» così delineata è, nelle intenzioni della Corte, conforme agli obiettivi di prevedibilità e di buona amministrazione della giustizia. Infatti, a parere dei Giudici di Lussemburgo: «L'impatto, sui diritti della personalità di un soggetto, di un'informazione messa in rete può essere valutata meglio dal giudice del luogo in cui la presunta vittima possiede il proprio centro di interessi[125]». Inoltre, come affermato nella sentenza *Shevill*: «Il giudice

---

[122] Idem, punto 48.

[123] T. LUTZI, *op. cit.* Cap. 1, n. 37, p. 132. Si veda anche: P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market*, pp. 81-108, Intersentia, 2016.

[124] CGUE, *e-Date*, punto 49.

[125] CGUE, *e-Date*, punto 48.

di ciascuno Stato contraente in cui la pubblicazione diffamatoria è stata diffusa e in cui la vittima asserisce aver subito una lesione della propria reputazione è, dal punto di vista territoriale, il più qualificato per valutare la diffamazione commessa in questo Stato e determinare la portata del danno che ne deriva[126]». Insegnamento che, come detto, è stato mutuato in *e-Date* per giustificare l'attribuzione della competenza giurisdizionale ai giudici di ciascuno Stato membro attraverso cui si possa o si sia potuto accedere ai contenuti diffamatori attraverso internet.

La soluzione in questione non è, peraltro, andata esente da critiche in dottrina[127], in particolare da chi ha sottolineato i rischi in termini di prevedibilità[128] della giurisdizione e di «*forum shopping*», correlati soprattutto all'effetto «mosaico» dato dalla possibilità di agire in ciascuno Stato membro in cui il contenuto è stato reso accessibile. Simili rischi sono stati sottolineati[129] anche con riferimento all'art. 79 GDPR, nelle cui previsioni speciali sulla giurisdizione in

---

[126] CGUE, *Shevill*, punto 31.

[127] V. *ex multis*: I. PRETELLI, *op. cit.* sub Cap. 1, n. 11, p. 27; O. FERACI, *Digital Rights and Jurisdiction: The European Approach to Online Defamation and IPRs Infringements*, in E. CARPANELLI, N. LAZZERINI (a cura di), *Use and Misuse of New Technologies*, pp. 277-304, Springer, 2019.

[128] V. a questo proposito il considerando 16 Regolamento Bruxelles I*bis*, a mente del quale «Il criterio del foro del domicilio del convenuto dovrebbe essere completato attraverso la previsione di fori alternativi, basati sul collegamento stretto tra l'autorità giurisdizionale e la controversia, ovvero al fine di agevolare la buona amministrazione della giustizia. L'esistenza di un collegamento stretto dovrebbe garantire la certezza del diritto ed evitare la possibilità che il convenuto sia citato davanti a un'autorità giurisdizionale di uno Stato membro che non sia per questi ragionevolmente prevedibile. Tale aspetto è importante soprattutto nelle controversie in materia di obbligazioni extracontrattuali derivanti da violazioni della privacy e dei diritti della personalità, compresa la diffamazione».

[129] V. *ex multis*: P. FRANZINA, *op. cit.* n. 123; M. BRKAN, *Data Protection and European Private International Law*, Robert Schuman Centre for Advanced Studies Research Paper n. RSCAS 2015/40, 2015. Disponibile su SSRN: https://ssrn.com/abstract=2631116; F. MARONGIU BONAIUTI, *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 Ibis"*, in Cuadernos de Derecho Transnacional, Vol. 9, n. 2, pp. 448-464, 2017; L. LUNDSTEDT, *International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR*, Faculty of Law, Stockholm University Research Paper, n. 57, link SSRN: https://ssrn.com/abstract=3159854.

materia di protezione dei dati personali riecheggiano in parte gli insegnamenti della giurisprudenza *Shevill* e *e-Date*.

Vi è inoltre in dottrina[130] chi scorge nella «teoria del mosaico» il tentativo di massimizzare le possibilità di tutela una vittima di lesioni della personalità attraverso le molteplici facoltà di scelta in merito ai giudici dinnanzi a cui agire in giudizio. Questo obiettivo, espressione di quello è stato definito[131] come «*favor leasi*», sembra in particolare emergere da un passaggio della sentenza *e-Date* in cui la Corte menziona esplicitamente la «gravità della lesione che può subire il titolare del diritto della personalità, il quale constata che un'informazione lesiva di suddetto diritto è disponibile in qualunque parte del mondo[132]».

In assenza di previsioni generali, la rilevanza del *favor leasi* appare, tuttavia, circoscritta ai diritti della personalità – peraltro nella misura in cui è ammessa dalla Corte in *e-Date* – e non adattabile anche agli altri illeciti civili che possono rientrare nell'ambito di applicazione dell'art. 7, punto 2 del Regolamento Bruxelles I*bis*. Quest'ultima norma persegue, infatti, obiettivi di prevedibilità del foro e di certezza del diritto che, come chiarito dagli stessi Giudici di Lussemburgo nella sentenza *Folien Fischer*[133], «non attengono né all'attribuzione dei rispettivi ruoli di attore e convenuto né alla tutela dell'uno o dell'altro[134]».

---

[130] V. *ex multis*: P. FRANZINA, *op. cit.* n. 123, p. 90; I. PRETELLI, *op. cit.* sub Cap. 1, n. 11, p. 27; I. PRETELLI, *op. cit.* n. 2, p. 7.

[131] Espressione che si ritrova in entrambi gli scritti di Ilaria Pretelli menzionati alla nota precedente per quanto riguarda lo specifico ambito delle piattaforme digitali. In generale si vedano anche: C. HONORATI, *Regolamento n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali*, in F. PREITE (a cura di), *Atti notarili - Diritto dell'Unione e internazionale,* Vol. IV, t. 1, pp. 483-558, Utet Giuridica, 2011; F. MARONGIU BONAIUTI, *op. cit.* n. 116 (in particolare p. 133 e 221).

[132] CGUE, *e-Date*, punto 47.

[133] CGUE, causa C-133/11, *Folien Fischer AG e Fofitec AG* c. *Ritrama SpA*, 25 ottobre 2012 – ECLI:EU:C:2012:664.

[134] CGUE, *Folien Fischer*, punti 45-47. V. su questo aspetto in particolare P. FRANZINA, *op. cit.* n. n. 123, p. 102.

Per concludere, occorre fare soltanto qualche breve considerazione sulla legge applicabile. In particolare, è il caso di sottolineare come in relazione alla stessa le incertezze siano tuttora maggiori rispetto a quanto accade con la competenza giurisdizionale. Questo dipende principalmente dal fatto che l'art. 1, par. 2, lett. g) del Regolamento Roma II esclude esplicitamente dal campo di applicazione dello stesso «le obbligazioni extracontrattuali che derivano da violazioni della vita privata e dei diritti della personalità, compresa la diffamazione». Si tratta di una scelta del legislatore dell'Unione allora motivata da ragioni di tipo politico, rappresentate delle diverse sensibilità presenti nei vari Stati membri circa il bilanciamento tra tutela dei diritti della personalità e libertà di stampa[135]. Una scelta che, nonostante la realizzazione di un apposito studio[136] da parte della Commissione europea ai sensi dell'art. 30, par. 3 del Regolamento e la presentazione di una risoluzione[137] *ad hoc* del Parlamento europeo, non è stata rivista dal legislatore.

Conseguenza della predetta impostazione è quella per cui le soluzioni in materia di legge applicabile vadano ricercate nelle norme di conflitto nazionali, con l'impossibilità di stabilire dei paradigmi unici a livello di Unione europea[138]. La questione si intreccia, ancora una volta, con quanto previsto dalla

---

[135] V. a questo proposito: K. SIEHR, *Violation of Privacy and Rights Relating to Personality*, in A. MALATESTA (a cura di), *The Unification of Choice of Law Rules on Torts and Other Non-Contractual Obligations in Europe*, pp. 159-172, Cedam, 2006; O. FERACI, *La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria*, in Rivista di diritto internazionale, Vol. 92, n. 4, pp. 1020-1085, 2009; C. HONORATI, *op. cit.* n. 131, p. 492; F. MARONGIU BONAIUTI, *op. cit.* n. 116, pp. 206ss; C. CAMPIGLIO, *La legge applicabile alle obbligazioni extracontrattuali (con particolare riguardo alla violazione della privacy)* in Rivista di diritto internazionale privato e processuale, Vol. 51, fasc. 4, pp. 857-866, 2015.

[136] Commissione europea, *Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality*, JLS/2007/C4/028, Final Report, 1 febbraio 2009.

[137] Risoluzione del Parlamento europeo del 10 maggio 2012 recante raccomandazioni alla Commissione concernenti la modifica del regolamento (CE) n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali (Roma II) (2009/2170(INI)).

[138] V. *ex multis* C. HONORATI, *op. cit.* n. 131, p. 492; F. MARONGIU BONAIUTI, *op. cit.* n. 116, pp. 206ss.

normativa speciale in materia di protezione dei dati personali. A questo proposito, in particolare, mentre la vecchia Direttiva 95/46/CE[139] conteneva una norma (l'art. 4)[140] col tempo assimilata alle tradizionali norme di diritto internazionale privato[141], il GDPR costituisce un esempio del nuovo approccio unilateralista intrapreso negli ultimi anni dal legislatore dell'Unione, sul quale ci si soffermerà a breve (v. *infra*: par. 5.1).

4.2 La violazione dei diritti di proprietà intellettuale in rete e il caso *Wintersteiger*

La tutela dei diritti di proprietà intellettuale in rete è un tema al centro del dibattito giuridico sin dalla diffusione di internet, posto che la facilità con cui il *web* permette la condivisione di contenuti favorisce indirettamente anche la commissione di attività illegali in violazione delle norme sul diritto d'autore, così come di quelle sulla tutela di marchi, brevetti e di altre creazioni protette.

---

[139] 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.

[140] Art. 4 - Diritto nazionale applicabile «1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:
a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile; b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico; c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea. 2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento».

[141] V. a questo proposito: L. A BYGRAVE, *Determining Applicable Law pursuant to European Data Protection Legislation*, in Computer Law and Security Report, Vol. 16, n. 4 pp. 252-257, 2000; P. PIRODDI, *Profili internazionalprivatistici della responsabilità del gestore di un motore di ricerca per il trattamento dei dati personali*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, pp. 63-98, Roma TrE-Press, 2015.

L'argomento, come si è avuto modo di vedere, si lega a doppio filo con il tema della responsabilità degli *internet service provider*, sui quali la nuova Direttiva Copyright ed il Digital Services Act pongono diversi e penetranti doveri di controllo. Molteplici sono anche le questioni internazionalprivatistiche sottese alla tematica, sulle quali non è peraltro possibile soffermarsi nel dettaglio in questa sede[142], concentrandosi piuttosto su un'analisi settoriale.

Per i fini che qui interessano, occorre innanzi tutto sottolineare come, con riguardo alla proprietà intellettuale, gli strumenti dell'Unione europea valorizzino in primo luogo il criterio di collegamento del «*locus protectionis*[143]». Nello specifico, l'art. 8 del Regolamento Roma II dispone che la legge applicabile ad un'obbligazione extracontrattuale derivante da una violazione di un diritto di proprietà intellettuale è quella del paese per il quale la protezione è chiesta. Per quanto riguarda i diritti di proprietà intellettuale dell'Unione europea a carattere unitario, il criterio in questione è bilanciato da quello del

---

[142] Per approfondire vedi, *ex multis*: F. MARONGIU BONAIUTI, *op. cit.* n. 116, pp. 133ss; M. PERTEGAS SENDER, *Cross-Border Enforcemenr of Patent Rights – An Analysis of the Interface Between Intellectual Property and Private International Law*, Oxford University Press, 2002; T. KONO, *Intellectual Property Rights, Conflict of Laws and International Jurisdiction: Applicability of the ALI Principles in Japan?*, in Brooklyn Journal of International Law, Vol. 30, n. 3, pp. 865-883, 2005; J. BASEDOW, *Foundations of Private International Law in Intellectual Property*, in J. BASEDOW, T. KONO, A. METZGER (a cura di), *Intellectual Property in the Global Arena*, pp. 3-29. Mohr Siebeck, 2010; P. A. DE MIGUEL ASENSIO, *Recognition and Enforcement of Judgments in Intellectual Property Litigation: The CLIP Principles*, in J. BASEDOW, T. KONO, A. METZGER (a cura di), *Intellectual Property in the Global Arena*, Mohr Siebeck, pp. 239-292, 2010;P.A. DE MIGUEL ASENSIO, *Intellectual Property in European Private Law*, in E. PILLOT (a cura di), *Les frontiers du droit privé européen / The Boundaries of European Private Law*, Larcier, pp. 189-213, 2012; B. UBERTAZZI, *Recognition and Enforcement of Foreign Judgments in Intellectual Property: a Comparison for the Intellectual Property Association*, in Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 3, n. 3, pp. 306-349, 2012; F. HEINDLER, *Streaming Platforms and Copyright in Conflict of Laws*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 193-202, Schulthess, 2018.

[143] Si veda il considerando 26 del Regolamento Roma II: «Quanto alle violazioni dei diritti di proprietà intellettuale, sarebbe opportuno mantenere il principio della *lex loci protectionis*, universalmente riconosciuto. Ai fini del presente regolamento, per «diritti di proprietà intellettuale» si dovrebbero intendere, per esempio, il diritto d'autore, i diritti connessi, il diritto sui generis alla protezione delle banche dati, nonché i diritti di proprietà industriale»

luogo della condotta, posto che, per le questioni non disciplinate dal relativo strumento dell'Unione, si applica la legge del paese in cui è stata commessa la violazione. Si tratta, in entrambi i casi, di previsioni inderogabili, che contribuiscono a garantire la prevedibilità delle soluzioni anche nel mondo virtuale.

La questione è diversa per quanto riguarda la competenza giurisdizionale, posto che né il Regolamento Bruxelles I*bis* né altri strumenti dell'Unione contengono norme specifiche di diritto internazionale privato sulla proprietà intellettuale. Di conseguenza, occorre nuovamente far riferimento all'art. 7, punto 2 Regolamento Bruxelles I*bis* ed alla teoria dell'ubiquità.

Dei chiarimenti sull'applicazione di tale norma alle violazioni commesse su internet sono stati forniti dalla Corte di Giustizia nella sentenza *Wintersteiger*[144]. Il caso in questione riguardava una controversia tra la società austriaca Wintersteiger AG («Wintersteiger»), produttore e commerciante di macchinari per la messa a punto di sci e *snowboard* nonché titolare dell'omonimo marchio registrato in Austria, e la società tedesca Products 4U Sondermaschinenbau GmbH («Products 4U»), distributore e rivenditrice della prima. Quest'ultima, in particolare, aveva riservato la parola chiave («AdWord») «Wintersteiger» nell'ambito del sistema pubblicitario sviluppato da Google per il dominio nazionale di primo livello «google.de». Di conseguenza, l'utente che, accedendo da tale dominio, inseriva la parola chiave «Wintersteiger» nel popolare motore di ricerca vedeva apparire come primo risultato il sito della Products 4U ed era pertanto indirizzato verso lo stesso invece che verso quello della titolare del marchio. La Winstersteiger riteneva tale condotta come lesiva del proprio marchio austriaco e aveva pertanto intentato un'azione giudiziaria in Austria

[144] CGUE, causa C-523/10, *Wintersteiger AG* c. *Products 4U Sondermaschinenbau GmbH*, 19 aprile 2012 – ECLI:EU:C:2012:220.

per far cessare la condotta della Products 4U. Giova aggiungere per completezza come la Products 4U non avesse riservato alcuno spazio per quanto riguarda il dominio austriaco «google.at».

Nell'occasione, come detto, la Corte ha avuto modo di pronunciarsi sulla competenza giurisdizionale, allora disciplinata dall'art. 5, punto 3 del Regolamento Bruxelles I. A tal proposito, i Giudici di Lussemburgo, discostandosi rispetto a quanto affermato nella sentenza *e-Date*[145] in materia di diritti della personalità, hanno riconosciuto la giurisdizione austriaca, individuando lo Stato membro in cui è stato registrato il marchio oggetto dell'asserita violazione come quello della concretizzazione del danno ai fini della norma in commento[146]. A parere della Corte, tale conclusione è funzionale sia all'obiettivo della prevedibilità sia a quello della buona amministrazione della giustizia[147], considerando anche che, ai sensi delle norme del Regolamento Roma II poc'anzi richiamate, la legge applicabile alla violazione è proprio quella del medesimo «*locus protectionis*».

In applicazione della teoria dell'ubiquità i Giudici di Lussemburgo hanno, inoltre, riconosciuto come l'azione potesse anche essere promossa in Germania, quale Stato del «fatto generatore del danno». In particolare, la Corte è giunta a tale conclusione a seguito di un ragionamento che si è in primo luogo basato sulla constatazione per cui la limitazione territoriale della tutela di un marchio nazionale non è idonea ad escludere la competenza giurisdizionale di giudici diversi da quelli dello Stato membro in cui il marchio è registrato[148]. La Corte ha quindi considerato come, in caso di comparsa di pubblicità su un motore di ricerca tramite parola chiave, il «fatto generatore del danno» sia non

[145] CGUE, *Wintersteiger*, punti 22-24.
[146] Idem, punto 25.
[147] Idem, punti 26-28.
[148] Idem, punto 30.

la suddetta comparsa ma l'avviamento, da parte dell'inserzionista, del processo tecnico finalizzato alla stessa[149]. Posto ciò, i Giudici di Lussemburgo hanno escluso la rilevanza del luogo del server utilizzato per tale operazione, dato che l'incerta localizzazione dello stesso mette in pericolo l'obiettivo della prevedibilità della giurisdizione[150]. Di contro, proprio perché si tratta di un luogo certo e identificabile, la Corte ha concluso affermando che il luogo da cui è deciso l'avvio del processo finalizzato alla visualizzazione degli annunci, rilevante per l'operazione di cui all'art. 7, punto 2 del Regolamento Bruxelles I*bis*, debba essere individuato in quello dello stabilimento dell'inserzionista (nel caso di specie la Products 4U)[151].

Nella sentenza *Wintersteiger* si scorgono alcune delle riflessioni già svolte in merito ai rischi in termini di prevedibilità derivanti dall'applicazione dei criteri di collegamento di diritto internazionale privato in rete. Ciò vale, in particolare, per l'esclusione della rilevanza del luogo del server (v. *supra* par. 2.2). Più in generale, il tentativo della Corte appare quello, già sperimentato in *e-Date*, di adattare le tradizionali norme di diritto internazionale privato al mondo virtuale, individuando *ex novo* – come nel caso del «centro di interessi[152]» – o mutuando criteri di collegamento utilizzati per altre situazioni, come è nel caso dello «stabilimento[153]». Scopo ultimo della Corte appare quello

---

[149] Idem, punto 34.

[150] Idem, punto 36.

[151] Idem, punti 37-38.

[152] V. T. LUTZI, *op. cit.* sub Cap. 1, n. 37, p. 132.

[153] La nozione di «stabilimento» (con la dicitura inglese «*establishment*») compare più volte all'interno del Regolamento Bruxelles I*bis*: art. 7, punto 5; art. 11, par. 2, art. 17, par. 2; art. 20, par. 2. Importante è il riferimento agli artt. 49-55 TFUE, che stabiliscono il diritto di stabilimento sancito dal diritto dell'Unione. Per una interpretazione estensiva della nozione ai fini dell'esercizio di tale diritto si veda: CGUE, causa C-106/16, *Polbud* c. *Wykonawstwo*, 25 ottobre 2017 – ECLI:EU:C: 2017:804 (punto 38). La nozione viene utilizzata, ai fini della competenza giurisdizionale, dall'art. 79 GDPR. Il considerando 22 di tale strumento fornisce una nozione assai ampia del concetto di stabilimento, in linea con l'evoluzione della giurisprudenza dell'Unione europea: «[…] Lo stabilimento implica l'effettivo e reale svolgimento di attività

di garantire la salvaguardia degli obiettivi generali di prevedibilità e buona amministrazione della giustizia. Sembra esserci invece poco spazio, in questo caso, per la dottrina del *favor laesi*, posto che in un passaggio della sentenza si legge chiaramente come il luogo di stabilimento dell'inserzionista costituisca un criterio di collegamento idoneo in quanto luogo certo e identificabile, «sia per il ricorrente che per il convenuto[154]». Non è quindi dato ravvisare, a differenza che in *e-Date*, l'intento di massimizzare o comunque garantire le possibilità di tutela per la parte lesa.

4.3 Piattaforme e norme di diritto internazionale privato in materia di concorrenza

Altri illeciti civili che possono sorgere nell'ambito delle piattaforme digitali sono quelli derivanti dalla violazione delle norme in materia di concorrenza. Si tratta di una tematica complessa, disciplinata da un gran numero di strumenti di diritto materiale dell'Unione su cui non è qui possibile soffermarsi[155].

Con specifico riguardo alle piattaforme, abbiamo visto come la tutela della concorrenza nei mercati digitali sia considerata dal Regolamento P2B (v. *supra*: Cap. 2, par. 3.1). Essa, inoltre, si colloca al centro del nuovo Digital Markets Act (v. *supra*: Cap. 1, par. 5) e permea, in generale, tutto il progetto della Commissione relativo alla creazione di un Mercato Unico Digitale. Filo comune che unisce il Regolamento P2B e il Digital Markets Act è la tutela degli utenti delle piattaforme digitali nei confronti dei comportamenti dei gestori di queste – ed

---

nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica». Per una interpretazione giurisprudenziale della nozione in materia di protezione dei dati personali si veda: CGUE, causa C-230/14, *Weltimmo s.r.o.* c. *Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 ottobre 2015 – ECLI:EU:C:2015:639.

[154] CGUE, *Wintersteiger*, punto 37.

[155] Basti pensare che la «definizione delle regole di concorrenza necessarie al funzionamento del mercato interno» rientra tra le materie su cui l'Unione europea ha competenza esclusiva ai sensi dell'art. 3, par. 1, lett. b) TFUE.

in particolare dei c.d. *gatekeeper* nel caso del Digital Markets Act – suscettibili di pregiudicare la concorrenza all'interno del Mercato Unico.

Dal punto di vista del diritto internazionale privato, le violazioni in materia di concorrenza – siano esse perpetrate dagli utenti o dai gestori delle piattaforme – assumono rilevanza sia ai sensi del Regolamento Bruxelles I*bis* per quanto riguarda la disciplina sulla giurisdizione che ai sensi del Regolamento Roma II a proposito della legge applicabile. Su entrambi gli aspetti ci soffermeremo nelle pagine seguenti.

4.3.1 Le questioni relative alla legge applicabile: tra «teoria del mosaico» e rapporti con la Direttiva e-Commerce

Punto di partenza della nostra analisi è proprio quello relativo alla legge applicabile, in quanto il Regolamento Roma II contiene una norma specifica, ossia l'art. 6, relativa alle obbligazioni extracontrattuali derivanti da atti di concorrenza sleale e da atti limitativi della libera concorrenza[156].

In particolare, l'art. 6, par. 1 riguarda la «concorrenza sleale», una categoria che, nonostante i ripetuti tentativi dottrinali e gli addentellati presenti nella normativa di settore[157], non conosce una vera e propria definizione omnicomprensiva[158] all'interno dell'Unione europea. Tuttavia, ai fini della disposizione in commento, appare possibile affermare[159] come essa si ponga, in generale, a

---

[156] Per approfondire: M. ILLMER, Article 6 – *Unfair Competition and Acts Restricting Free Competition*, in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome II Regulation: Commentary*, pp. 230-286, Verlag Dr. Otto Schmidt, 2019.

[157] Si vedano ad esempio le nozioni di «pratiche commerciali sleali» e «pratiche commerciali ingannevoli» descritte, rispettivamente, dagli artt. 5 e 6 della Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (direttiva sulle pratiche commerciali sleali) (Testo rilevante ai fini del SEE) – apparsa in *GU L 149 dell'11.6.2005, pagg. 22–39*.

[158] M. ILLMER, *op. cit.* n. 156 p. 237.

[159] Idem, p. 237.

tutela dei concorrenti, dei consumatori e del pubblico in senso lato, nonché del corretto funzionamento dell'economia di mercato, come affermato dal considerando 21 Regolamento Roma II. In questo senso, tra gli atti di concorrenza sleale possono annoverarsi diverse condotte tipicamente attuate attraverso internet e le piattaforme digitali, quali la pubblicità ingannevole[160], la pubblicità comparativa[161] o l'utilizzo di parole chiave ingannevoli nell'ambito dei motori di ricerca[162]. Tra le condotte in questione, secondo parte della dottrina[163] sarebbe possibile includere anche la diffamazione perpetrata ai danni di concorrenti (si pensi, ad esempio, al caso delle recensioni false). A parere della richiamata dottrina, infatti, non si tratterebbe di atti lesivi dei diritti della personalità – e quindi, come tali, esclusi dall'ambito di applicazione del Regolamento Roma II – ma della possibilità dei soggetti colpiti dalle condotte diffamatorie di agire correttamente sul mercato.

Venendo all'analisi dalla norma, essa individua come criterio di collegamento il paese sul cui territorio sono pregiudicati, o rischiano di esserlo, i rapporti di concorrenza o gli interessi collettivi dei consumatori. Il criterio in questione si fonda, pertanto, sul mercato pregiudicato dagli atti di concorrenza sleale piuttosto che sui soggetti direttamente colpiti da questi. Significativo, a questo proposito, il successivo art. 6, par. 2, ai sensi del quale nel caso in cui un atto di concorrenza sleale leda esclusivamente gli interessi uno specifico concorrente, si applicano le regole generali di cui all'art. 4. Eccezione che, peraltro, necessita di essere interpretata in maniera restrittiva[164].

---

[160] Idem, p. 238. Per la relativa definizione v. art. 2, lett. b) Direttiva 2006/114/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, concernente la pubblicità ingannevole e comparativa (versione codificata) (Testo rilevante ai fini del SEE) – apparso su *GU L 376 del 27.12.2006, pagg. 21–27*.

[161] Per la relativa definizione v. art. 2, lett. c) Direttiva 2006/114/CE.

[162] M. ILLMER, *op. cit.* n. 156 p. 238, 285.

[163] Idem, p. 242.

[164] Idem, p. 235.

Nell'ambito delle piattaforme, è invero piuttosto comune che una singola condotta – ad esempio una recensione falsa o una pubblicità ingannevole diffusa indiscriminatamente in rete – possa costituire un atto di concorrenza sleale che coinvolga i mercati di più paesi. In questi casi, pertanto, l'operare in concreto dell'art. 6, par. 1 Regolamento Roma II è suscettibile di portare all'individuazione delle leggi di più di un paese, ciascuna delle quali sarà applicabile soltanto ai danni prodottisi all'interno del mercato del proprio Stato, in una maniera non dissimile a quanto previsto dalla «teoria del mosaico» richiamata a proposito della competenza giurisdizionale in materia di lesione dei diritti della personalità (v. *supra*: par. 4.1). Di conseguenza, in applicazione della medesima teoria, ciascun interessato potrebbe agire di fronte alle autorità del paese della condotta o del proprio «centro di interessi» per la totalità dei danni, che dovrà essere calcolata applicando, in maniera proporzionale, tutte le leggi individuate ai sensi dell'art. 6, par. 1 Regolamento Roma II. Allo stesso modo, egli potrebbe agire in ciascuno degli Stati membri colpiti dalle condotte al solo scopo di richiedere i danni ivi prodottisi, ai quali si dovrebbe applicare la medesima legge del foro, individuata in applicazione dell'art. 6, par. 1 Regolamento Roma II[165].

Un'altra questione rilevante per le piattaforme digitali è quella relativa al rapporto tra lo stesso art. 6, par. 1 Regolamento Roma II e l'art. 3, par. 1-2 della Direttiva e-Commerce. Quest'ultimo, in particolare, afferma il c.d. «principio del paese d'origine», in base al quale un *internet service provider* stabilito in uno Stato membro che fornisca i propri servizi anche in altri Stati membri sia comunque sottoposto alle disposizioni nazionali vigenti nel paese di stabilimento, con il conseguente divieto per gli Stati membri di limitare la libera circolazione dei servizi società dell'informazione provenienti da un altro Stato

[165] Idem, p. 266.

membro per motivi che rientrano nell'ambito regolamentato dalla Direttiva. Il cuore della questione discussa in dottrina[166] attiene alla natura del richiamato art. 3 della Direttiva e-Commerce, a proposito del quale ci si domandava se costituisse o meno una norma di conflitto. La questione non è meramente teorica in quanto tale qualificazione avrebbe comportato la prevalenza[167] di tale norma su quelle del Regolamento Roma II, con la conseguenza che alle condotte anticoncorrenziali poste in essere da un *provider* di cui alla Direttiva e-Commerce avrebbe trovato esclusiva applicazione il diritto del relativo paese d'origine.

La risposta a questo interrogativo è stata fornita dalla Corte di Giustizia nella sentenza *e-Date*, che abbiamo avuto modo di richiamare a proposito della teoria del mosaico[168]. In essa, in particolare, i Giudici di Lussemburgo – in conformità con quanto affermato dal considerando 23 e dall'art. 1, par. 4 della direttiva – hanno confermato che l'art. 3, par. 1 della Direttiva e-Commerce non costituisce una norma di diritto internazionale privato e non imponga un recepimento in forma di norma specifica di conflitto[169]. Da questa lettura la dottrina[170] ha ricavato che, in materia di concorrenza, resta salva la rilevanza dell'art. 6, par. 1 Regolamento Roma II. Quest'ultima opera, infatti, su un livello differente rispetto all'art. 3 della Direttiva e-Commerce e determina in

---

[166] Idem, p. 249ss. Lo stesso autore discute, in termini simili, dei rapporti tra art. 6, par. 1 Regolamento Roma II e 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) (versione codificata) (Testo rilevante ai fini del SEE) – apparsa su *GU L 95 del 15.4.2010, pagg. 1–24*.

[167] La prevalenza in questione discenderebbe dall'art. 27 Regolamento Roma II, in base al quale «Il presente regolamento non pregiudica l'applicazione delle disposizioni dell'ordinamento dell'Unione che, con riferimento a settori specifici, disciplinino i conflitti di leggi in materia di obbligazioni extracontrattuali».

[168] CGUE, *e-Date*, punti 53-68.

[169] CGUE, *e-Date*, punto 61.

[170] M. ILLMER, *op. cit.* n. 156 p. 238, 285.

ogni caso la legge applicabile agli atti di concorrenza sleale posti in essere da un *internet service provider*. L'art. 3, par. 1 della Direttiva e-Commerce interverrebbe, quindi, soltanto in un momento successivo, nel caso in cui il diritto individuato ai sensi dell'art. 6, par. 1 Regolamento Roma II ponga al *provider* delle restrizioni all'accesso al mercato dei servizi più restrittive rispetto a quelli del suo paese d'origine.

Per concludere l'*excursus* relativo alla legge applicabile, facciamo soltanto un accenno al successivo art. 6, par. 3 Regolamento Roma II, il quale contiene la disciplina relativa alle obbligazioni extracontrattuali derivanti da «restrizioni della concorrenza[171]» ed è quindi meno rilevante ai fini del nostro ragionamento. Analogamente all'art. 6, par. 1, lo stesso utilizza come criterio di collegamento il mercato su cui ha effetto, o potrebbe averlo, una determinata restrizione, individuando come applicabile la legge dello Stato di tale mercato[172]. La norma specifica, inoltre[173], che, nel caso di restrizioni che abbiano, o possano avere, effetto sui mercati di più di un paese, chi promuove un'azione di risarcimento dei danni dinanzi al giudice del domicilio del convenuto può scegliere di fondare le sue pretese sulla legge del giudice adito, purché il mercato di tale Stato membro sia tra quelli «direttamente e sostanzialmente» interessati dalla restrizione contestata. Per l'attore è possibile fondare le proprie pretese sulla legge del foro anche nel caso in cui agisca nei confronti di più convenuti

[171] V. al riguardo il considerando 23 Regolamento Roma II, secondo cui: «Ai fini del presente regolamento, la nozione di restrizione della concorrenza dovrebbe comprendere divieti di accordi tra imprese, decisioni di associazioni di imprese e le pratiche concordate che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza in uno Stato membro o nel mercato interno, nonché il divieto di abusare di una posizione dominante nell'ambito di uno Stato membro o del mercato interno, quando tali accordi, decisioni, pratiche concordate e abusi di posizione dominante siano vietati dagli articoli 81 e 82 del trattato o dalla legge di uno Stato membro».

[172] Art. 6, par. 3, lett. a) Regolamento Roma II.

[173] Art. 6, par. 3, lett. b) Regolamento Roma II.

conformemente alle regole in materia di competenza giurisdizionale, a condizione che la restrizione della concorrenza su cui si basano le sue pretese contro ciascun convenuto interessi direttamente e sostanzialmente anche il mercato dello Stato membro del giudice adito.

4.3.2 La competenza giurisdizionale: assenza di regimi specifici e problemi qualificatori

Venendo adesso all'analisi delle questioni relative alla competenza giurisdizionale, occorre evidenziare come il Regolamento Bruxelles I*bis*, così come accade con la proprietà intellettuale, non preveda un regime dedicato alla concorrenza. Di conseguenza, anche agli illeciti derivanti dalla violazione delle norme in materia sono disciplinati dall'art. 7, punto 2 Bruxelles I*bis*.

La Corte di Giustizia ha avuto modo di interpretare tale norma in più occasioni[174] proprio per chiarirne la portata applicativa in materia di concorrenza. Aspetto centrale di questa giurisprudenza attiene all'individuazione del luogo – o meglio, del relativo mercato – in cui avviene la condotta o si concretano i danni conseguenza della violazione. A tal fine, i Giudici di Lussemburgo hanno, di volta in volta, considerato vari ancoraggi con il territorio, facendo uso di interpretazioni sistematiche che tenessero conto di quanto previsto dall'art. 6 Regolamento Roma II a proposito della legge applicabile. Tra i criteri considerati dalla Corte si possono menzionare, ad esempio, il luogo in cui è stato raggiunto l'accordo[175] sull'intesa restrittiva della concorrenza, quello

[174] V. ad esempio: CGUE, causa C-352/13, *Cartel Damage Claims (CDC) Hydrogen Peroxide SA* c. *Akzo Nobel NV e a.*, 21 maggio 2015 – ECLI:EU:C:2015:335; CGUE, causa C-451/18, *Tibor-Trans Fuvarozó és Kereskedelmi Kft*. c. *DAF Trucks NV*, 29 luglio 2019 – ECLI:EU:C:2019:635; CGUE, causa C-343/19, *Verein für Konsumenteninformation* c. *Volkswagen AG*, 9 luglio 2020 – ECLI:EU:C:2020:534; CGUE, causa C-30/20, *RH* c. *AB Volvo, Volvo Group Trucks Central Europe GmbH, Volvo Lastvagnar AB, Volvo Group España SA*, 15 luglio 2021 – ECLI:EU:C:2021:604.
[175] CGUE, *Tibor-Trans*.

della sede legale dei soggetti colpiti dalla violazione[176], o quello in cui un'impresa ha acquistato dei beni oggetto di accordi collusivi sulla fissazione e sull'aumento dei prezzi[177]. Viene inoltre in rilievo, come anticipato al paragrafo precedente, la teoria del mosaico, che consente di incardinare la giurisdizione in tutti i paesi i cui mercati sono colpiti dalle violazioni, per poter domandare il risarcimento dei danni ivi prodottisi.

Una questione ai nostri fini importante, su cui si sono pronunciati i Giudici di Lussemburgo, attiene alla qualificazione da assegnare, ai fini della competenza giurisdizionale, alle condotte dei gestori delle piattaforme consistenti nel modificare continuamente le proprie condizioni generali sottoponendole unilateralmente agli utenti commerciali delle proprie piattaforme. L'occasione in cui la Corte ha fornito dei chiarimenti sul punto è la già menzionata sentenza *Booking.com*[178] (v. *supra*: par. 2.5), relativa ad una controversia tra la società di diritto olandese Booking.com BV ("Booking"), gestore della nota piattaforma per prenotazioni di strutture alberghiere, e la società di diritto tedesco Wikingerhof GmbH & Co. KG ("Wikingerhof"), gestore di un albergo in Germania e utente commerciale della medesima piattaforma. In particolare, quest'ultima aveva presentato un'azione inibitoria contro le pratiche della Booking di modificare continuamente le condizioni generali della propria piattaforma, denunciandone la natura di abuso di posizione dominante in violazione delle norme tedesche sulla concorrenza.

La questione internazionalprivatistica sottoposta all'attenzione dei Giudici di Lussemburgo atteneva alla necessità di qualificare tale azione come rientrante nella materia «contrattuale» o in quella di «illeciti civili dolosi o colposi»

[176] CGUE, *Cartel Damage Claims (CDC)*.
[177] CGUE, *RH* c. *AB Volvo*.
[178] Per i riferimenti della sentenza e alcuni commenti dottrinali v. nota 100.

ai sensi dell'art. 7 del Regolamento Bruxelles I*bis*, in quanto esperita nei confronti di condotte lesive della concorrenza. Nel rispondere, la Corte ha innanzi tutto ribadito il principio, già affermato nella sentenza *Brogsitter*[179], per cui un un'azione rientra nella materia contrattuale (art. 7, punto 1 Regolamento Bruxelles I*bis*) se l'interpretazione del contratto che vincola le parti appare indispensabile per stabilire la liceità o l'illiceità del comportamento oggetto di contestazione. Al contrario, nel caso di specie i Giudici di Lussemburgo hanno evidenziato come per valutare la natura abusiva della condotta della Booking non fosse necessario esaminare ed interpretare il contratto in essere tra le parti, dal momento che l'albergo rimproverava alla piattaforma la violazione di un obbligo di legge, vale a dire il diritto tedesco sulla concorrenza[180]. Di conseguenza, la Corte ha concluso per l'applicabilità dell'art. 7, punto 2 del Regolamento Bruxelles I*bis*, riconoscendo la natura di illecito civile alle pratiche di abuso di posizione dominante contestate dalla Wikingerhof, anche se messe in atto nell'ambito del rapporto contrattuale[181]. Nel giungere a questa conclusione, i Giudici di Lussemburgo hanno fatto riferimento agli obiettivi di prossimità e di buona amministrazione della giustizia menzionati al considerando 16 del Regolamento Bruxelles I*bis*, indicando il giudice del mercato interessato dal presunto comportamento anticoncorrenziale come quello più idoneo a pronunciarsi sull'effettiva illiceità di tale comportamento[182].

Ulteriore conseguenza dell'assegnazione della qualifica di illecito civile alle condotte in questione è quella per cui ad esse si applica, ai fini dell'individuazione della legge applicabile, l'art. 6 Regolamento Roma II. Circostanza che,

---

[179] CGUE, causa C-548/12, *Marc Brogsitter* c. *Fabrication de Montres Normandes EURL e Karsten Fräßdorf*, 13 marzo 2014 - ECLI:EU:C:2014:148 (v. in particolare punti 25-27).
[180] CGUE, *Booking.com*, punto 37.
[181] Fermo restando che la valutazione di merito sulla liceità o meno delle condotte della Booking spetta al giudice di rinvio. V. in particolare punto 36 della sentenza.
[182] Idem, punto 38.

come abbiamo avuto modo di vedere, è in grado di portare alla corrispondenza tra foro e diritto applicabile (v. *supra*: par. 4.3.1).

5 I «nuovi» paradigmi del diritto internazionale privato *online*: dal ritorno dell'unilateralismo al «*regulatory overreaching*»

Dalle analisi svolte nelle pagine precedenti emerge come le norme di diritto internazionale privato dell'Unione siano soltanto parzialmente in grado di rispondere agli interrogativi sorti a seguito dello sviluppo di internet e della sempre maggior diffusione delle piattaforme digitali. L'evoluzione tecnologica e, soprattutto, quella dei rapporti sociali e giuridici che essa porta con sé richiede infatti al giurista un'attività interpretativa di volta in volta sempre più creativa che, se fondata unicamente sulle attuali norme di diritto internazionale privato, non sempre consente di stabilire dei teoremi di validità generale.

Ciò porta ad interrogarsi sulla necessità di nuovi paradigmi, ovvero di riscoprire e adattare alle piattaforme alcuni tradizionali insegnamenti internazionalprivatistici, sulla base innanzi tutto delle tendenze legislative più recenti, tanto del legislatore dell'Unione quanto di altri nel mondo, che saranno analizzate nelle prossime pagine.

5.1 Il metodo unilateralista come tentativo di estendere la sovranità degli ordinamenti giuridici in rete

Una delle più comuni tendenze legislative degli ultimi anni è, per quanto riguarda internet e le piattaforme digitali, quella di produrre strumenti normativi che determinano unilateralmente il proprio ambito di applicazione territoriale prescindendo dalle norme di conflitto. Si tratta di una tecnica non nuova, che richiama anzi gli insegnamenti di Bartolo da Sassoferrato relativi

al metodo unilateralista[183], contrapposto, nella dottrina internazionalprivatista, a quello multilateralista di Savigny[184], che è invece alla base dei regolamenti esaminati nei paragrafi precedenti.

Il sempre maggior ricorso alla suddetta tecnica risponde al tentativo dei vari ordinamenti giuridici di estendere la propria sovranità[185] sulla rete, dettando unilateralmente le condizioni, territoriali oltre che materiali, al ricorrere delle quali un soggetto è tenuto a conformarsi ad una determinata prescrizione normativa a prescindere dalle norme di conflitto. È la legge (o il regolamento, nel caso dell'Unione) che determina unilateralmente il proprio ambito di applicazione (la propria «gittata[186]»), senza bisogno di norme di diritto internazionale privato bilaterali che localizzino a tale scopo la fattispecie in un determinato Stato.

Esempi di tale approccio si ritrovano, come detto, tanto nell'Unione europea quanto in altri ordinamenti giuridici.

Casi frequenti riguardano le legislazioni in materia di protezione dei dati personali. A livello di Unione europea, rileva in particolare l'art. 3 GDPR, il

---

[183] V. ex *multis*: G. ROMANO, *L'unilateralismo nel diritto internazionale privato moderno*, Schulthess, 2014; S. FRANCQ, *Chapter U.4: Unilateralism*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (a cura di), *Encyclopedia of Private International Law*, pp. 1780–179, Edward Elgar, 2017.

[184] V. *ex multis*: J. BOMHOFF, A. MEUWESE, p. 149; O. KAHN-FREUND., entrambi *op. cit.* sub Cap. 1, n. 44; M. SONNENTAG, *Chapter S.4: Savigny, Friedrich Carl von*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (a cura di), *Encyclopedia of Private International Law*, pp. 1610–1615, Edward Elgar, 2017.

[185] Sul tema della sovranità degli Stati in rete si vedano *ex multis*: G. DELLA MORTE, *op. cit.* sub Cap. 1, n. 47; G. DELLA MORTE, *Limiti e prospettive del diritto internazionale del cyberspazio*, in Rivista di diritto internazionale, fasc. 1, pp. 5-42, 2022; V. ZENO-ZENCOVICH, *op. cit.* sub Cap. 1, n. 47; D.J. SVANTESSON, *Sovereignity in International Law – How the Internet Changed Everything, but not for Long*, in Masaryk University Journal of Law and Technology, Vol 8, n. 1, pp. 137-155, 2014; T. CHRISTAKIS, *"European Digital Sovereignty" Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, 2020, disponibile su SSRN: https://ssrn.com/abstract=3748098; T. MADIEGA, *op. cit.* Cap. 1, n. 19.

[186] P. FRANZINA, *op. cit.* sub. Cap 2, n. 51, p. 151.

quale stabilisce unilateralmente l'ambito di applicazione territoriale del regolamento facendo uso di diversi criteri[187]. Innanzi tutto, ai sensi del predetto articolo il GDPR si applica in caso di un trattamento svolto «nell'ambito delle attività di uno stabilimento[188]» di un titolare o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento in questione sia effettuato o meno nell'Unione. Altro criterio è quello per cui il GDPR si applica ai trattamenti di dati di interessati «che si trovano nell'Unione», effettuati da titolari o responsabili stabiliti al di fuori dell'Unione, al sussistere di una delle seguenti condizioni: il trattamento riguarda l'offerta di beni o la prestazione di servizi ai suddetti interessati, indipendentemente dall'obbligatorietà di un pagamento, oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento abbia luogo all'interno dell'Unione. Condizioni da cui si scorge il ricorso alla tecnica del «*targeting approach*[189]».

---

[187] Art. 3 GDPR «1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. 2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico».

[188] Sull'interpretazione del criterio, presente anche nell'abrogato art. 4, par. 1, lett. a) Direttiva 95/46/CE, v. CGUE, causa C-131/2012, *Google Spain SL e Google Inc*. c. *Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, 13 maggio 2014 – ECLI:EU:C:2014:317. Per dei commenti sulla pronuncia si vedano: B. VAN ALSENOY, M. KOEKKOEK, *Internet and Jurisdiction after Google Spain: the Extra-Territorial Reach of the EU's "Right to be Forgotten"*, KU Leuven, Working Paper n. 153, 2015; C. KUNER, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, in B. HESS, C.M. MARIOTTINI (a cura di), *Protecting Privacy in Private International and Procedural Law and by Data Protection*, pp. 19-55, Nomos Verlagsgesllschaft, 2015.

[189] D.J. SVANTESSON, *op. cit.* n. 78, p. 232.

I criteri dell'art. 3 hanno sollevato numerose discussioni in dottrina[190] in merito alla presunta applicazione extraterritoriale del GDPR. Tramite gli stessi, infatti, il regolamento appare suscettibile di applicarsi alla pressocché totalità delle imprese o organizzazioni di Stati terzi che vogliano operare nel Mercato Unico, la cui grandezza ed importanza strategica porta a configurare, almeno in astratto, un'estensione potenzialmente universale[191] del GDPR.

Pur non essendo questa la sede per addentrarsi in analisi approfondite sul punto, va ai nostri fini sottolineato come l'esteso ambito di applicazione del GDPR sembri rispondere ad una precisa scelta politica del legislatore dell'Unione di fare del regime dell'Unione in materia di protezione dati personali uno standard globale[192] che, oltre ad imporre l'adeguamento ad esso alla

---

[190] Copiosi sono i contributi sulla questione dell'applicazione extraterritoriale della normativa comunitaria in materia di protezione dei dati personali, sia precedenti che successivi all'entrata in vigore (aprile 2016) e alla piena applicabilità (maggio 2018) del GDPR. *Ex multis* si citano: D.J. SVANTESSON, *A "Layered Approach" to Extraterritoriality of Data Privacy Laws*, in *International Data Privacy Law*, Vol. 3, n. 4, pp. 278-286, 2013; D.J. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and its Practical Effect on U.S. Businesses*, in Stanford Journal of International Law, Vol. 50, n. 1, pp. 53-117, 2014; D.J. SVANTESSON, *op. cit.* n. 78; B. VAN ALSENOY, M. KOEKKOEK, *op. cit.* n. 188; C. KUNER, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, in International Data Privacy Law, Vol. 5, n. 4, pp. 235-245, 2015; C. KOHLER, *Conflict of Law Issues in the Data Protection Regulation of the European Union*, in Rivista di Diritto Internazionale Privato e Processuale, Vol. 52, n. 3, pp. 653-675, 2016; C. KUNER, *The Internet and the Global Reach of EU Law*, in M. CREMONA, J. SCOTT (a cura di), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, pp. 112-145, Oxford University Press, 2019, disponibile su SSRN: https://ssrn.com/abstract=2890930; T. CHRISTAKIS, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)* in AA.VV, *The White Book: Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection,* pp. 16-44, *CEIS & The Chertoff Group White Paper*, 2017, disponibile su SSRN: https://ssrn.com/abstract=3086820; C.G. GRANMAR, *Global Applicability of the GDPR in Context*, in International Data Privacy Law, Vol. 11, n. 3, pp. 225-244, 2021. A livello istituzionale si veda: EDPB, *Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3) – versione 2.0 adottata dopo la pubblica consultazione*, 12 novembre 2019.

[191] V. dottrina citata alla nota precedente.

[192] Si veda a questo proposito il discorso del 28 gennaio 2014 della allora vicepresidente della Commissione europea e commissaria europea per la giustizia, i diritti fondamentali e la cittadinanza, Viviane Reding, *A data protection compact for Europe*. Nello stesso, in particolare, la commissaria, a proposito degli sviluppi dell'epoca in materia di protezione dei dati personali ha dichiarato: La stessa commissaria Reding, nel commentare la Proposta originaria, aveva

maggior parte degli attori presenti sulla rete, serva come modello per altri ordinamenti giuridici. Una chiave di lettura, quest'ultima, che appare corroborata da significative pronunce della Corte di Giustizia dell'Unione europea[193] e che colloca la protezione dei dati personali tra le materie principali in cui si concretizzerebbe il fenomeno, originariamente teorizzato dalla dottrina statunitense, del c.d. «*Brussels Effect*[194]». Un fenomeno che è costituito proprio dalla capacità dell'Unione europea di influenzare in maniera decisiva, grazie alle proprie regole ed all'importanza del suo mercato, gli standard e le legislazioni di altri ordinamenti giuridici, oltre che le *policy* dei grandi gruppi multinazionali che si trovano ad operare sul Mercato Unico, innescando un fenomeno di «*race to the top*».

L'esempio del GDPR è tra i più significativi, considerata l'importanza della materia e le differenti sensibilità che essa suscita nei diversi ordinamenti giuridici, in particolare quando si tratta di bilanciare la protezione dei dati personali con altri diritti, libertà o valori tutelati a livello di costituzioni o di diritto internazionale, come la libertà di espressione, la ricerca scientifica o la sicurezza nazionale[195]. Non si tratta, peraltro, di un caso isolato. Al contrario, la tecnica unilateralista viene utilizzata da diverse legislazioni in materia di protezione dei dati personali adottate, soprattutto di recente, nel mondo. È il caso,

---

avuto modo di dichiarare: «*Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world*». Il discorso è disponibile online al seguente indirizzo: http://europa.eu/rapid/press-release_IP-14-62_en.htm.

[193] CGUE, *Google Spain*; CGUE, *Schrems I*, CGUE, *Schrems II*.

[194] Sul fenomeno si vedano *ex multis*: A. BRADFORD, *The Brussels Effect,* in Northwestern University Law Review, Vol. 107, n. 1, pp. 1-68, 2012, Columbia Law and Economics Working Paper N. 533, 2012. Disponibile su SSRN: https://ssrn.com/abstract=2770634; A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020 (v. in particolare cap. 5, *Digital Economy*, pp. 131-169); T. CHRISTAKIS, *op. cit.* n. 185.

[195] Per un'esaustiva trattazione sul punto si veda G. DELLA MORTE, *op. cit.* sub Cap. 1, n. 47.

solo per citarne alcune, di leggi come quella del Sudafrica[196] o della Malesia[197]. Sulla scia del GDPR, peraltro, altre grandi potenze globali si sono dotate di legislazioni in materia di protezione dei dati personali che determinano unilateralmente il proprio ambito di applicazione, facendo ricorso a criteri e tecniche e criteri non dissimili da quelli utilizzati dal Regolamento dell'Unione. È

[196] Protection of Personal Information Act (POPIA), n. 4/2013, apparso sulla *Government Gazette* Vol. 581, n. 37067, 26 novembre 2013. In particolare, la Sec. 3 del POPIA, con una formulazione analoga all'art. 4, par. 1, lett. c) dell'abrogata Direttiva 95/46/CE prevede: «This Act applies to the processing of personal information—entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and where the responsible party is— domiciled in the Republic; or not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic […]».

[197] Personal Data Protection Act 2010 (PDPA), Act n. 709, 10 giugno 2010. La norma che determina unilateralmente la «gittata» dello strumento è la Sec. 2 che, similmente al caso sudafricano, presenta una formulazione analoga all'art. 4 dell'abrogata Direttiva 95/46/CE: «(1) This Act applies to— (a) any person who processes; and (b) any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions. (2) Subject to subsection (1), this Act applies to a person in respect of personal data if— (a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b) the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia […]».

il caso del Brasile[198], della California[199] (con il c.d. «CCPA») e, più di recente, della Cina[200] (con il c.d. «PIPL»).

---

[198] Lei Geral de Proteção de Dados Pessoais (LGPD o LGPDP), Lei n° 13.709/2018. Si veda in particolare l'art. 3: «Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou […] III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional […]». Traduzione non ufficiale: «La presente legge si applica a qualsiasi trattamento effettuato da persone fisiche o giuridiche di diritto pubblico o privato, indipendentemente dal mezzo utilizzato, dal paese della sede o dal paese in cui si trovano i dati, a condizione che: I - il trattamento viene effettuato sul territorio nazionale; II - la finalità dell'attività di trattamento è l'offerta o la fornitura di beni o servizi o il trattamento di dati di persone fisiche situate nel territorio nazionale; o […] III - i dati personali oggetto del trattamento sono stati raccolti nel territorio nazionale».

[199] California Consumer Privacy Act (CCPA) – CA Civ Code § 1798.100 (2018), Title 1.81.5 (inizio Section 1798.100) aggiunto alla Part 4 della Division 3 del Civil Code californiano da *Stats. 2018, Ch. 55, Sec. 3*, approvato il 28 giugno 2018. In particolare, Sec. 1798.145 (Exemptions) determina, per differenza, l'ambito di applicazione territoriale del CCPA stabilendo: «(a) The obligations imposed on businesses by this title shall not restrict a business' ability to: […] (6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California».

[200] Personal Information Protection Law of the People's Republic of China (in cinese: 中华人民共和国个人信息保护法; traslitterato: *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*), adottata il 20 agosto 2021 e applicabile dall'1 novembre 2021. In particolare, l'art. 3 recita: «This Law applies to the activities of handling the personal information of natural persons within the borders of the People's Republic of China. Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well: 1) Where the purpose is to provide products or services to natural persons inside the borders; 2) Where analyzing or assessing activities of natural persons inside the borders; 3) Other circumstances provided in laws or administrative regulations» (traduzione non ufficiale a cura di Rogier Creemers e Graham Webster della Stanfor University, reperibile online: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/).

Rimanendo nell'ambito dell'Unione, è possibile scorgere altri esempi di norme unilateraliste al di fuori della protezione dei dati personali. Ai nostri fini, anticipiamo soltanto come la tecnica sia utilizzata anche dal Digital Services Act, il quale determina autonomamente il proprio raggio di applicazione sostanziale e territoriale similmente a quanto fatto dal GDPR (v. *infra*: Cap. 6, par. 2). Si tratta di un deciso passo in avanti che rispecchia la svolta unilateralista dei tempi recenti, soprattutto se si considera che la Direttiva e-Commerce, vero predecessore del nuovo regolamento, affermava esplicitamente di non voler introdurre norme di diritto internazionale privato[201]. Quest'ultima, infatti, prevedeva soltanto, all'art. 3, che ciascuno Stato membro provvedesse affinché i servizi della società dell'informazione, forniti da un prestatore stabilito nel suo territorio, rispettassero le disposizioni nazionali vigenti in detto Stato membro. Ciò si è peraltro tradotto, quanto meno in Italia, nella formulazione di una norma che delimita unilateralmente la «gittata» del relativo strumento di recepimento, vale a dire l'art. 3, comma 1 D.lgs. 70/2003 (c.d. Codice del commercio elettronico), che – con un linguaggio molto simile a quello della direttiva – impone ai prestatori stabiliti sul territorio italiano di conformare i propri servizi della società dell'informazione allo stesso decreto ed alle disposizioni nazionali applicabili nell'ambito regolamentato.

5.2 Il Regolamento P2B tra unilateralismo e assenza di norme sulla giurisdizione

Oltre al Digital Services Act, sul quale ci si soffermerà specificamente in seguito, esemplificativo del nuovo paradigma unilateralista in materia di piattaforme digitali è anche il Regolamento P2B.

In particolare, l'art. 1, par. 2 di quest'ultimo ne determina l'ambito di applicazione territoriale, disponendo esplicitamente quanto segue:

[201] V. considerando 23 e art. 1, par. 4 Direttiva 2000/31/CE.

«*Il presente regolamento si applica ai servizi di intermediazione online e ai motori di ricerca online, a prescindere dal luogo di stabilimento o di residenza del fornitore di tali servizi e dal diritto altrimenti applicabile, forniti o proposti per essere forniti, rispettivamente, agli utenti commerciali e agli utenti titolari di siti web aziendali, che hanno il luogo di stabilimento o di residenza nell'Unione e che, tramite i servizi di intermediazione online o i motori di ricerca online, offrono beni o servizi a consumatori nell'Unione*».

La disposizione in commento stabilisce, in altre parole, che il Regolamento P2B si applica ai rapporti intercorrenti tra il gestore di una piattaforma stabilito in uno Stato terzo (come sovente capita con gli Stati Uniti) e un utente commerciale stabilito o residente nell'Unione, nella misura in cui questi si rivolga ad un consumatore che si trova in uno Stato membro (non è invece necessario che quest'ultimo risieda nell'Unione o sia cittadino di uno dei suoi Stati membri[202]). Analogamente al GDPR, pertanto, anche il Regolamento P2B pretende di applicarsi a situazioni e rapporti collocati, almeno in parte, al di fuori del territorio dell'Unione. Ciò sulla base dell'assunto per cui «i servizi di intermediazione online e i motori di ricerca online in genere hanno dimensione globale[203]».

Si noti inoltre come, nel determinare il proprio perimetro di applicazione, anche il Regolamento P2B faccia ricorso alla tecnica del «*targeting approach*». A tal proposito, il considerando 9 chiarisce come, per stabilire se un utente commerciale (o un utente di un sito web aziendale) offra beni o servizi a consumatori situati nell'Unione, occorra accertare se questi «rivolga» o meno le proprie attività verso uno o più Stati membri, interpretando il criterio sulla base della già ricordata giurisprudenza della Corte di giustizia relativa all'art. 17, par. 1,

[202] V. considerando 9 Regolamento P2B
[203] Idem.

lett. c) Regolamento Bruxelles I*bis* e all'art. 6, par. 1 Regolamento Roma I (v. *supra* par. 2.4.3, A)).

Il medesimo considerando 9 aggiunge, in chiusura, come il Regolamento P2B «dovrebbe inoltre applicarsi qualunque sia la legge altrimenti applicabile ad un contratto». Da tale previsione, letta in correlazione con la parte dell'art. 1, par. 2 per cui il Regolamento P2B si applica a prescindere «dal diritto altrimenti applicabile», è possibile dedurre l'intenzione del legislatore dell'Unione, già segnalata in dottrina[204], di qualificare il Regolamento P2B come «norma di applicazione necessaria» ai sensi dell'art. 9 Regolamento Roma I e dell'art. 16 Regolamento Roma II. Di conseguenza, nelle materie da esso regolate il Regolamento P2B troverebbe applicazione senza che l'interprete abbia bisogno di ricorrere alle norme di conflitto, per espresso volere dello stesso diritto internazionale privato dell'Unione. Una visione che rafforza ancora di più l'intento marcatamente unilateralista sotteso allo strumento.

Si è appena visto come il Regolamento P2B affronti quindi la questione della legge applicabile determinando unilateralmente la propria «gittata[205]» e qualificandosi come norma di applicazione necessaria. A differenza di quanto accade con il GDPR[206] tuttavia, lo stesso non si occupa della giurisdizione ma chiarisce, al contrario, di non pregiudicare il diritto dell'Unione applicabile, tra gli altri[207], nel settore della cooperazione giudiziaria in materia civile[208].

---

[204] P. FRANZINA, *op. cit.* sub Cap. 2, n. 51, p. 151.

[205] Idem.

[206] V. art. 79 GDPR.

[207] V. art. 1, par. 5 Regolamento P2B, che recita: «Il presente regolamento non pregiudica il diritto dell'Unione, in particolare il diritto dell'Unione applicabile nei settori della cooperazione giudiziaria in materia civile, della concorrenza, della protezione dei dati, della protezione dei segreti commerciali, della protezione dei consumatori, del commercio elettronico e dei servizi finanziari».

[208] V. art. 81 TFUE per la competenza dell'Unione europea in materia.

Come sottolineato in dottrina[209], il legislatore dell'Unione sembra quindi essersi preoccupato soltanto di realizzare uno strumento normativo uniforme per quanto riguarda la disciplina dei rapporti tra piattaforme e utenti commerciali, non ritenendo necessario intervenire con delle norme *ad hoc* sulla giurisdizione ma reputando sufficienti quelle generali di cui al Regolamento Bruxelles I*bis*. A questo proposito, si sono peraltro già analizzate le principali difficoltà relative all'applicazione nel mondo delle piattaforme dei criteri di collegamento previsti dal predetto Regolamento Bruxelles I*bis* (v. *supra* par. 2).

La scelta in questione è stata sottolineata con preoccupazione in dottrina[210] da chi ha visto nell'assenza di norme sulla giurisdizione un ostacolo all'effettivo raggiungimento degli obiettivi del Regolamento P2B. In particolare, il rischio rilevato è quello per cui le norme del Regolamento Bruxelles I*bis* – incluse quelle degli Stati membri, richiamate indirettamente dall'art. 6, par. 1 – non sempre consentirebbero di individuare come competenti i giudici di uno Stato membro.

Conseguenza di ciò sarebbe quella per cui un utente commerciale di uno Stato membro potrebbe, in alcuni casi, non essere in grado di invocare le tutele previste a suo favore del Regolamento P2B nei confronti di piattaforme e motori di ricerca stabiliti al di fuori dell'Unione. Infatti, in caso di procedimento incardinato presso uno Stato terzo, il Regolamento P2B potrebbe trovare applicazione soltanto se individuato come applicabile dal diritto internazionale privato del predetto Stato, eventualmente grazie a norme che, analogamente all'art. 9, par. 3 Regolamento Roma I[211], consentano di dare rilievo a norme di

---

[209] P. FRANZINA, *op. cit.* n. 51, pp. 148-150.

[210] Idem, pp. 152ss.

[211] Art. 9, par. 3 Regolamento Roma I: « Può essere data efficacia anche alle norme di applicazione necessaria del paese in cui gli obblighi derivanti dal contratto devono essere o sono stati eseguiti, nella misura in cui tali norme di applicazione necessaria rendono illecito l'adempimento del contratto. Per decidere se vada data efficacia a queste norme, si deve tenere conto

applicazione necessaria di ordinamenti diversi rispetto a quelli della *lex causae* o della *lex fori*[212]. Diversamente, il Regolamento P2B, nonostante le sue mire extraterritoriali figlie proprio della consapevolezza per cui gran parte dei gestori delle piattaforme digitali e dei motori di ricerca hanno sede al di fuori del territorio dell'Unione, fallirebbe in questi casi l'obiettivo di proteggere gli utenti commerciali dell'Unione europea.

5.3 Il «*regulatory overreaching*» e il bisogno strutturale della cooperazione delle piattaforme

L'analisi appena effettuata permette di affermare come la recente svolta unilateralista abbia portato con sé la tendenza degli ordinamenti giuridici ad estendere l'ambito di applicazione delle proprie legislazioni relative ad internet e alle nuove tecnologie sino a configurare, quanto meno in astratto, vere e proprie applicazioni extraterritoriali. Si tratta di una situazione che acuisce i conflitti tra i diversi ordinamenti giuridici, specie in aree che attengono alla tutela dei diritti fondamentali, come dimostrano vicende giudiziarie come la saga *Schrems*[213], relativa al trasferimento dei dati personali di cittadini dell'Unione europea verso gli Stati Uniti d'America.

Esempi come quello del Regolamento P2B portano inoltre a sollevare dei dubbi in merito all'effettività delle normative in questione, le quali, pur configurando in astratto un'applicazione (extra)territoriale piuttosto estesa, avrebbero concretamente poche possibilità di applicazione reale alle fattispecie da esse considerate. Si tratta di un fenomeno definito dalla dottrina «*regulatory*

della loro natura e della loro finalità nonché delle conseguenze derivanti dal fatto che siano applicate, o meno».

[212] P. FRANZINA, *op. cit.* n. 51, pp. 152ss.

[213] CGUE, *Schrems I*; CGUE, *Schrems II*.

overreaching[214]» e che interessa diversi ambiti del diritto relativi ad internet. Un fenomeno che è visto con sospetto sia in dottrina che dalle competenti autorità giurisdizionali o amministrative come, in materia di protezione dei dati personali, l'ex Gruppo di lavoro articolo 29[215] e il suo successore ai sensi del GDPR, vale a dire il Comitato europeo per la protezione dei dati (EDPB)[216].

Nell'ambito delle piattaforme digitali, i rischi di «*regulatory overreaching*» sono acuiti dalla constatazione per cui, per poter effettivamente applicare le proprie leggi ed eseguire le proprie decisioni all'interno di tali ambienti, gli Stati abbiano strutturalmente bisogno della cooperazione delle piattaforme stesse. Queste restano, infatti, i soggetti più «prossimi» alle fattispecie che si concretizzano nel mondo virtuale e risultano, tecnicamente, le sole in grado di applicare le regole e le decisioni degli ordinamenti statali in materie come la

---

[214] V. sul concetto di «*regulatory overreaching*» nel mondo digitale, ed in particolare in materia di protezione dei dati personali: L. A BYGRAVE, *op. cit.* n. 141; B. MAIER, *How Has the Law Attempted to Tackle the Borderless Nature of the Internet?* in International Journal of Law and Information Technology, Vol. 18, n. 2, pp. 145-172, 2010; C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, in International Journal of Law and Information Technology, Vol. 18, n. 3, pp. 227-247, 2010; L. MOEREL, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, in International Data Privacy Law, Vol. 1, n. 1, pp.28-46, 2011; D.J. SVANTESSON, *The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach*, EUI Working Papers, RCAS 2015/45, Robert Schuman Centre for Advanced Studies - Florence School of Regulation, 2015. Nelle opere appena menzionate il fenomeno viene trattato con preoccupazione. In senso parzialmente diverso D.J. SVANTESSON, *op. cit.* n. 78 (in particolare p. 233), il quale distingue tra «*bite jurisdiction*» e «*bark jurisdiction*», inquadrando nella seconda il «*regulatory overreaching*». Per Svantesson il fenomeno non sarebbe di per sé problematico ma lo sarebbe soltanto nel caso in cui le normative interessate dallo stesso non perseguano scopi «*morally justifiable*».

[215] Si vedano in particolare: WP29, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* – 5035/01/EN/Final WP 56, 30 maggio 2002; WP29, *Opinion 8/2010 on applicable law* – 0836-02/10/EN WP179, 16 dicembre 2010; WP29, *Orientamenti per l'esecuzione della sentenza della Corte di giustizia dell'Unione europea nella causa C-131/12 "Google Spain e Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González"* – 14/IT WP 225, 26 novembre 2014; WP29, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* – 176/16/EN WP 179 update, 16 dicembre 2015.

[216] EDPB, *Linee-guida 3/2018*, *cit.* n. 190.

proprietà intellettuale, il commercio elettronico o la diffusione di contenuti offensivi, diffamatori o comunque illegali. Si pensi, ad esempio, ai provvedimenti inibitori nei confronti di utilizzi illeciti di marchi, come nel già esaminato caso *Wintersteiger* (v. *supra*: par. 4.2).

Questa dipendenza di fatto dalle piattaforme è stata analizzata anche dalla giurisprudenza oltreoceano, in particolare nel caso *Google* v. *Equustek*, culminato in una decisione[217] della Corte Suprema del Canada resa nel 2017. La vicenda riguardava una serie di episodi di violazione dei diritti di proprietà intellettuale della società canadese Equustek Inc. commessi dalle distributrici del gruppo Datalink – vale a dire la canadese Datalink Technology Gateways Inc. e la statunitense Datalink Technology Gateways LLC. – attraverso la pratica del *re-labeling* e della vendita dei prodotti Equustek con l'etichetta di Datalink, oltre che con il furto di segreti industriali.

Si tratta di una saga giudiziaria che ha molto diviso la dottrina[218], sia nordamericana che europea, su questioni come l'estensione territoriale del diritto alla deindicizzazione, recentemente affrontata anche dalla Corte di Giustizia dell'Unione europea con riferimento al diritto all'oblio ex art. 17 GDPR[219]. La controversia ha inoltre visto l'intervento di associazioni a tutela dei diritti umani e della libertà di espressione, come Human Rights Watch, preoccupata dalla possibilità che Google divenisse una sorta di «censore mondiale[220]» delle informazioni condivise in rete.

---

[217] Supreme Court of Canada, 2017 SCC 34, *Google Inc.* v. *Equustek Solutions Inc.*, 28 giugno 2017.

[218] Per alcuni commenti sulla pronuncia si vedano: I. PRETELLI, *op. cit.* sub Cap. 1, n. 11, (pp. 28, 41-42); I. PRETELLI, *op. cit.* n. 2 (pp. 5-6).

[219] CGUE, causa C-507/17, *Google LLC* c. *Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019 – ECLI:EU:C:2019:772.

[220] V. la nota pubblicata da Human Rights Watch a commento a caldo della decisione: *Canada: Court Decision a Global Threat to Information Access*, 29 giugno 2017. Reperibile online: https://www.hrw.org/news/2017/06/29/canada-court-decision-global-threat-information-access.

Ai nostri fini, occorre evidenziare come la Equusteek avesse richiesto ed ottenuto una serie di ingiunzioni preliminari da parte di diverse autorità giudiziarie canadese, che non avevano però avuto l'effetto di far cessare le condotte illecite della propria controparte. Quest'ultima, infatti, aveva semplicemente deciso di lasciare il Canada e continuare con le proprie attività di vendita *online* in altre paesi. Di conseguenza, la Equustek si era rivolta, in via prima stragiudiziale poi giudiziale, a Google, chiedendo la deindicizzazione di tutti i risultati relativi ai prodotti controversi commercializzati dalla Datalink.

Di fronte alle resistenze iniziali di Google, a parere del quale la deindicizzazione avrebbe dovuto essere limitata soltanto al dominio canadese, la Corte ha fatto suo l'assunto per cui l'intervento della piattaforma fosse necessario per garantire l'effettiva tutela ai diritti della Equustek, affermando che:

«*Despite court orders prohibiting the sale of inventory [the foreign company] continues to carry on its business from an unknown location, selling its impugned product on its websites to customers all over the world* […].

Google controls between 70-75 percent of the global searches on the Internet and that Datalink's ability to sell its counterfeit product is, in large part, contingent on customers being able to locate its websites through the use of Google's search engine. Only by preventing potential customers from accessing the Datalink websites, could Equustek be protected. Otherwise, Datalink would be able to continue selling its product online and the damages Equustek would suffer would not be recoverable at the end of the lawsuit[221]»

Partendo da ciò, la *Supreme Court* ha inoltre riconosciuto la necessità di applicare su scala globale i provvedimenti inibitori a favore della Equustek, non limitando la propria efficacia al solo dominio canadese, facendo leva sulla natura intrinsecamente globale ed immateriale di internet:

[221] SCC, *Google Inc.* v. *Equustek Solutions Inc.*, punto 11.

«Where it is necessary to ensure the injunction's effectiveness, a court can grant an injunction enjoining conduct anywhere in the world. The problem in this case is occurring online and globally. The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally[222]».

Con la pronuncia in commento, la Corte Suprema canadese ha quindi preso sostanzialmente atto dell'impossibilità degli ordinamenti statali di esercitare la propria sovranità in rete senza la cooperazione delle piattaforme e dei motori di ricerca. Una constatazione che, unita alle riflessioni svolte nelle pagine precedenti ed alle sempre più diffuse mire extraterritoriali degli ordinamenti giuridici, rafforza la tesi della necessità di nuovi paradigmi che prendano in considerazione, oltre ai tradizionali diritti di matrice statale o comunque pubblica, anche il potere regolatorio di soggetti privati come le piattaforme digitali. Ciò, innanzi tutto, allo scopo di controllarlo o comunque di orientarlo al rispetto di principi stabiliti dal regolatore pubblico.

[222] SCC, *Google Inc.* v. *Equustek Solutions Inc.*, punto 18.

Capitolo 4 – *Private regulation* e diritto di fonte pubblica nella *governance* delle piattaforme digitali

SOMMARIO: 1 *Private regulation*: caratteri essenziali, dimensione transnazionale e rapporti con il diritto internazionale privato. – 1.1 Inquadramento del fenomeno *della private regulation*. – 1.2 La dimensione transnazionale della regolamentazione privata e la *nozione di* «*transnational private regulation*». – 1.3 La risoluzione dei conflitti tra regimi di «*transnational private regulation*». – 1.3.1 La «*meta-regulation*» e la regolamentazione delle attività dei regolatori privati. – 1.3.2 . – 2 La *Lex Informatica*: dalla sua teorizzazione al rifiuto della dottrina internazionalprivatista. – 2.1 L'emersione del fenomeno e i suoi caratteri essenziali. – 2.2 I rapporti tra norme di fonte pubblica e Lex Informatica nella regolamentazione di Internet. – 2.2.1 Internet (o il ciberspazio) come spazio in grado di dar vita ad ordinamenti giuridici autonomi. – …*Segue*: e le implicazioni di diritto internazionale privato. – 2.2.2 Gli avversari della *Lex Informatica* nella dottrina statunitense. –…*Segue*: e quelli nella dottrina e nella giurisprudenza dell'Unione europea. – 2.2.3 La ricerca di soluzioni mediane che valorizzino l'autoregolamentazione della rete. – 3 Il riconoscimento della dimensione istituzionale delle piattaforme da parte del legislatore dell'Unione ed il suo tentativo di controllarla. – 3.1 Le strategie regolatorie delineate dalla Commissione europea. – 3.1.1 La prima opzione: la tradizionale «*top-down regulation*». – 3.1.2 La promozione di sistemi di auto. – 3.1.3 La coregolamentazione: una soluzione mediana. – 3.2 La dimensione istituzionale delle piattaforme nel diritto dell'Unione. – 3.2.1 Il sostegno istituzionale all'adozione di codici di condotta e di regole coerenti con il diritto dell'Unione. – 3.2.2 Il GDPR e l'approvazione formale di strumenti di regolamentazione privata. – A) Codici di condotta e meccanismi di certificazione. – B) La regolamentazione privata nella disciplina sul trasferimento dei dati verso paesi terzi. – 3.2.3 Altri elementi distintivi: trasparenza, *accountability*, sanzioni pecuniarie.

1 *Private regulation*: caratteri essenziali, dimensione transnazionale e rapporti con il diritto internazionale privato

Nel presente capitolo ci si concentrerà sul rapporto tra diritto di fonte pubblica, incluso il diritto internazionale privato, e «*private regulation*» nell'ambito delle piattaforme digitali. Un'analisi che risulta essenziale per comprendere appieno la dimensione istituzionale delle piattaforme e l'operare dei loro gestori come regolatori privati.

1.1 Inquadramento del fenomeno della *private regulation*

L'espressione «*private regulation*» viene utilizzata in dottrina[1] per indicare dei veri e propri sistemi normativi composti da regole, inclusi standard tecnici o regole di condotta, stabilite da soggetti privati – come società, associazioni di categoria, organizzazioni non governative, gruppi di attivisti o esperti tecnici – ed afferenti a determinati settori o comunità. In particolare, con l'espressione «*regulation*» (traducibile in italiano con «regolamentazione») si intende l'esercizio di un controllo su alcune attività attraverso un insieme di norme definite allo scopo di raggiungere determinati obiettivi[2]. Il controllo esercitato dai regolatori privati non è, peraltro, limitato alla determinazione delle regole ma si estende anche alla creazione e all'utilizzo degli strumenti necessari per garantirne l'applicazione e il rispetto nei settori di riferimento («*enforcement*»).

---

[1] Per una ricognizione generale del fenomeno si rimanda innanzi tutto, *ex multis*, alla dottrina citata nelle note n. 44 e 57 di cui al Capitolo I. Si vedano altresì: M. DE BELLIS, *Public Law and Private Regulators in the Global Legal Space*, in International Journal of Constitutional Law, Vol. 9, n. 2, pp. 425-448, 2011; H. SCHEPEL, *Private Regulators in Law*, in J. PAUWELYN, R. WESSEL, J. WOUTERS, (a cura di), *Informal International Lawmaking*, pp. 356-367, Oxford University Press, 2012; K. PURNHAGEN, *Mapping Private Regulation – Classification, Market Access and Market Closure Policy and Law's Response*, in Journal of World Trade, Vol. 49, n .2, pp. 309-324, 2015; P. VERBRUGGEN, *Regulating Private Regulators: Understanding the Role of Private Law*, in European Review of Private Law, Vol. 27, n. 2, pp. 175-186, 2019. Per una definizione ed analisi del concetto di «regulation» si veda invece: R. BALDWIN, M. CAVE, M. LODGE, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2010.

[2] R. BALDWIN, M. CAVE, M. LODGE, *op. cit*, p. 2.

Si tratta di un fenomeno non nuovo, posto che già in epoche passate si è più volte assistito allo sviluppo spontaneo di sistemi di norme di fonte privata destinate a disciplinare alcuni settori economici o i rapporti afferenti a determinate comunità di individui. Uno degli esempi più noti forniti in dottrina è la c.d. «*lex mercatoria*[3]», sviluppatasi spontaneamente a partire dall'epoca medioevale nel settore del commercio.

Pur non costituendo una novità dei tempi recenti, tuttavia, il fenomeno della *private regulation* non è ancora stato ricondotto ad unità dalla dottrina, ove si registrano diverse resistenze in merito al riconoscimento stesso della categoria[4]. Non è questa la sede per addentrarci nel dibattito relativo alla valenza generale della nozione. Ai nostri fini, basti qui indicare alcune caratteristiche essenziali e stabilire dei punti fermi.

Fenomeni di *private regulation* si sono, come detto, sviluppati nel tempo nell'ambito di alcuni settori economici – come il commercio internazionale, la tutela dell'ambiente o il mercato energetico – o comunità di individui in cui il potere regolatorio dei tradizionali soggetti pubblici ha lasciato spazio a quello di attori privati, sia per tramite di formali atti di delega o de-regolamentazione («*de-regulation*») sia a causa dello spontaneo e crescente emergere di regole di fonte privata in grado di prevalere su quelle di fonte pubblica[5]. Peraltro, a seconda del settore di riferimento, la «privatizzazione» dell'attività regolatoria ha avuto come risultato una sempre maggior concentrazione del potere rego-

---

[3] Sul tema si vedano *ex multis*: R. MICHAELS, *op. cit.* Cap. 1, n. 44; F. BASSAN, *Digital Platforms and Global Law*, Edward Elgar, 2021 (v. in particolare p. 94); A.M. LUCIANI, *La nuova lex mercatoria*, in Osservatorio sulle fonti, fasc. 1, pp. 241-254, 2021. Disponibile online su: www.osservatoriosullefonti.it

[4] A questo proposito si veda, ad esempio, F. CAFAGGI, *op. cit.* Cap. 1, n. 44. In quest'opera l'autore afferma esplicitamente «*for many, 'private regulation' remains an oxymoron*» indicando come per gran parte della dottrina gli unici regolatori esistenti possano essere soltanto quelli pubblici.

[5] V. *ex multis*: F. CAFAGGI, *op. cit.* Cap. 1, n. 44; P. VERBRUGGEN, *op. cit.* Cap. 4, n. 1.

latorio in capo a pochi soggetti mentre, in altri, ha dato luogo ad una proliferazione (e conseguente frammentazione) di standard e regole di condotta di fonti diverse[6].

La regolamentazione privata si estrinseca in diverse forme. Tradizionalmente, con l'espressione «*private regulation*» si sono intesi i fenomeni di autoregolamentazione pura, attraverso cui taluni soggetti privati adottano strumenti come norme interne alla loro specifica comunità (come, ad esempio, alcuni settori economici o le stesse piattaforme digitali[7]), codici di condotta[8] o standard tecnici[9] all'esclusivo scopo di orientare i propri comportamenti. Questa prima forma di regolamentazione privata si connota pertanto per una tendenziale coincidenza tra colui che stabilisce regole e colui che vi è sottoposto, da cui deriva la qualificazione in termini di «autoregolamentazione» («*self-regulation*» in inglese) operata dalla dottrina[10].

Accanto a queste forme tradizionali di «*private regulation*», la dottrina[11] ne ha individuate altre di più recente emersione, che si distinguono dalle precedenti in quanto non sono caratterizzate dalla coincidenza tra regolatori e destinatari delle norme. Al contrario, si tratta, infatti, di fenomeni emersi in settori in cui determinati attori privati stabiliscono regole volte a disciplinare non soltanto le proprie condotte ma anche quelle di altri soggetti. A tal proposito, la richiamata dottrina distingue ulteriormente tra le organizzazioni in cui un unico regolatore stabilisce le regole destinate agli altri soggetti ad esse aderenti e le

---

[6] F. CAFAGGI, *op. cit.* Cap. 1, n. 44, p. 1.
[7] D. WIELSCH, *Private Law Regulation of Digital Intermediaries*, in European Review of Private Law, Vol. 27, n. 2, pp. 197-220, 2019.
[8] A. BECKERS, *Towards a Regulatory Private Law Approach for CSR Self- Regulation? The Effect of Private Law on Corporate CSR Strategies*, in European Review of Private Law, Vol. 27, n. 2, pp. 220-244, 2019.
[9] J. CONTRERAS, *Private Law, Conflict of Laws, and a Lex Mercatoria of Standards-Development Organizations*, in European Review of Private Law, Vol. 27, n. 2, pp. 245-268, 2019.
[10] V. a questo proposito: F. CAFAGGI, *op. cit.* Cap. 1, n. 44; P. VERBRUGGEN, *op. cit.* n. 1.
[11] V. in particolare F. CAFAGGI, *op. cit.* Cap. 1, n. 57.

organizzazioni c.d. «*multi-stakeholder*», in cui più soggetti portatori di interessi, anche tra loro eterogenei, stabiliscono le norme applicabili in un determinato settore. La platea dei soggetti coinvolti nella «*private regulation*» risulta ulteriormente allargata nei regimi in cui la dottrina ha individuato, oltre ai regolatori e ai destinatari delle norme, figure come i «beneficiari» – tra cui si collocano, ad esempio, consumatori, lavoratori e comunità che traggono vantaggio, anche indirettamente, delle regole adottate – o gli «intermediari» delle norme, vale a dire esperti, consulenti tecnici, o organi di certificazione che ne favoriscono il rispetto da parte dei destinatari[12].

1.2 La dimensione transnazionale della regolamentazione privata e la nozione di «*transnational private regulation*»

Uno dei tratti caratteristici della regolamentazione privata è la sua capacità di disciplinare gli ambiti cui essa afferisce trascendendo i confini degli Stati e degli altri ordinamenti giuridici tradizionali, come le organizzazioni internazionali. Questa caratteristica ha portato gli studiosi del fenomeno[13] a riferirsi allo stesso con la formula «*transnational private regulation*», che indica sia la natura privata che quella transnazionale di esso.

L'espressione «diritto transnazionale» è stata utilizzata per la prima volta nella dottrina statunitense[14] degli anni '50 per segnalare l'esistenza di norme che, pur interessando fattispecie che coinvolgono più ordinamenti giuridici, non appaiono del tutto riconducibili alle tradizionali categorie del diritto internazionale pubblico e privato. Senza pretese di addentrarci nell'ampio di-

[12] V. P. VERBRUGGEN, *op. cit.* n. 1.
[13] V. dottrina citata alla nota n. 57 del Capitolo 1.
[14] P.C. JESSUP, *Transnational Law*, Yale University Press, 1956.

battito dogmatico sviluppatosi intorno a questa nozione dai confini ancora incerti[15], basti ai nostri fini rilevare come si tratti di una categoria residuale, in cui la dottrina tradizionale[16] ha ricondotto quei fenomeni che portano all'impiego di norme giuridiche comuni nell'ambito di ordinamenti diversi, per via dello spontaneo riconoscimento dell'idoneità di un principio o di una regola a valere come norma giuridica anche fuori dall'area con riferimento alla quale è stata adottata, in maniera indipendente rispetto ad una sua formale adozione. In questo senso, quindi, la nozione include norme originariamente prodotte da fonti eterogenee, anche diverse da quelle pubbliche e tra cui si annoverano, per i fini che qui interessano, quelle private. Tra gli esempi di diritto transnazionale si possono citare, oltre alla *lex mercatoria*, la *lex informatica* (su cui v. *infra* par. 2) e la *lex sportiva*[17].

La dottrina[18] ha individuato diverse cause per spiegare l'emersione di fenomeni di *transnational private regulation*. Tra queste, vi è innanzi tutto la difficoltà per gli Stati di disciplinare in maniera esaustiva gli scambi e le esternalità che caratterizzano l'economia della globalizzazione. Ciò vale in particolare per la tutela dei cosiddetti «beni pubblici globali» (come la deforestazione, le emissioni, la sicurezza alimentare o la stabilità finanziaria), ambito in cui si sono sviluppati diversi regimi di regolamentazione privata a livello transnazionale,

---

[15] V. *ex multis*: R. TARCHI, *Diritto transnazionale o diritti transnazionali? Il carattere enigmatico di una categoria giuridica debole ancora alla ricerca di un proprio statuto*, in Osservatorio sulle fonti, fasc. 1, pp. 1-16, 2021. Disponibile online su: www.osservatoriosullefonti.it

[16] V. a questo proposito: A. PIZZORUSSO, *Corso di diritto comparato*, Giuffré, 1983; R. TARCHI, *op. cit*.

[17] V. *ex multis*: R.C.R, SIEKMANN, J. SOEK, *Lex Sportiva. What is Sport Law?*, Springer, 2012; S. BASTIANON, *La lex sportiva*, in Osservatorio sulle fonti, fasc. 1, pp. 349-366. Disponibile online su: www.osservatoriosullefonti.it

[18] V. dottrina citata alla nota 44 di cui al Cap. 1. Per una ricostruzione del fenomeno anche in chiave storica si rimanda in particolare a: F. CAFAGGI, A. RENDA, R. SCHMIDT, *Transnational Private Regulation*, in OECD, *International Regulatory Co-operation: Case Studies, Vol. 3: Transnational Private Regulation and Water Management*, pp. 9-58, OECD Publishing, 2013; F. CAFAGGI, *A Comparative Analysis of Transnational Private Regulation: Legitimacy, Quality, Effectiveness and Enforcement*, EUI Working Paper LAW 2014/15, 2014.

viste anche le difficoltà di raggiungere il consenso politico necessario per l'adozione di strumenti di diritto internazionale tradizionale. Sempre alla globalizzazione si ricollega la crescita del fenomeno nel contesto delle economie delle c.d. «catene del valore» («*supply chain*»), in cui la diffusione di norme uniformi di fonte privata dovrebbe facilitare il rispetto di standard minimi – ad esempio, in materia di diritti umani o di sicurezza sul lavoro – anche nell'ambito di giurisdizioni le cui norme di fonte pubblica si collochino al di sotto di tali livelli.

Un altro fattore che ha favorito la proliferazione del diritto transnazionale di fonte privata è rappresentato dai costanti e rapidi cambiamenti che interessano alcuni settori cruciali dell'economia contemporanea, come le tecnologie digitali. Questa continua evoluzione ha infatti portato i regolatori pubblici ad affidarsi in maniera sempre più decisiva ai privati, perlomeno per quanto riguarda la definizione di standard tecnici e misure esecutive. È il caso della *governance* di internet, in cui il ruolo di regolatori privati come l'Icann (Corporation for Assigned Names and Numbers) o il World Wide Web Consortium (W3C) risulta molto esteso (v. *infra* par. 2.1). In altri casi, la necessità di risolvere questioni tecniche di particolare difficoltà ha favorito l'intervento regolatorio di soggetti privati in possesso delle necessarie conoscenze in ambiti come la sostenibilità, le grandi infrastrutture o l'utilizzo delle risorse naturali.

1.3 La risoluzione dei conflitti tra regimi di «*transnational private regulation*»

La proliferazione dei regimi di «*transnational private regulation*» ha portato alla moltiplicazione dei conflitti normativi[19], soprattutto per quanto riguarda i

[19] V. *ex multis*: R. MICHAELS, *The Re-State-ment of Non-State Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism*, in Wayne Law Review, Vol. 51, n. 3, p. 1209-1260, 2005, p. 1250.

settori in cui si sono sviluppati più di un sistema di regolamentazione privata transnazionale. È il caso, ad esempio, delle norme in materia di deforestazione, ambito nel quale la dottrina[20] ha individuato la presenza di diversi regimi di *transnational private regulation*, emersi a partire della metà degli anni '90 a causa delle difficoltà nel raggiungere, a livello di Stati, il consenso politico necessario per l'adozione di strumenti di diritto internazionale tradizionale.

Per risolvere i conflitti in questione – che coinvolgono, oltre ai regimi di *transnational private regulation*, anche le norme di fonte pubblica – la dottrina ha teorizzato diversi metodi. Tra questi si possono scorgere, innanzi tutto, metodi volti a orientare l'attività dei regolatori privati transnazionali allo scopo di favorire la coerenza o l'uniformità tra i vari sistemi. Altri metodi, propugnati sinora da una parte minoritaria della dottrina, coinvolgono invece il diritto internazionale privato.

1.3.1 La «*meta-regulation*» e la regolamentazione delle attività dei regolatori privati

Con il termine «*meta-regulation*» la dottrina[21] indica una serie di fenomeni di creazione di regole, pratiche o standard in grado di influenzare l'attività e le procedure dei regolatori privati in modo da indurli al rispetto di principi comuni. In questo senso, la meta-regolamentazione viene considerata come uno degli strumenti principali attraverso cui risolvere i conflitti tra i diversi regimi di *transnational private regulation* creando, allo scopo, un coordinamento tra i medesimi.

I predetti fenomeni si basano sulle attività di meta-regolatori («*meta-regulator*») sia privati che pubblici che, a seconda delle proprie caratteristiche e dei

[20] V. *ex multis*: J. BOMHOFF, A. MEUWESE, *op. cit.* Cap. 1 n. 44; F. CAFAGGI, *op. cit.* Cap. 1 n. 57.
[21] Idem.

rispettivi ambiti di riferimento, possono agire in modi diversi studiati dalla dottrina[22] e di seguito brevemente richiamati.

Un primo tipo di meta-regolamentazione è rappresentato dalla definizione, da parte di un meta-regolatore privato, di principi comuni per i singoli regolatori attivi in un medesimo ambito. Questi principi, a seconda della relazione che ciascun regolatore privato ha con il meta-regolatore, possono assumere natura vincolante[23] ovvero di semplici raccomandazioni il cui rispetto è meramente volontario. Dal punto di vista contenutistico, essi riguardano in genere la definizione, il monitoraggio e l'applicazione degli standard stabiliti da ciascun regolatore, definendo dei requisiti minimi sul processo di adozione, la separazione delle funzioni e i requisiti di conformità. Tra gli esempi rilevanti di meta-regolatori che agiscono in questo modo la dottrina[24] indicata l'Iso (Organizzazione Internazionale per la Standardizzazione), organizzazione non governativa con sede in Svizzera nata nel 1947 proprio allo scopo di creare standard uniformi a livello mondiali e che svolge anche diverse funzioni consultive per organismi delle Nazioni Unite. Il rispetto dei principi e delle *best practice* stabilite da questo genere di meta-regolatori viene perseguito – più che

[22] V. *ex multis*: J. BOMHOFF, A. MEUWESE, *op. cit.* Cap. 1, n. 44; F. CAFAGGI, *A Comparative Analysis of Transnational Private Regulation: Legitimacy, Quality, Effectiveness and Enforcement*, *op. cit.* Cap. 1, n. 57, p. 27ss.

[23] La vincolatività cui si fa riferimento non discende da norme di diritto di fonte pubblica quanto all'utilizzo di strumenti di diritto privato (come contratti) che disciplinano i rapporti tra il meta-regolatore ed il singolo regolatore privato. L'utilizzo di tali strumenti rileva in particolare nei regimi di *meta-regulation* che prevedono l'adesione ad organizzazioni con strutture basate sul diritto privato, come associazioni. Per approfondire si vedano le opere di F. CAFAGGI, ed in particolare: F. CAFAGGI, *op. ult. cit*; F. CAFAGGI, *The Architecture of Transnational Private Regulation*, EUI Working Paper LAW 2011/12, 2011; F. CAFAGGI, *op. cit.* Cap. 1 n. 57; F. CAFAGGI, *Transnational Private Regulation: Regulating Private Regulators*, in S. CASSESE (a cura di), *Research Handbook on Global Administrative Law*, pp. 212-141, Edward Elgar, 2016.

[24] F. CAFAGGI, *op. cit.* n. 22, p. 27. Tra gli altri esempi citati dall'autore vale la pena di menzionare l'EASA (European Advertising Standard Alliance), organizzazione che riunisce i principali regolatori privati nazionali europei in materia di annunci pubblicitari e che stabilisce *best practice* di settore applicabili per questi ultimi.

attraverso l'utilizzo di sanzioni legali – attraverso la pressione degli altri regolatori, i ritorni d'immagine negativi e il rischio di isolamento in caso di non conformità agli stessi.

Un'altra categoria individuata dalla dottrina[25] include i meta-regolatori che stabiliscono norme di equivalenza tra i diversi regimi di *private regulation*, con l'obiettivo di favorire il mutuo riconoscimento tra gli stessi. Il mutuo riconoscimento serve a favorire la certezza del diritto e lo sviluppo di relazioni transnazionali, oltre che a consentire ai soggetti sottoposti ai regimi oggetto dello stesso di ridurre i costi necessari per conformarsi a ciascuno di essi. Questo tipo di meta-regolamentazione non persegue, quindi, l'obiettivo dell'uniformità tra i diversi sistemi di *private regulation* ma piuttosto quello della loro coerenza ed effettività, lasciando più spazio all'autonomia dei regolatori privati[26].

Un terzo genere[27] di meta-regolamentazione vede invece coinvolti attori pubblici come organizzazioni internazionali (come il Fao, l'Ocse o l'Ilo) o altri soggetti promotori della cooperazione intergovernativa in determinati settori, come è il caso dello Iosco (International Organization of Security Commission). Tali soggetti, infatti, talvolta stabiliscono delle regole e dei principi comuni per i regolatori privati attivi nei propri ambiti di riferimento. Importante, per i fini di questo lavoro, il ruolo di meta-regolatore che viene svolto da organizzazioni regionali come l'Unione europea che, nell'ambito di taluni settori – la dottrina[28] porta come esempi la sicurezza alimentare, i sistemi di pagamento, la pubblicità o la diffusione di contenuti sui *social network* – definiscono

[25] V. *ex multis*: F. CAFAGGI, *op. ult. cit.* p. 27.
[26] Idem, p. 28. L'autore cita come esempi di meta-regolamentazione di questo genere i regimi in materia di sicurezza alimentare, soffermandosi in particolare sugli standard Gfsi (Global Food Safety Initiative), e quelli in materi agricola, menzionando a questo proposito il GLOBAL.G.A.P.
[27] Idem, p. 28.
[28] Idem, p. 28.

principi comuni o incoraggiano i regolatori privati a definirli essi stessi, anche attraverso strumenti di *soft-law* o intraprendendo con questi un confronto.

Dall'analisi, seppur sommaria, del fenomeno è possibile stabilire dei punti fermi. In particolare, la diffusione dei regimi di *meta-regulation* non sembra rispondere – nemmeno per i regimi del primo tipo – alla necessità di centralizzare il potere regolatorio in capo ad alcuni soggetti ma, al contrario, esprime il bisogno di coordinare i processi e le attività dei regolatori attivi nel medesimo ambito, conservando il pluralismo ma assicurando la coerenza, la credibilità e l'effettività di vari regimi[29]. Come rilevato in dottrina[30], inoltre, il fenomeno si caratterizza principalmente per promuovere la cooperazione tra regolatori privati attraverso strumenti, di fonte sia pubblica che privata, che abbiano l'effetto di influenzare il comportamento di tali regolatori senza disciplinarlo in maniera diretta ma promuovendo, al contrario, il dialogo tra le parti e l'adesione spontanea ai principi stabiliti dai meta-regolatori.

A questo riguardo, merita in ultimo di essere segnalato come parte della dottrina[31] abbia utilizzato l'espressione «*better regulation*», con cui si suole indicare le pratiche di regolamentazione attraverso procedimenti volti a valorizzare il dialogo tra regolatori pubblici – e, segnatamente, le organizzazioni internazionali e regionali – e privati, piuttosto che i tradizionali metodi «*command-and-control*» propri del diritto di fonte pubblica. Lo sviluppo dei processi di *better regulation*, segnalato e promosso anche dalla Commissione europea[32], ha portato la richiamata dottrina a ricondurre gli stessi nell'alveo dei fenomeni di

---

[29] Vedi: F. CAFAGGI, *Transnational Private Regulation: Regulating Private Regulators*, in S. CASSESE (a cura di), *Research Handbook on Global Administrative Law*, pp. 212-241, Edward Elgar, 2016, *op. cit* Cap. 1, n. 57, p. 234.

[30] V. *ex multis*: J. BOMHOFF, A. MEUWESE, *op. cit.* Cap. 1, n. 57, p. 141.

[31] Idem.

[32] V. in particolare: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Legiferare con intelligenza*

meta-regulation. Essi, infatti, appaiono capaci di influenzare in senso positivo i comportamenti dei regolatori spingendoli ad aprire dialoghi con i soggetti interessati ove occorra intraprendere dei processi di regolamentazione, anche nelle ipotesi in cui tali aperture non siano prescritte dal diritto vigente di fonte pubblica.

1.3.2 Il rapporto tra *transnational private regulation* e diritto internazionale privato

Una questione controversa in dottrina è quella relativa al rapporto tra regolamentazione privata e diritto internazionale privato. Ci si domanda, in particolare, se quest'ultimo possa assumere rilevanza nella risoluzione dei conflitti tra sistemi di *transnational private regulation*.

Le perplessità a riguardo si registrano sia tra gli studiosi del fenomeno della *transnational private regulation* che tra gli internazionalprivatisti. I primi, infatti, tendono – o quanto meno tendevano in passato –a disconoscere qualsiasi ruolo al diritto internazionale privato in merito all'attività regolatoria dei privati, inclusa la risoluzione dei conflitti tra i sistemi normativi frutto di tale attività[33]. Di contro, la dottrina internazionalprivatista è restia a riconoscere rilevanza alle norme di fonte diversa da quella pubblica – incluse quelle di *transnational private regulation* – ai fini della risoluzione dei conflitti di legge e della disciplina sulla giurisdizione. Ciò, in particolar modo, nell'ambito dell'Unione eu-

nell'Unione europea, COM(2010) 543 definitivo, 8 ottobre 2010; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Legiferare meglio per ottenere risultati migliori — Agenda dell'UE*, COM(2015) 215 final, 19 maggio 2015.

[33] V. *ex multis*: J. BOMHOFF, A. MEUWESE, *op. cit* Cap. 1, n. 57; F. CAFAGGI, *op. cit.* n. 29. Di quest'ultimo si veda anche F. CAFAGGI, *The Architecture of Transnational Private Regulation*, EUI Working Paper LAW 2011/12, 2011, *op. cit.* n. 23; R. MICHAELS, *op. cit.* n. 19; A. FISCHER-LESCANO, G. TEUBNER, *Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law*, in Michigan Journal of International Law, Vol. 25, n. 4, pp. 999-1046.

ropea, il cui diritto internazionale privato è, come abbiamo avuto modo di saggiare, fortemente improntate su logiche «stato-centriche» (v. *supra*: Cap. 3, par. 1.2).

Posto quanto sopra, come rilevato anche da attenta dottrina[34], nell'approcciarsi ai conflitti tra regimi di *transnational private regulation* non appare possibile omettere del tutto di considerare il diritto internazionale privato.

In primo luogo, infatti, le norme internazionalprivatistiche entrano comunque in gioco se si considera che alla base di qualsiasi sistema di *transnational private regulation* vi sono strumenti di diritto privato. Ad esempio, è grazie al loro inserimento in accordi contrattuali che viene perseguito il rispetto degli standard di fonte privata in materia ambientale o di sicurezza sul lavoro. Ancora, il fatto che gli stessi regolatori privati siano, come si è già avuto modo di constatare, soggetti come organizzazioni non governative, associazioni di categoria o imprese multinazionali, presuppone che la loro costituzione e la loro *governance* avvengano in conformità con norme di diritto privato di fonte pubblica. Trovandoci in contesti transnazionali, occorre chiedersi a quale ordinamento appartengono le norme in questione. Analogamente, è necessario domandarsi quale legge disciplini i contratti attraverso cui sono applicati gli standard della *private regulation*, così come porsi domande in merito alle questioni di giurisdizione relative agli stessi. Si tratta di interrogativi tipici del diritto internazionale privato, a cui quest'ultimo è chiamato a dare le relative risposte.

In aggiunta a ciò, una tesi minoritaria[35] sostiene che il diritto internazionale privato possa essere utilizzato allo scopo di orientare l'attività dei regolatori privati transnazionali, assumendo in questo modo funzioni meta-regolatorie analoghe a quelle poc'anzi esaminate (v. *supra* par. 1.3.1). Essa si basa sull'idea,

[34] J. BOMHOFF, A. MEUWESE, *op. cit.* Cap. 1, n. 57, p. 149.
[35] V. J. BOMHOFF, A. MEUWESE, *op. cit*. Cap. 1, n. 57, p. 151.

diffusa soprattutto nella dottrina nordamericani[36], per cui le norme di conflitto possano perseguire finalità di diritto materiale. In particolare, secondo questa corrente di pensiero le norme di conflitto andrebbero considerate alla stregua di altri strumenti di meta-regolamentazione in quanto influenzerebbero le attività dei regolatori privati inducendoli a ricercare una soluzione ai conflitti normativi per essi rilevanti senza tuttavia dover violare le disposizioni di diritto ad essi applicabili.

La tesi in questione, oltre che minoritaria, è eterodossa rispetto alla tradizionale impostazione su cui si fonda la scuola internazionalprivatista europea, per cui il diritto internazionale privato non persegue finalità di diritto materiale ma è caratterizzato dalla neutralità, funzionale alla localizzazione delle fattispecie e alla risoluzione dei conflitti di legge[37] a prescindere da valutazioni *lato sensu* politiche.

Eterodossa è anche la tesi per cui le norme di diritto internazionale privato possano considerare i regimi di *transnational private regulation* alla stregua di diritti di fonte pubblica, potendo in questo modo individuare gli stessi come «legge applicabile» ad una determinata fattispecie ricadente sotto il proprio ambito di applicazione[38]. Sul punto, come si è già visto (v. *supra*: Cap. 1, par. 3; Cap. 3, par. 1.2), la dottrina internazionalprivatista europea conserva un atteggiamento di generale chiusura, figlio dell'impostazione «stato-centrica» delle norme di diritto internazionale privato dell'Unione, in cui vi è uno spazio assai ridotto per diritti di fonte diversa da quella pubblica.

---

[36] Idem. Si veda inoltre, *ex multis*: C. JOERGES, *Constitutionalism in Postnational Constellations: Contrasting Social Regulation in the EU and in the WTO* in C. JOERGES, E.U. PETERSMANN (a cura di), *Constitutionalism, Multilevel Trade Governance and Social Regulation*, pp. 491-507, Hart Publishing, 2006.

[37] J. BOMHOFF, A. MEUWESE, *op. cit.* Cap. 1, n. 57, pp. 153ss.

[38] In senso positivo, quanto meno con riferimento alle regole delle piattaforme digitali: F. BASSAN, *op. cit.* n. 3, p. 112.

Il permanere di questa impostazione – che si fonda anche sul presupposto del carattere derivato delle regole di fonte privata, le quali abbisognerebbero sempre di un riconoscimento da parte degli ordinamenti pubblici per poter spigare i propri effetti[39] – non implica tuttavia una totale mancanza di considerazione della *private regulation* da parte del diritto di fonte pubblica, ed in particolare del diritto internazionale privato.

A tal proposito, nell'ambito della dottrina nordamericana[40] sono state individuate tre modalità attraverso cui i legislatori pubblici possono conferire rilevanza a norme di fonte diversa. Una prima modalità è rappresentata dall'incorporazione materiale dei precetti di queste ultime in strumenti di fonte pubblica. La seconda consiste invece nel considerare le regole non statali come dato di fatto, analogamente a quanto fatto dal già menzionato art. 17 del Regolamento Roma II (v. *supra*: Cap. 3, par. 3.2.2). La terza è quella per cui il regolatore pubblico, anziché intervenire direttamente a disciplinare determinate materie, delegherebbe la disciplina di esse al privato. Quest'ultimo fenomeno è tipico innanzi tutto della regolamentazione tecnica ma è stato altresì richiamato a proposito di norme generali in materia di contratti, come l'art. 1372 c.c. o l'art. 1134 del Code Napoléon, che conferiscono al contratto «forza di legge tra le parti[41]».

Quanto sopra rafforza l'idea per cui la regolamentazione dei soggetti privati, pur continuando a ricoprire un ruolo marginale nell'attuale sistema di diritto internazionale privato dell'Unione europea, non sia del tutto sconosciuta ai regolatori pubblici. Essi, al contrario, dimostrano di considerarla in più occasioni, in special modo nell'ambito di norme di matrice unilateralista (v. *supra*: Cap. 3, par. 5) contraddistinte dalla crescente responsabilizzazione di alcune

[39] R. MICHAELS, *op. cit.* n. 19.
[40] Idem, pp. 1231ss.
[41] Idem, p. 1235.

categorie di regolatori privati (v. *supra*: Cap 2, par. 2.3, 3.1) e, in alcuni casi, dal loro coinvolgimento nei processi legislativi o regolatori (v. *supra* par. 1.3.1, in particolare a proposito del fenomeno del *better regulation*). Aspetti che suggeriscono di perseguire l'idea per cui la creazione di nuovi paradigmi internazionalprivatistici possa essere funzionale anche ad un miglior inquadramento del fenomeno della *transnational private regulation* e, di conseguenza, dei conflitti tra regimi di questo genere.

2 La *Lex Informatica*: dalla sua teorizzazione al rifiuto della dottrina internazionalprivatista

Affrontato il tema della regolamentazione privata transnazionale, ci occupiamo adesso di un tipo specifico di *private regulation*, ossia la c.d. «*Lex Informatica*», più volte menzionata nelle pagine precedenti (v. *supra* par. 1.2; Cap. 1, par. 2.3). L'analisi del fenomeno, in parte già svolta, è rilevante ai nostri fini in quanto in esso rientra a pieno titolo anche l'attività regolatoria dei gestori delle piattaforme digitali.

2.1 L'emersione del fenomeno e i suoi caratteri essenziali

L'espressione «*Lex Informatica*[42]», al pari di formule tipo «*Code is Law*[43]», è stata coniata dalla dottrina statunitense degli anni '90 – momento in cui la rete iniziava realmente a diffondersi su scala globale – per segnalare l'esistenza di norme diverse da quelle di fonte pubblica in grado di regolare le attività degli utenti su internet (v. *supra*: Cap. 1, par. 2.3).

[42] L'espressione «Lex Informatica» è stata utilizzata per la prima volta da J.R. REIDENBERG, in *op. cit*. sub Cap. 1, n. 32.

[43] L'espressione «Code is Law» è stata utilizzata per la prima volta da L. LESSIG, *op. cit.* sub Cap. 1, n. 32 (I edizione).

La dottrina dell'epoca si riferiva, in primo luogo, agli standard e ai protocolli tecnici che permettono il funzionamento delle tecnologie digitali e il cui rispetto è necessario per chi vuole agire sulla rete. Tali protocolli sono stabiliti da attori privati come gli *internet service provider* o organizzazioni già citate (v. *supra* par. 1.2) come l'Icann (Ong statunitense responsabile, tra le altre cose, dell'assegnazione degli indirizzi IP e dei nomi a dominio) o la 3WC, anch'essa Ong statunitense che ha come scopo la promozione dello sviluppo del World Wide Web e che è responsabile, fra l'altro, della gestione del protocollo html.

A queste regole di tipo prettamente tecnico la dottrina affiancava (e tuttora affianca) le regole di condotta vigenti nell'ambito di una *community* online, sia essa un sito, una *mailing list*, una piattaforma *social*, un motore di ricerca o una *community* di altro tipo. Anche queste norme sono stabilite da soggetti diversi dai tradizionali regolatori pubblici e il loro rispetto è del pari necessario per chi vuole «far parte» della *community* o compiere attività giuridicamente rilevanti all'interno della stessa. Peraltro, se nei primi anni di diffusione di *internet* tali regole risultavano in prevalenza l'effetto di un processo di autogenerazione spontanea frutto dei comportamenti dei membri delle varie comunità digitali – da questo punto di vista assimilabile alla genesi della *Lex Mercatoria*[44] – con l'avvento delle piattaforme e, in generale, con l'affermarsi dei colossi c.d. «*big-tech*», le regole in questione sono diventate sempre più l'espressione di un incisivo potere regolatorio concentrato nelle mani di pochi soggetti privati[45].

---

[44] V. in questo senso: J.R. REIDENBERG, *op. cit*; L. LESSIG, *op. cit* (versione 2.0) sub Cap. 1, n. 32; D.R. JOHNSON, D. POST, *Law and Borders-The Rise of Law in Cyberspace,* Vol. 48, n. 5, Stanford Law Review, pp. 1378-1389, 1996.

[45] Già Lessig, nelle opere citate, ammoniva sul fatto che il ciberspazio, lungi dall'essere un luogo (virtuale) senza alcun tipo di regolamentazione sarebbe, al contrario, divenuto «*a perfect tool of control*» – v. L. LESSIG, *op. cit.* (versione 2.0), sub Cap. 1, n. 32, p. 4. Più di recente si veda, nell'ambito della dottrina italiana: G. L. CONTI, *La lex informatica*, in Osservatorio sulle fonti, fasc. 1/2021, pp. 317-347, 2021. Disponibile online su: www.osservatoriosullefonti.it

Dal punto di vista strutturale, la dottrina ha individuato tre caratteristiche distintive della *Lex Informatica* che ne avrebbero favorito l'emersione[46]. La prima è data dal fatto che le regole alla base della stessa, ed in particolare quelle tecniche, sono uniformi e hanno un'efficacia che prescinde dai territori e dai confini degli Stati. La seconda è rappresentata dal relativamente agevole – specie se paragonato alle procedure tipiche degli ordinamenti giuridici tradizionali – processo di creazione e modificazione delle norme, sia tecniche che di condotta, che ne facilita l'adattamento ai continui progressi tecnologici e la loro differenziazione, anche a seconda dell'area geografica in cui si trovano gli utenti della rete. In ultimo, la *Lex Informatica* si contraddistingue per la più volte richiamata capacità dei regolatori privati di monitorarne il rispetto e garantirne l'applicazione senza bisogno di azioni coercitive esterne («*self-enforcement*»), in particolare da parte degli Stati.

2.2 I rapporti tra norme di fonte pubblica e *Lex Informatica* nella regolamentazione di Internet

Sin dai primi studi in merito alla regolamentazione di internet, la dottrina[47] si è interrogata sui rapporti tra *Lex Informatica* e diritti di fonte pubblica, rilevando la presenza di molteplici conflitti. A tal riguardo, da entrambe le sponde dell'Atlantico sono state (e sono tuttora) tenute in particolare considerazione le questioni internazionalprivatistiche, inevitabilmente sollevate dall'interazione, spesso in tempo reale, tra soggetti stabiliti in qualsiasi parte del mondo. Nel dibattito, non scevro di contrasti ideologici e di ricadute cruciali in termini di diritti umani e tenuta della democrazia[48], si sono in particolare contrapposte

---

[46] V. in questo senso: J.R. REIDENBERG, *op. cit*, p. 577ss.

[47] Per una sintesi del dibattito si veda: R. MICHAELS, *op. cit*. n. 19, pp. 1215ss; L. LESSIG, *op. cit.* sub Cap. 1, n. 32, p. 300ss; P.S. BERMAN, *The Globalization of Jurisdiction*, in University of Pennsylvania Law Review, Vol. 151, n. 2, pp. 311-529, 2002 (v. in particolare pp. 367ss e pp. 400ss).

[48] V. ex multis: F. BIGNAMI-G. RESTA, *op. cit*; G. DELLA MORTE; *op. cit.* n. 47, Cap. 1. Si veda inoltre la dottrina già citata alla nota 44 del presente capitolo.

due correnti dottrinali, con una terza ha tentato una sintesi che, per certi versi, viene condivisa da chi scrive.

2.2.1 Internet (o il ciberspazio) come spazio in grado di dar vita ad ordinamenti giuridici autonomi

Secondo una prima tesi[49], internet – o, meglio, il ciberspazio[50] – dovrebbe essere considerato, ai fini giuridico-regolatori[51], come uno «spazio» (seppur virtuale) separato dai territori su cui esercitano il proprio potere i tradizionali regolatori pubblici. Uno spazio governato da proprie regole – la *Lex Informatica* – capaci di dar vita, all'interno di esso, ad ordinamenti giuridici autonomi rispetto a quelli degli Stati o delle organizzazioni internazionali.

Questa visione si basava sull'assunto per cui le novità portate da internet sarebbero state talmente dirompenti da mettere in crisi il concetto stesso di sovranità territoriale. In particolare, la natura immateriale del ciberspazio e la sua capacità di azzerare le distanze spazio-temporali tra gli utenti[52], permettendo in ogni momento la costituzione di rapporti transnazionali, aveva fatto propendere la dottrina[53] in commento per la sostanziale impossibilità, da parte dei regolatori pubblici, di disciplinare e controllare le attività effettuate nello stesso. Nello specifico, veniva constatata già allora la tendenza degli Stati (o delle organizzazioni internazionali) a tentare di estendere la propria sovranità

---

[49] Tra i fautori di questa prima tesi si vedano, *ex multis*: J.R. REIDENBERG, *op. cit*. p. 568ss; D.R. JOHNSON, D. POST, *op. cit*.

[50] Per la differenza tra i concetti di «Internet» e di «ciberspazio» si veda L. LESSIG, *op. cit*, sub Cap. 1, n. 32, p. 83ss.

[51] L'espressione generale è stata scelta in quanto la prima dottrina, soprattutto negli Stati Uniti, si è soffermata in generale sul tema della regolamentazione di Internet, in una prospettiva multidisciplinare. Il tema è stato poi approfondito avendo riguardo a specifiche branche del diritto. Per quanto riguarda il diritto internazionale privato si veda *ex multis*: D.J. SVANTESSON, *op. cit.* sub. Cap. 1, n. 46. Per quanto riguarda il diritto internazionale pubblico si veda invece G. DELLA MORTE, *op. cit.* Cap. 3, n. 185.

[52] Sui concetti di «despazializzazione» e «detemporalizzazione» si veda G. DELLA MORTE, *op. cit.* n. 51, p. 10ss.

[53] D.R. JOHNSON, D. POST, *op. cit.* n. 44 p. 1371ss.

in rete attraverso norme con ambiti di applicazione (extra)territoriali[54] in astratto molto ampi ma con possibilità di applicazione pratica sostanzialmente nulle (v. *supra*: Cap. 3, par. 5.3 sul fenomeno del «*regulatory overreaching*»). A questa tendenza veniva affiancata quella relativa all'adozione di norme protettive, anch'esse difficilmente attuabili in concreto.

Dal fallimento dei regolatori pubblici, la menzionata dottrina ricavava la conseguenza per cui le sole norme in grado di regolare in maniera esaustiva e concreta le attività che si svolgono nel ciberspazio fossero quelle originatisi nell'ambito dello stesso[55], ossia le medesime regole tecniche e di condotta alla base della teoria della *Lex Informatica*. Secondo questo approccio, nella rete non si sarebbe costituito un solo ordinamento giuridico, ma diversi ordinamenti facenti capo ai rispettivi regolatori privati, ciascuno dei quali «sovrano» su una specifica parte del ciberspazio. È il caso di siti internet, delle piattaforme o delle altre «*community*» digitali, così come quello delle già citate organizzazioni private responsabili dell'architettura tecnica e della gestione dei protocolli di *internet* (v. *supra* par. 1.2 e par. 2.1).

In altre parole, secondo questa impostazione – non a caso sostenuta a livello ideologico dai fautori del movimento dei c.d. *cyberanarchist*[56] – il ciberspazio veniva percepito come uno spazio virtuale i cui legami con il territorio fisico avrebbero avuto un'importanza del tutto marginale ai fini della sua regolamentazione e in cui il diritto di fonte pubblica avrebbe semplicemente ceduto

[54] La categoria dell'extraterritorialità permea tutto il dibattito sorto nell'ambito della dottrina statunitense in merito alla regolamentazione di Internet.
[55] Idem, p. 1387.
[56] Si veda in particolare la *Cyberspace Independence Declaration* pubblicata nel 1996 dal poeta, attivista e sociologo John Perry Barlow – già autore di diversi testi delle canzoni dei Grateful Dead –in risposta all'approvazione da parte del Congresso degli Stati Uniti del *Telecommunications Act of 1996*.

il passo davanti al potere regolatorio dei codici e dei protocolli informatici alla base dell'architettura della rete.

…*Segue*: e le implicazioni di diritto internazionale privato

Dal punto di vista del diritto internazionale privato, questa tesi aveva come prima conseguenza quella per cui gli ordinamenti giuridici tradizionali avrebbero dovuto riconoscere ed applicare il diritto della rete, o quanto meno non interferire con l'applicazione di esso da parte dei regolatori privati all'interno dell'ambiente virtuale[57]. Negli Stati Uniti, studiosi come Johnson e Post[58] hanno tentato di utilizzare a questo scopo la dottrina della c.d. «*comity*[59]», tipica dell'ordinamento statunitense[60] e definita dalla Corte Suprema come «*the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its law*[61]».

I due studiosi, inoltre, hanno fondato le proprie argomentazioni sulla dottrina della c.d. «*delegation*», che indica il fenomeno per cui i regolatori pubblici delegano la regolamentazione di determinati ambiti a soggetti privati, spesso nelle vesti di autoregolatori (in senso analogo v. *supra*, par. 1.1). L'applicazione

---

[57] V. R. MICHAELS, *op. cit.* n. 19, p. 1216.

[58] D.R. JOHNSON, D. POST, *op. cit.* n. 44 p. 1391ss.

[59] Per approfondire la dottrina della «*comity*» si rimanda ai seguenti scritti citati da Johnson e Post: H.E. YNTEMA, *The Comity Doctrine*, in Michigan Law Review, Vol 65, n. 1, pp. 9-32, 1966; S.R. SWANSON, *Comity, International Dispute Resolution and the Supreme Court*, in Georgetown Journal of International Law, Vol. 21, pp. 333-365, 1990, disponibile su SSRN: https://ssrn.com/abstract=1955652; L. BRILMAYER, *Conflict of Laws: Foundations and Future Directions*, Little Brown & Co, 1991; J.R. PAUL, *Comity in International Law*, in Harvard International Law Journal, Vol. 32, n. 1, pp. 2-44, 1991.

[60] Si veda ad esempio la Sec. 403 del Foreign Relations Law, citata in D.R. JOHNSON, D. POST *op. cit.* p. 1391.

[61] V. in particolare la sentenza 159 U.S. 113, *Henry Hilton* v. *Gustave Bertin Guyot, et al.*, 3 giugno 1895, nella quale la Corte Suprema degli Stati Uniti ha per la prima volta fatto uso della nozione per il riconoscimento e l'esecuzione di decisioni di Stati esteri.

congiunta di entrambe le dottrine avrebbe quindi dovuto portare alla delega, da parte degli ordinamenti giuridici tradizionali, della regolamentazione di intere questioni attinenti al ciberspazio a favore di regolatori privati non per forza sottoposti alla giurisdizione dei primi ma le cui regole sarebbero state riconosciute da questi proprio in virtù della «*comity*».

Sempre nell'ambito della dottrina statunitense – che, come si è già detto, è stata la prima ad essersi interessata al fenomeno dell'autoregolamentazione di internet – merita infine di essere richiamato il pensiero di Reidenberg, autore a cui si deve l'espressione «*Lex Informatica*». A parere dello studioso, in particolare, le già citate caratteristiche del sistema normativo da egli teorizzato – vale a dire l'essere formato da un sistema di norme uniformi a livello transnazionale, facilmente adattabili a seconda delle peculiarità di ciascuna area geografica e applicabili all'interno del proprio spazio (virtuale) di riferimento senza bisogno di forza coercitiva esterna (sulle quali v. *infra* par. 2.1) – avrebbero potuto far sì che lo stesso risolvesse la gran parte dei conflitti di legge e giurisdizione sorti all'interno della rete[62], superando così il tradizionale metodo delle norme di conflitto. Anche questo, tuttavia, avrebbe dovuto presupporre un riconoscimento della «*Lex Informatica*» e dei suoi meccanismi da parte dei regolatori pubblici.

2.2.2 Gli avversari della *Lex Informatica* nella dottrina statunitense

Come anticipato, ai fautori della teoria della *Lex Informatica* si è sin da subito contrapposta, nella dottrina[63] statunitense, un'opposta corrente di pensiero per la quale, essenzialmente, le novità conseguenti allo sviluppo di internet

[62] J.R. REIDENBERG, *op. cit*, p. 577ss.
[63] V. in particolare: J.L. GOLDSMITH-T. WU, *op. cit.* sub Cap. 1, n. 46; J.L. GOLDSMITH, *op. cit.* sub Cap. 1, n. 47.

non sarebbero state tali da portare al riconoscimento di un'autoregolamentazione esclusiva del ciberspazio né all'accantonamento del diritto internazionale privato[64] per la risoluzione dei conflitti di legge e giurisdizione sorti nell'ambito dello stesso.

La dottrina in questione riteneva, in particolare, che i problemi creati dalla rete non fossero di molto dissimili rispetto a quelli creati da altri strumenti di comunicazione – quali la radio o la televisione – o da altri fenomeni, come l'inquinamento ambientale, in grado di produrre nello stesso momento effetti in più di uno Stato. La stessa dottrina contestava inoltre la tesi per cui internet costituisse uno spazio totalmente immateriale. Al contrario, studiosi come Goldsmith hanno a più riprese[65] rilevato come per accedere alla rete ed ivi compiere azioni giuridicamente rilevanti fosse necessaria la presenza di infrastrutture tecnologiche – computer, dispositivi mobili, *data center* – localizzabili sul territorio fisico. Gli stessi hanno inoltre sostenuto come le azioni compiute nel ciberspazio producessero in realtà sempre degli effetti nel mondo reale, se non altro nella misura in cui queste fossero compiute (o subite) da soggetti fisicamente presenti nel mondo reale.

Dai rilievi di cui sopra, la dottrina in commento ha ricavato una duplice conseguenza. In primo luogo, quella per cui i regolatori pubblici sarebbero stati pienamente legittimati a disciplinare le attività svolte sulla rete. Le caratteristiche del ciberspazio avrebbero, infatti, al più dato luogo a delle oggettive difficoltà in termini di applicazione ed effettività delle loro normative, tenuto

---

[64] Trattandosi, quanto meno agli albori, di un dibattito interno alla dottrina statunitense, lo stesso riguarda in particolare i conflitti di legge tra i vari Stati federali degli Stati Uniti, oltre che quelli tra Stati indipendenti, disciplinati dal diritto internazionale privato. Nel dibattito si affacciano in maniera decisa concetti tipici della dottrina nordamericana, quale la già citata «*comity*» o il «*choice-of-law*» inteso come metodo di risoluzione dei conflitti di legge tra Stati federali. V. in questo senso J.L. GOLDSMITH, *op. cit.* Cap. 1, n. 47.

[65] V.: J.L. GOLDSMITH, *op. cit.* Cap. 1, n. 47, p. 21; J.L. GOLDSMITH-T. WU, *op. cit.* Cap. 1, n. 46, pp. 156-161.

anche conto dei rischi di applicazione extraterritoriale, comunque non dissimili a quelli riscontrati in altri ambiti del diritto[66].

A questo proposito, Goldsmith aveva fatto leva sulla distinzione tra «*prescriptive jurisdiction*» e «*enforcement jurisdiction*», che indicano, rispettivamente, il potere di uno Stato di disciplinare una determinata attività con delle proprie norme e la capacità di garantirne la concreta applicazione grazie all'attività dell'autorità giudiziaria e delle forze dell'ordine[67]. La distinzione è rilevante in quanto, a parere dello stesso Goldsmith, le caratteristiche del ciberspazio non avrebbero fatto venire meno la legittimità delle aspirazioni dei regolatori pubblici a disciplinare le attività che si svolgono sulla rete con delle proprie regole ma avrebbero soltanto reso più difficoltosa l'applicazione pratica di queste ultime.

Per risolvere le anzidette difficoltà, l'autore aveva fatto leva innanzi tutto sulla nozione di «*indirect regulation of extraterritorial activity*[68]», che indica la capacità degli Stati di influenzare le attività effettuate al di fuori del proprio territorio attraverso la regolamentazione delle infrastrutture (*hardware* e *software* nel caso della rete) o degli intermediari presenti sullo stesso, vale a dire gli *internet service provider*. Centrale nel ragionamento di Goldsmith erano inoltre l'utilizzo di tecnologie di geolocalizzazione o di «*content-filtering*[69]» – che già all'epoca iniziavano ad affacciarsi sul mercato – o l'imposizione di sanzioni

---

[66] Oltre al già menzionato diritto ambientale, Goldsmith nei suoi scritti fa riferimento anche ad ambiti come il diritto tributario o il diritto societario, in cui non è raro assistere a trasferimenti di sede volti esclusivamente ad evitare l'applicazione di una determinata normativa. Ancora, l'autore fa riferimento all'esperienza di Radio Free Europe, radio le cui trasmissioni, all'epoca della Guerra Fredda, venivano diffuse nell'Unione Sovietica senza che la stessa avesse alcune sede nel paese. Vedi: J.L. GOLDSMITH, *op. cit*. Cap. 1, n. 47.

[67] V. in particolare: J.L. GOLDSMITH, *The Internet, Conflicts of Regulation, and International Harmonization*, in C. ENGEL, K.H. KELLER (a cura di), *Governance of Global Networks in the Light of Differing Local Values*, pp. 197-207, Nomos Verlagsges, 2000. Si veda anche P.S. BERMAN, *op. cit.* n. 47, p. 401.

[68] J.L. GOLDSMITH, *op. cit.* Cap. 1, n. 47, p. 18.

[69] Idem.

elevate[70], volte ad incrementare i costi connessi alla violazione di norme relative ad internet. Finalità, quest'ultima, che richiama alla mente la già menzionata funzione di «*market destroying measure*» assunto dalle sanzioni pecuniarie nel mondo digitale (v. *supra*: Cap. 1, par 5; *infra*, par. 3.2.3).

Dall'assunto per cui il ciberspazio non costituisse uno spazio totalmente immateriale, Goldsmith ricavava inoltre la conseguenza per cui il diritto internazionale privato potesse essere utilizzato come strumento di risoluzione dei conflitti di legge anche nell'ambito dello stesso[71]. Peraltro, riconoscendo le oggettive difficoltà comunque esistenti, l'autore aveva proposto alcuni correttivi, auspicando anche una forma di armonizzazione a livello sovranazionale[72]. In particolare, l'autore sosteneva la valorizzazione di criteri di collegamento con ancoraggi territoriali facilmente individuabili, quali quello del domicilio (sul punto v. *supra*: Cap. 3, par. 2.2), invece che quelli difficilmente utilizzabili nel ciberspazio, come il luogo dell'evento dannoso[73].

Dal punto di vista metodologico, Goldsmith sosteneva inoltre l'opportunità di risolvere i conflitti di legge e di giurisdizione non attraverso le tradizionali norme di conflitto di impostazione multilateralista ma facendo proprio l'approccio unilateralista[74]. In particolare, a parere dell'autore l'utilizzo di norme di matrice unilateralista – che, come abbiamo visto, sono tipiche della rete (v. *supra*: Cap. 3 par. 5) – permetterebbe di determinare quando una fattispecie abbia o meno un collegamento stretto con un ordinamento giuridico tale da

[70] Idem, p. 31. Vedi anche J.L. GOLDSMITH, *op. cit.* n. 67, p. 201.
[71] Vedi *ex multis*: J.L. GOLDSMITH, Cap. 1, n. 47; J.L. GOLDSMITH-T. WU, *op. cit*. Cap. 1, n. 46. Si veda inoltre: J.L. GOLDSMITH, *The Internet and the Abiding Significance of Territorial Sovereignty*, in Indiana Journal of Global Legal Studies, Vol. 5, n. 2, pp. 475-491, 1998.
[72] Vedi in particolare: J.L. GOLDSMITH, *op. cit.* Cap. 1, n. 46, p. 24.
[73] Idem, p. 29.
[74] Idem, p. 29.

ricadere sotto l'ambito di applicazione del diritto di questi. In caso di collegamento non abbastanza stretto, infatti, la fattispecie non rientrerebbe nella «gittata» della norma unilateralista, con ciò escludendone l'applicazione. L'utilizzo di una norma unilateralista permetterebbe, quindi, ad un giudice di stabilire direttamente, senza bisogno delle norme di conflitto in senso tradizionali, se la stessa legge si applichi o meno alla fattispecie considerata.

…*Segue*: e quelli nella dottrina e nella giurisprudenza dell'Unione europea

La teoria della *Lex Informatica* in grado di soppiantare la regolamentazione di fonte pubblica all'interno del ciberspazio ha trovato degli avversari anche nella dottrina internazionalprivatista europea, nonché nella giurisprudenza della Corte di Giustizia dell'Unione. Queste ultime, come abbiamo già avuto modo di segnalare (v. *supra*: Cap. 3, par. 1.2), sono infatti tradizionalmente restie al riconoscimento di norme di fonte diversa da quella pubblica, motivo per cui anche la menzionata teoria ha avuto poco seguito del vecchio continente.

Si è già visto, del resto, come sin dall'emersione di internet la Corte di Giustizia non abbia mai preso in reale considerazione l'idea di una *Lex Informatica* ma si sia piuttosto concentrata sull'adattare – talvolta creandone di nuovi o estendendo in maniera considerevole quelli esistenti – i criteri di collegamento previsti dal diritto internazionale privato dell'Unione allo scopo di risolvere i conflitti di legge e di giurisdizione sorti all'interno dello spazio virtuale. In altre parole, il dibattito all'interno dell'ordinamento dell'Unione ha presto abbandonato la domanda «*Does State Law Apply?*» spostandosi su quella «*Which State Law Applies?*[75]».

[75] T. LUTZI, *op. cit.* Cap. 1, n. 37 p. 130.

La richiamata impostazione è peraltro rimasta maggioritaria[76] nella dottrina dell'Unione, anche a seguito della comparsa sulla scena delle piattaforme digitali e dello sviluppo del web 2.0. Tuttavia, ciò non ha impedito, come si è già potuto saggiare (v. *supra* Cap. 3, par. 5) e si vedrà meglio in seguito (v. *infra*, par. 3), la teorizzazione di nuovi paradigmi fondati sul metodo unilateralista per quanto riguarda il diritto internazionale privato e volti a valorizzare, seppur indirettamente, il potere regolatorio delle piattaforme sotto il profilo del diritto materiale.

2.2.3 La ricerca di soluzioni mediane che valorizzino l'autoregolamentazione della rete

Come anticipato, tra le due antitetiche correnti poc'anzi esaminate vi sono stati, nella dottrina statunitense, alcuni studiosi che hanno provato a teorizzare delle soluzioni mediane che, allo stesso tempo, valorizzassero la spinta all'autoregolamentazione di internet e consentissero ai regolatori pubblici di esercitare il proprio potere (o quanto meno la propria influenza) anche all'interno dello spazio virtuale. Le soluzioni proposte si fondavano, in particolare, sull'idea per cui l'autoregolamentazione del ciberspazio, a prescindere dal proprio inquadramento dogmatico, potesse costituire un valido supporto per i regolatori pubblici per riuscire ad applicare le proprie norme sulla rete[77].

Tra i fautori di queste soluzioni vi era innanzi tutto Reidenberg, per il quale i regolatori pubblici avrebbero dovuto ricorrere alla *Lex Informatica* se avessero voluto raggiungere determinati obiettivi che sarebbero stati invece a rischio nel caso in cui si fossero limitati a disciplinare le fattispecie del mondo digitale

---

[76] Idem. Oltre a T. LUTZI si vedano inoltre: I. PRETELLI, *op. cit.* Cap. 1, n. 11; M. LEHMANN, *Who Owns Bitcoin? Private Law Facing the Blockchain,* EBI Working Paper Series, n. 42, 2019. In senso favorevole ad un riconoscimento delle regole delle piattaforme quale «diritto applicabile» ai sensi del diritto internazionale privato si veda invece: F. BASSAN, *op. cit.* n. 3, p. 112.

[77] Vedi in particolare: J.R. REIDENBERG, *op. cit.* p. 586; L. LESSIG, *op. cit.* (versione 2.0) Cap. 1, n. 32, p. 301ss.

utilizzando i tradizionali strumenti legislativi. Il ricorso alla *Lex Informatica* avrebbe, infatti, consentito ai regolatori pubblici di controllare in maniera relativamente agevole il flusso di informazioni sulla rete, contribuendo all'effettività delle norme di fonte pubblica grazie alle sue caratteristiche distintive già esaminate (v. *supra* par. 2.1).

Per far sì che ciò accedesse, nell'idea dello studioso sarebbe stato necessario un cambio di paradigma. In particolare, i regolatori pubblici avrebbero dovuto entrare nell'ottica non di regolare direttamente le attività svolte sulla rete ma di influenzarle indirettamente, mantenendo per sé un ruolo di supervisione. Le strade per giungere a questo cambio avrebbero dovuto essere la promozione e l'incentivo all'adozione di standard tecnici da inglobare nella *Lex Informatica* per garantire la rispondenza di questa agli obiettivi politici dei regolatori privati. Reidenberg aveva inoltre illustrato alcuni possibili modi attraverso cui i regolatori pubblici avrebbero potuto, concretamente, esercitare la propria influenza[78]. Tra questi rientrano, in particolare, il c.d. «*bully-pulpit approach*[79]», la partecipazione dei regolatori pubblici ai lavori delle organizzazioni in cui vengono sviluppati gli standard tecnici, la destinazione di fondi pubblici allo sviluppo di determinate tecnologie, la previsione di standard tecnici come requisiti per partecipare alle gare di appalti pubblici e la regolamentazione diretta di standard tecnici. Nell'idea dello studioso, sempre più importante sarebbe dovuto diventare il ruolo ricoperto da organizzazioni come le già citate Iso o 3WC (v. *infra* par. 1.3.1 e 2.1) nel processo di definizione di standard tecnici funzionali al raggiungimento degli obiettivi dei regolatori pubblici.

---

[78] Si veda in particolare: J.R. REIDENBERG, *op. cit.* p. 588.

[79] L'espressione «*bully-pulpit*» risale a Theodore Roosevelt e indica il potere di un'autorità pubblica di portare avanti le proprie istanze grazie al prestigio e alla notorietà garantita dalla carica stessa. Per approfondire anche da un punto di vista storico v. *ex multis*: B.J. WETZEL, *Theodore Roosevelt: Preaching from the Bully Pulpit*, Oxford University Press, 2021.

Su posizioni simili si era attestato anche Lessig, tra i primi studiosi ad occuparsi del tema della regolamentazione indiretta delle condotte che avvengono nel ciberspazio attraverso la regolamentazione delle tecnologie alla base di internet[80]. Secondo Lessig, inoltre, le stesse tecnologie avrebbero dovuto rappresentare uno strumento utile per determinare, in concreto, se una fattispecie (o persona) ricadesse nell'ambito di applicazione di una determinata norma, con ciò, almeno implicitamente, avallando l'utilizzo del metodo unilateralista nell'ambito della rete. Questo grazie a tecniche come il «*content filtering*» o la geolocalizzazione che si sarebbero poi sviluppate in maniera decisa nei decenni successivi e che già all'epoca venivano individuate da Lessig come un importante mezzo per favorire la collaborazione tra regolatori pubblici e privati nell'ambito della rete. Da segnalare, peraltro, come lo stesso studioso avesse, già all'epoca, evidenziato i rischi in termini di trasparenza e di legittimazione democratica di un approccio basato prevalentemente sulla regolamentazione indiretta delle attività dei privati.

3 Il riconoscimento della dimensione istituzionale delle piattaforme da parte del legislatore dell'Unione ed il suo tentativo di controllarla

Analizzati gli aspetti teorici principali relativi alla *private regulation* ed alle sue declinazioni in ambito transnazionale e nel ciberspazio, ci soffermiamo adesso sull'atteggiamento tenuto dal legislatore dell'Unione europea nei confronti del fenomeno auto-regolatorio della rete e, nello specifico, delle piattaforme digitali[81]. Si tenterà, in particolare, di dimostrare come il legislatore dell'Unione, pur non avallando le teorie radicali proposte da Johnson e Post negli Stati Uniti, abbia a più riprese riconosciuto tali fenomeni, tentando di

[80] L. LESSIG, *op. cit.* Cap. 1, n. 32. Vedi in particolare, della Versione 2.0: pp 61-82, 83-119, 120-137, 281-293, 294-312.
[81] Per un approfondimento sul tema si veda anche F. BASSAN, *op. cit*, n. 3, p. 9ss.

controllarli e di orientarli al rispetto delle proprie regole e al raggiungimento dei propri obiettivi, confermando in una certa misura le idee di Reidenberg e Lessig sulla regolamentazione indiretta della rete.

3.1 Le strategie regolatorie delineate dalla Commissione europea

Si è già avuto modo di rilevare (v. *supra* Cap. 2, par. 3) come, nel solco della Digital Single Market Strategy, la Commissione europea abbia intrapreso una strategia regolatoria basata anche sulla valorizzazione della «dimensione istituzionale» delle piattaforme – e quindi del loro potere regolatorio – e dei concetti di «trasparenza» e «*accountability*». Nell'ambito di questa strategia, importanza centrale riveste la già citata Comunicazione[82] del 2016 sulle piattaforme online e il mercato unico digitale, nella quale l'Esecutivo dell'Unione ha tratteggiato tre possibili modalità attraverso cui regolare le piattaforme digitali, i cui relativi vantaggi e svantaggi sono stati oggetto di diversi commenti dottrinali[83].

3.1.1 La prima opzione: la tradizionale «*top-down regulation*»

La prima delle opzioni regolatorie considerate dalla Commissione europea è costituita dalla tradizionale regolamentazione di fonte pubblica, volta a disciplinare le attività delle piattaforme digitali attraverso strumenti normativi aventi forza di legge e il cui rispetto è garantito dalla previsione di sanzioni. In questo senso, la menzionata tecnica è stata definita «*top-down regulation*» dalla dottrina[84].

A questo proposito, la Commissione europea ha individuato alcuni caratteri essenziali che dovrebbero essere propri di un'efficace regolamentazione di

[82] COM(2016) 288 final, *cit.* Cap. 2, n. 7.
[83] Vedi in particolare: M. CANTERO GAMITO, *op. cit.* Cap. 1, n. 19; C. BUSCH, *op. cit.* Cap. 1, n. 19,; M. FINCK, *op. cit.* Cap. 2, n. 46; C. BUSCH, *op. cit.* Cap. 2, n. 63.
[84] M. FINCK, *op. cit.* Cap. 2, n. 46.

fonte pubblica delle piattaforme. In particolare, tanto l'Esecutivo quanto i commentatori in dottrina[85] hanno posto enfasi sull'importanza di norme semplici, chiare, prevedibili ed omogenee per tutti gli Stati membri, segnalando quindi la necessità di interventi a livello di Unione. Allo stesso modo, la Commissione ha sottolineato il carattere fondamentale dell'effettività delle norme in materia di piattaforme digitali, anche alla luce della dimensione transnazionale di queste ultime, evidenziando, a tal fine, l'importanza della cooperazione tra le diverse autorità nazionali o eurounitarie competenti, come nel caso di strumenti come il GDPR. A livello sostanziale, la citata Comunicazione ha promosso un approccio improntato al principio della «*better regulation*» (v. *supra* par. 1.3.1) e teso ad individuare e disciplinare soltanto «problemi chiaramente circoscritti relativi a un tipo specifico di piattaforme online o a un'attività che queste svolgono». In altre parole, si identificano e si valutano con precisione gli ambiti di intervento dei legislatori dell'Unione, allo scopo di garantire la certezza e l'uniformità del diritto, oltre che una sua maggiore effettività.

Si è già a più riprese rilevato come il tradizionale approccio «*top-down*» alla regolamentazione delle piattaforme digitali presenti delle problematiche sia da un punto di vista di diritto materiale che nella prospettiva internazionalprivatista. Inoltre, occorre segnalare come, a seguito della Comunicazione, vi sia stato in dottrina[86] chi, dopo aver ricordato le richiamate criticità, abbia portato degli argomenti a sostegno della tesi per cui il solo ricorso alla regolamentazione di fonte pubblica non costituisca garanzia di trasparenza e di rispetto dei principi democratici, sollevando ulteriori perplessità in merito all'opportunità di utilizzare soltanto la suddetta tecnica per regolare le piattaforme digitali.

[85] Idem, p. 6.
[86] Idem, p. 7.

3.1.2 La promozione di sistemi di autoregolamentazione

Come accennato, nella Comunicazione in commento la Commissione europea ha affermato come, accanto alla tradizionale «*top-down regulation*», possano svolgere un ruolo importante altre due tecniche regolatorie, rappresentate dagli strumenti autoregolamentazione e di coregolamentazione[87]. Nell'idea dell'Esecutivo, peraltro, entrambe dovrebbero fondarsi su principi comuni di riferimento, tra cui vengono menzionati gli «strumenti del settore[88]» – formula assimilabile alle *best practice* o ad altri standard o codici di condotta di fonte privata – idonei a garantire l'applicazione e il rispetto dei requisiti di legge, presidiati da «adeguati meccanismi di monitoraggio». Espressione, quest'ultima, che segnala la preoccupazione dell'Esecutivo nei confronti dell'effettività dei suddetti strumenti.

Cominciando dall'autoregolamentazione, abbiamo già avuto modo di vedere come con essa gli studiosi della «*private regulation*» siano soliti indicare la forma più tipica di quest'ultima, connotata dalla tendenziale coincidenza tra regolatori e regolati (v. *infra* par. 1.1). A tal proposito, è utile richiamare la definizione fornita dalle tre principali istituzioni dell'Unione europea nel Progetto interistituzionale[89] «Legiferare meglio» del 2003, a mente della quale con

---

[87] Per approfondire i concetti si vedano *ex multis*: L. SENDEN, E. KICA, M. HIEMSTRA, K. KLINGER, *Mapping Self- and Co-regulation Approaches in the EU Context. Explorative Study for the European Commission, DG Connect*, Commissione Europea, 2015; M.E. BARTOLINI, *La regolamentazione privata nel sistema costituzionale dell'Unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione tecnologica*, in Osservatorio sulle fonti, fasc. 3, pp. 1331-1355, Disponibile in: http://www.osservatoriosullefonti.it

[88] COM(2016) 288 final, *cit.* Cap. 2, n. 7, p. 6. L'espressione è presente nella versione italiana della comunicazione ed è una traduzione dall'inglese «*industry tools*».

[89] *Progetto interistituzionale — "Legiferare meglio"*, apparso sulla Gazzetta Ufficiale dell'Unione europea GU C 321 del 31.12.2003, pagg. 1–5. Il progetto è stato poi abrogato e sostituito dall'Accordo interistituzionale «Legiferare meglio» tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea, apparso sulla Gazzetta Ufficiale dell'Unione europea GU L 123 del 12.5.2016, pagg. 1-14.

«autoregolamentazione» si intende «la possibilità lasciata agli operatori economici, alle parti sociali, alle organizzazioni non governative o alle associazioni, di adottare tra di loro e per sé stessi orientamenti comuni a livello europeo». Sulla base di questa definizione, pertanto, l'autoregolamentazione costituisce uno strumento di disciplina volontario, privo di effetti giuridici, distinto e separato dai meccanismi di regolamentazione pubblica[90].

Analogamente, abbiamo già potuto constatare come i gestori delle piattaforme digitali esercitino, nel proprio ambito di riferimento, poteri regolatori cui sono sottoposti sia essi stessi che gli utenti delle loro *community* (v. *supra* Cap. 1, par. 2.2). In questo senso, pertanto, l'autoregolamentazione cui fa riferimento la Comunicazione del 2016 va intesa come una delle già citate forme moderne di «*private regulation*», volte a disciplinare anche i comportamenti di soggetti diversi dai regolatori (gli utenti) che decidono volontariamente di esservi sottoposti[91].

La dottrina[92] favorevole all'autoregolamentazione delle piattaforme ha indicato tra i vantaggi della stessa alcune delle caratteristiche già evidenziate nel presente lavoro (v. *supra*: Cap. 1, par. 2.1, 5). In particolare, sono state richiamate la capacità dei gestori delle piattaforme di stabilire regole facilmente adattabili alle diverse aree geografiche con cui queste vengono in contatto grazie all'utilizzo di algoritmi e tecnologie di geolocalizzazione (v. *supra*: par. 2.2.3). Analogamente, è stata evidenziata la possibilità, per le piattaforme, di definire standard minimi in materie come il diritto del lavoro, applicabili anche in giurisdizioni in cui simili standard non sono presenti (v. *supra*: par. 1.2).

[90] M.E. BARTOLINI, *op. cit.* n. 87, p. 1345.
[91] M. FINCK, *op. cit.* Cap. 2, n. 46, p. 9.
[92] Idem, p. 12ss per una ricapitolazione generale delle diverse posizioni dottrinali.

Gli argomenti principali a sostegno dell'autoregolamentazione sono, peraltro, rappresentati da fattori come l'asimmetria informativa esistente tra regolatori pubblici e gestori delle piattaforme, i quali sarebbero i soli in possesso dei dati e delle informazioni necessarie per disciplinare in maniera efficace quanto avviene nell'ambito degli ambienti virtuali. A ciò si aggiunge la circostanza, a più riprese già evocata (v. *supra* par. 2.1; Cap. 1, par. 5; Cap. 3, par. 1.2), per cui le norme stabilite dai gestori delle piattaforme avrebbero un carattere auto-esecutivo («*self-enforcing*»), in quanto non necessiterebbero di azioni coercitive esterne per poter essere applicate. In definitiva, in base ai predetti argomenti i gestori delle piattaforme si troverebbero in una posizione migliore rispetto agli ordinamenti giuridici tradizionali per esercitare funzioni regolatorie e para-giurisdizionali all'interno dei propri ambienti.

Ai menzionati vantaggi sono stati contrapposti in dottrina[93] diversi aspetti negativi connessi all'utilizzo dell'autoregolamentazione. Le tesi contrarie hanno in primo luogo fatto leva sui rischi in termini di trasparenza delle attività dei regolatori privati, aspetto su cui, come già visto, il legislatore dell'Unione europea ha posto particolare attenzione nei suoi recenti interventi in materia di piattaforme digitali (v. *supra*: Cap. 2, par. 2.3 3; v. anche *infra*: par. 3.2.3; Cap. 4, par. 4.1, 4.3.2). Altre critiche si sono basate sull'ipotesi per cui i gestori delle piattaforme non sarebbero, in realtà, nella posizione più adatta per esercitare da soli le funzioni regolatorie in quanto, pur essendo in possesso di un grandissimo numero di informazioni relative ai propri ambienti, non sarebbero portatori di interessi generali ma soltanto di interessi particolari, che potrebbero anche non coincidere con quelli della collettività. Né a questo sembrerebbero in grado di supplire i meccanismi di valutazione e rating stabiliti

[93] Idem.

all'interno delle piattaforme, sulla trasparenza dei quali sono stati espressi ulteriori dubbi in dottrina[94].

Infine, sono stati sottolineati alcuni rischi in termini di certezza del diritto derivanti dall'autoregolamentazione effettuata in assenza di standard comuni per i regolatori (v. *infra*: par. 1.3.1), oltre che di violazione delle norme dell'Unione europea in materia di concorrenza. Più in generale, si può affermare come il minimo comune denominatore delle critiche nei confronti dell'utilizzo dell'autoregolamentazione sia costituito dalla preoccupazione di evitare di conferire ai gestori delle piattaforme un potere regolatorio troppo esteso. Un rischio che era già stato rilevato dai primi commentatori della dottrina statunitense a cavallo tra gli anni '90-2000 (v. *infra*: par. 2.1) e che, se concretizzato, avrebbe delle notevoli ricadute in diversi ambiti del diritto, come ad esempio i diritti della personalità, la concorrenza, la proprietà intellettuale o la libertà di espressione. Tematiche, queste ultime, al centro dei recenti interventi del legislatore dell'Unione in materia di piattaforme digitali.

3.1.3 La coregolamentazione: una soluzione mediana

L'ultima opzione proposta dalla Commissione europea è rappresentata, come detto, dalla «coregolamentazione». Per un inquadramento della nozione è utile anche in questo caso fare riferimento alla definizione[95] fornita dal Progetto interistituzionale del 2003, in base a cui, per coregolamentazione, si intende «il meccanismo mediante il quale un atto legislativo dell'Unione conferisce la realizzazione degli obiettivi definiti dall'autorità legislativa ai soggetti interessati riconosciuti in un determinato settore». Si tratta – sempre secondo

---

[94] Idem, p. 15. Sul tema delle recensioni false, molto discusso anche a livello politico-giornalistico, si vedano i recenti casi di cronaca giudiziale italiana: *Amazon, prima causa penale contro le recensioni false*, articolo apparso su www.ansa.it il 21 ottobre 2022 e consultabile online: https://www.ansa.it/sito/notizie/postit/Amazon/2022/10/20/amazon-prima-causa-penale-contro-le-recensioni-false_e7bbc95f-4663-4318-8b35-11ba6c7b4a58.html

[95] *Progetto interistituzionale – "Legiferare meglio"*, *cit.* n. 89.

la suddetta definizione – di un meccanismo a cui si può far ricorso «sulla base di criteri definiti nell'atto legislativo per assicurare che la legislazione sia adeguata ai problemi e ai settori interessati, alleggerire il lavoro legislativo concentrandolo sugli aspetti essenziali e beneficiare dell'esperienza dei soggetti interessati».

La coregolamentazione rappresenta, nella sostanza, un'opzione mediana tra la tradizionale «*top-down regulation*» e l'autoregolamentazione. In essa, infatti, il legislatore pubblico definisce i principi e gli obiettivi fondamentali in un determinato ambito, demandando la relativa regolamentazione ad attori privati specificamente individuati che presentino le caratteristiche e le competenze necessarie. Ciò non vale, peraltro, a conferire al privato una delega in bianco, in quanto il regolatore pubblico conserva il compito di supervisione delle attività del primo, allo scopo di garantire il rispetto dei principi e degli obiettivi da esso stabiliti. In questo senso, quindi, il meccanismo appare assimilabile alla già citata «*delegation*[96]» (v. *supra* par. 1.1, 2.2.1) e ai nuovi paradigmi invocati dalla dottrina statunitense negli anni '90 (v. *supra* par. 2.2.1).

Nell'ambito della coregolamentazione la dottrina[97] ha ricondotto diverse forme di collaborazione tra soggetti pubblici e privati, finalizzate alla disciplina di determinate questioni da parte dei regolatori privati nel rispetto degli obiettivi perseguiti dal legislatore pubblico. In questo senso, il fenomeno è stato ritenuto parte di una più ampia tendenza evolutiva in cui, soprattutto a livello di Unione, si assisterebbe ad un passaggio graduale da forme tradizionali di «*top-down regulation*» a procedure decisionali ed applicative più condivise, partecipate anche da soggetti privati. A questa tendenza sarebbe da ascrivere anche il già visto fenomeno della c.d. «*better regulation*» (v. *supra*: par.

[96] In questo senso anche M.E. BARTOLINI, *op. cit.* n. 87, p. 1347.
[97] M. FINCK, *op. cit.* Cap. 2, n. 46, p. 15ss.

1.3.1), a cui la Commissione europea ha dedicato una specifica comunicazione[98].

Per le sue caratteristiche la coregolamentazione è stata considerata da parte della dottrina[99] come l'opzione regolatoria preferibile. Essa, infatti, consentirebbe di sfruttare i vantaggi dell'autoregolamentazione delle piattaforme – in particolare, la posizione privilegiata dei loro gestori in termini di informazioni, l'agevole adattabilità delle regole da questi stabilite e la loro diretta applicabilità senza bisogno di forze coercitive esterne – conciliandoli con il rispetto degli interessi generali e con gli obiettivi stabiliti dai regolatori pubblici. A tal fine, peraltro, la dottrina in commento ha indicato come necessari sia il monitoraggio dei regolatori pubblici che l'esistenza di un sistema di norme di fonte pubblica da utilizzare in caso di fallimento dei meccanismi di (co)regolamentazione privata, anche allo scopo di incentivare la collaborazione dei privati stessi all'attività regolatoria. In questo senso, pertanto, la dottrina in commento ha chiarito come la coregolamentazione non possa essere considerata come una forma di deregolamentazione – né di delega in bianco ai privati – visto il continuo coinvolgimento dei soggetti pubblici nel processo regolatorio, seppur con ruoli diversi da quelli tipici.

3.2 La dimensione istituzionale delle piattaforme nel diritto dell'Unione

Esaminate le strategie regolatorie delineate dalla Commissione europea, si passano adesso brevemente in rassegna alcuni degli strumenti normativi in materia di nuove tecnologie e piattaforme digitali adottati negli anni recenti dal legislatore dell'Unione, diversi dei quali già esaminati o citati altrove nel presente lavoro (v. *supra* Cap. 1, par. 5; Cap. 2, par. 2.3, 3.1; v. *infra*, Cap. 6, par. 4). Dagli stessi, in particolare, emergono alcuni tratti comuni che segnalano

[98] COM(2015) 215 final, cit. n. 32

[99] V. in particolare: M. FINCK, *op. cit.* Cap. 2, n. 46, p. 15ss; C. BUSCH, *op. cit.* Cap. 1, n. 19, p. 17.

come il legislatore paia effettivamente aver intrapreso una strada fondata sul riconoscimento di una «dimensione istituzionale» delle piattaforme (e di altri protagonisti della rete) e sul tentativo di controllarla, orientando l'attività (anche in senso lato) regolatoria dei gestori delle stesse al rispetto dei principi e al perseguimento degli obiettivi da esso stabiliti, se dal caso ricorrendo a meccanismi di autoregolamentazione o di coregolamentazione[100].

3.2.1 Il sostegno istituzionale all'adozione di codici di condotta e di regole coerenti con il diritto dell'Unione

Nell'ambito della disciplina delle nuove tecnologie, uno degli strumenti con cui il legislatore dell'Unione ha, soprattutto in epoca recente, tentato di valorizzare ed orientare il potere regolatorio dei privati – ed in particolare dei gestori delle piattaforme digitali – è il sostegno all'adozione di norme coerenti con il diritto dell'Unione.

In particolare, sempre più di frequente il legislatore dell'Unione ha fatto ricorso a tecniche basate sulla «presa d'atto[101]» del potere regolatorio di alcuni soggetti privati e sull'incentivo all'adozione, da parte di questi ultimi, di strumenti normativi, come codici di condotta, che rispecchino i principi e gli obiet-

[100] Non è qui possibile soffermarsi nel dettaglio sull'ampio e stimolante dibattito relativo alla compatibilità degli strumenti di autoregolamentazione e coregolamentazione, in particolare nella forma della delega a soggetti privati da parte delle istituzioni dell'Unione, con i trattati dell'Unione europea. Per approfondimenti si rimanda *ex multis* a: M.E. BARTOLINI, *op. cit.* n. 87; L. SENDEN, E. KICA, M. HIEMSTRA, K. KLINGER, *op. cit.* n. 87. La prima, in particolare, afferma come «pur nel silenzio dei Trattati, una dimensione regolatoria "alternativa" o "complementare" a quella accentrata e pubblica può essere ammessa e considerata compatibile con l'ordinamento costituzionale dell'Unione soltanto nell'ambito del sistema di delega dei poteri», facendo in precedenza riferimento all'art. 291 TFUE. Nell'ambito della giurisprudenza della Corte di Giustizia si richiamano: CGUE, causa 10-56, *Meroni & Co., Industrie Metallurgiche, società in accomandita semplice* c. *Alta Autorità della Comunità europea del Carbone e dell'Acciaio*, 13 giugno 1958 – ECLI:EU:C:1958:8; CGUE, causa C-613/14, *James Elliott Construction Limited* c. *Irish Asphalt Limited*, 27 ottobre 2016 – ECLI:EU:C:2016:821.

[101] M.E. BARTOLINI, *op. cit.* n. 87, p. 1349.

tivi stabiliti dallo stesso legislatore. Val la pena precisare come, in questo contesto, si usano espressioni come «incentivare» o «promuovere» in quanto la menzionata tecnica si contraddistingue per il fatto che il regolatore pubblico di regola non interviene nei processi di definizione e approvazione degli strumenti normativi da parte dei privati, o comunque vi partecipa soltanto con ruoli di indirizzo.

Un esempio, invero piuttosto risalente, dell'uso di questa tecnica si può ritrovare nella Decisione 854/2005/CE, che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie online[102]. In questo strumento, in particolare, è stato definito il ruolo del forum Safer Internet – a sua volta istituito nel 2004 nel quadro del piano d'azione per l'uso sicuro di Internet[103] – quale piattaforma di discussione in cui riunire gli *stakeholder* coinvolti (rappresentanti dell'industria, autorità nazionali competenti, politici, associazioni di categoria, organizzazioni di utenti) anche allo scopo di promuovere iniziative di coregolamentazione e di autoregolamentazione. Tra gli obiettivi del forum vi sono, ad esempio, favorire il raggiungimento del consenso e l'autoregolamentazione in merito a determinate materie[104], nonché incoraggiare gli *internet service provider* «ad elaborare codici di condotta su questioni quali la gestione delle procedure di notifica e rimozione in modo trasparente e responsabile[105]», oltre che ad «informare gli

[102] Decisione n. 854/2005/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, che istituisce un programma dell'Unione pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie online (Testo rilevante ai fini del SEE), apparsa in *GU L 149 dell'11 giugno 2005, pagg. 1–13*.

[103] Decisione n. 854/2005/CE, *Azione 3: promozione di un ambiente più sicuro*.

[104] Idem, v. in particolare il seguente passaggio: «Il forum Safer Internet avrà i seguenti obiettivi specifici: […] 2) Favorire la formazione del consenso e l'autoregolamentazione in merito a problematiche quali la certificazione di qualità dei siti web, la classificazione dei contenuti intermediali, la classificazione e i sistemi di filtraggio, estendendoli a nuovi tipi di contenuti quali i giochi online e a nuovi tipi di accesso quali la telefonia mobile […]».

[105] Idem, punto 3).

utenti su un uso più sicuro di Internet e l'esistenza di "*hotline*" per segnalare contenuti illegali». La decisione in commento, peraltro, si limita ad istituire e promuovere uno spazio per lo sviluppo dell'autoregolamentazione privata, senza incidere sullo svolgimento di essa. In questo senso, quindi, il legislatore incoraggia le attività autoregolatorie con un intervento meramente prodromico ad esse, le quali rimangono nella piena disponibilità dei privati[106].

Un esempio più recente di tale approccio si trova nel Regolamento (UE) 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea[107]. In questo regolamento, in particolare, sin dal considerando 1 viene sottolineata l'importanza di «codici di autoregolamentazione e altre migliori prassi[108]» per la disciplina dei dati non personali. Il successivo art. 6 conferisce alla Commissione il compito di incoraggiare e facilitare l'adozione di tali codici di condotta «al fine di contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità». Lo stesso articolo, inoltre, indica espressamente alcuni aspetti[109] da tenere

---

[106] M.E. BARTOLINI, *op. cit.* n. 87, p. 1350.

[107] 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 (Testo rilevante ai fini del SEE), apparso in *GU L 303 del 28.11.2018, pagg. 59–68*.

[108] «[…] il rapido sviluppo dell'economia dei dati e di tecnologie emergenti come l'intelligenza artificiale, i prodotti e i servizi relativi all'Interne degli oggetti, i sistemi autonomi e la tecnologia 5G sollevano nuove questioni giuridiche relative all'accesso ai dati e al loro riutilizzo, alla responsabilità, all'etica e alla solidarietà. Si dovrebbe considerare l'opportunità di lavorare in materia di responsabilità, segnatamente attraverso l'impiego di codici di autoregolamentazione e altre migliori prassi, tenendo conto delle raccomandazioni, delle decisioni e delle azioni adottate senza interazione umana lungo l'intera catena del valore del trattamento dei dati. Tali lavori potrebbero anche contemplare meccanismi appropriati per determinare la responsabilità, per trasferire la responsabilità tra servizi che cooperano, per l'assicurazione e per l'audit» (considerando 1 Regolamento (UE) 2018/1807). Si vedano inoltre i considerando 30 e 31 del medesimo regolamento.

[109] «1. La Commissione incoraggia e facilita l'elaborazione di codici di condotta di autoregolamentazione a livello dell'Unione ("codici di condotta"), al fine di contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità e nell'ambito della quale si tenga debitamente conto degli standard aperti, contemplando, tra l'altro, gli

in considerazione nell'elaborare i suddetti strumenti e stabilisce che la Commissione provveda affinché essi siano elaborati in stretta cooperazione con tutti i portatori di interesse[110]. A proposito di questi codici, va peraltro chiarito come, nonostante i menzionati requisiti – sia sostanziali che, *lato sensu*, procedurali – e i ruoli di indirizzo e monitoraggio[111] ricoperti della Commissione europea, essi non siano idonei a produrre effetti vincolanti e la loro adozione ed applicazione siano completamente rimessi alle dinamiche della prassi[112] e all'autonomia dei privati.

Come si è già visto, un esempio analogo è presente anche nel Regolamento P2B (v. *supra*: Cap. 2, par. 3.1). Si tratta, in particolare, dell'art. 17, secondo cui l'Esecutivo dell'Unione ha il compito di incoraggiare l'elaborazione di codici di condotta da parte dei fornitori delle piattaforme e delle relative organizzazioni di categoria, finalizzati a contribuire all'applicazione dello stesso Regolamento P2B. Quest'ultimo, peraltro, a differenza del Regolamento sui dati non personali, non fornisce indicazioni particolari in merito al contenuto dei

---

aspetti seguenti: a) le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati; b) gli obblighi d'informazione minimi per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate, chiare e trasparenti prima della conclusione di un contratto di trattamento di dati, per quanto riguarda le procedure e i requisiti tecnici, i tempi e gli oneri applicati nel caso in cui un utente professionale intenda cambiare fornitore di servizi o ritrasferire i dati nei propri sistemi informatici; c) gli approcci in materia di sistemi di certificazione che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali, tenendo conto delle norme consolidate a livello nazionale o internazionale che agevolano la comparabilità di tali prodotti e servizi. Tali approcci possono includere, tra l'altro, la gestione della qualità, la gestione della sicurezza delle informazioni, la gestione della continuità operativa e la gestione ambientale, d) tabelle di marcia in materia di comunicazione, con un approccio multidisciplinare volto a sensibilizzare i portatori di interessi a proposito dei codici di condotta». (art. 6, par. 1 Regolamento (UE) 2018/1807).

[110] Tra i portatori di interesse («stakeholder» in inglese) il Regolamento cita «le associazioni di PMI e start-up, gli utenti e i fornitori di servizi cloud».

[111] A questo proposito si vedano, in particolare l'art. 6, par. 3 e l'art. 8, par. 1, lett. c) del citato Regolamento (UE) 2018/1807.

[112] M.E. BARTOLINI, *op. cit.* n. 87, p. 1351.

codici di condotta, lasciando più spazio all'autonomia del regolatore privato. Anche in questo caso, i codici di condotta previsti dal Regolamento P2B non hanno effetto vincolante ma sono applicabili soltanto dai privati, pur mantenendo la Commissione un compito di monitoraggio[113] in merito all'efficacia degli stessi nel contribuire al rispetto del regolamento.

Esempi analoghi, su cui non ci si soffermerà qui nel dettaglio per ragioni di esposizione[114], si possono inoltre trovare nella Direttiva (UE) 2018/1808[115] e nella Direttiva (UE) 2019/770 sulla fornitura di servizi digitali[116].

3.2.2 Il GDPR e l'approvazione formale di strumenti di regolamentazione privata

Uno strumento normativo in cui viene valorizzato il potere regolatorio dei privati prevedendo al contempo un ruolo più incisivo per il regolatore pubblico è il GDPR, il già citato Regolamento (UE) 2016/679 generale sulla protezione dei dati personali. Non è questa la sede per addentrarsi nello studio dettagliato della complessa disciplina prevista da tale strumento[117]. Ai nostri fini

---

[113] V. a questo proposito art. 18 Regolamento P2B.

[114] Per approfondire si rimanda a M.E. BARTOLINI, *op. cit.* n. 87, p. 1350.

[115] 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, apparsa in GU L 303 del 28 novembre 2018, pagg. 69–92. Si veda in particolare il nuovo art. 4-bis della Direttiva 2010/13/UE, come modificato dalla Direttiva del 2018.

[116] Direttiva (UE) 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, apparsa in GU L 136 del 22 maggio 2019, pagg. 1–27. Si veda, in particolare, il considerando 50.

[117] Per approfondire si rimanda *ex multis* a: C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020; si veda altresì il relativo aggiornamento: C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary – Update of Selected Articles*, Oxford University Press, 2021, disponibile su SSRN: https://ssrn.com/abstract=3839645. Quanto alla dottrina italiana si rimanda *ex multis* a: G. DELLA MORTE, *op. cit.* Cap. 1, n. 47; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione, Ipsoa, 2022.

vale invece la pena concentrarsi sulle disposizioni relative al tema della regolamentazione privata, con l'ovvia premessa per cui il GDPR, applicandosi[118] a tutti i trattamenti[119] di dati personali[120] interamente o parzialmente automatizzati (così come a quelli non automatizzati di dati personali contenuti in un archivio o destinati a figurarvi), costituisce una norma rilevante per le piattaforme digitali.

In questo regolamento, in particolare, il legislatore dell'Unione ha previsto diversi sistemi di approvazione formale di strumenti di regolamentazione privata da parte di autorità pubbliche competenti, siano esse la Commissione europea ovvero le autorità di controllo nazionali[121]. La differenza è netta rispetto all'incoraggiamento previsto dalle norme esaminate nel precedente paragrafo (v. *supra*: par. 3.2.2), in quanto il controllo del regolatore pubblico su quello privato risulta qui più penetrante, non potendo quest'ultimo dotarsi di regole con effetti giuridici ai sensi del regolamento senza una formale approvazione

---

[118] Si veda l'art. 2 sull'ambito di applicazione materiale del GDPR. Sull'ambito di applicazione territoriale si veda invece l'art. 3. Per approfondire quest'ultimo aspetto si rimanda, *ex multis*, oltre che ai commentari precedentemente citati, a: P. FRANZINA, *op. cit.* Cap. 2, n. 123; F. MARONGIU BONAIUTI, *op. cit.* Cap. 2 n. 129.

[119] Per la definizione di «trattamento» si veda l'art. 4, n. 2) GDPR, per cui s'intende: «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

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

[121] Ai sensi dell'art. 4, n. 21) GDPR, per «autorità di controllo» si intende «l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51». Le autorità in questione sono incaricate di garantire il rispetto del GDPR all'interno dei rispettivi Stati membri (vi sono peraltro Stati, come la Germania, in cui sono state individuate più autorità di controllo). In Italia, l'autorità di controllo è il Garante per la protezione dei dati personali.

del primo. Questi conserva, peraltro, dei cruciali compiti di monitoraggio, sostenuti anche da incisivi poteri d'indagine e di irrogazione di sanzioni (v. *infra*: par. 3.2.3).

A) Codici di condotta e meccanismi di certificazione

Il primo dei menzionati sistemi[122] è previsto dall'art. 40 GDPR. Questa norma, infatti, oltre a contenere un incoraggiamento (par. 1) all'elaborazione di codici di condotta analoghi a quelli poc'anzi visti, stabilisce l'obbligo per le associazioni e gli organismi rappresentanti delle categorie di titolari[123] e responsabili[124] del trattamento di sottoporre gli stessi all'approvazione delle autorità di controllo nazionali per la loro adozione, modifica o proroga (par. 5). In caso di codici riferiti a trattamenti transfrontalieri è previsto un procedimento articolato che prevede l'intervento del comitato europeo per la protezione dei dati[125] e culmina con l'approvazione della Commissione europea.

Peraltro, le indicazioni del legislatore, così come l'influenza sua e delle autorità pubbliche competenti sull'attività dei regolatori privati, non si fermano al solo aspetto dell'adozione dei codici di condotta. Al contrario, l'art. 41 GDPR interviene direttamente anche sul monitoraggio di tali codici, che viene rimesso, oltre che alle autorità di controllo nazionali, ad organismi (anche pri-

---

[122] In questo senso v. C. BUSCH, *op. cit.* Cap. 1, n. 19.

[123] Ai sensi dell'art. 4, n. 7) GDPR, per «titolare del trattamento» s'intende: «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 […]».

[124] Ai sensi dell'art. 4, n. 8) GDPR, per «responsabile del trattamento» s'intende: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

[125] Il comitato europeo per la protezione dei dati (European Data Protection Board in inglese – "EDPB") è un organismo dell'Unione europea dotato di personalità giuridica e composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro, dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti (art. 68 GDPR). Il comitato ha diversi compiti relativi all'applicazione della normativa in materia di protezione dei dati personali, elencati nel dettaglio all'art. 70 GDPR.

vati) in possesso di competenze adeguate ed accreditati dalla autorità di controllo secondo un procedimento previsto dalla medesima norma. Per ottenere tale accreditamento sono previsti degli specifici requisiti di indipendenza e competenza ed è inoltre richiesto agli organismi in questione di istituire due tipi di procedure[126]. Le prime devono consentire di valutare l'ammissibilità dei titolari e dei responsabili del trattamento ad applicare il codice oggetto di monitoraggio, di controllare che detti titolari e responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento. Le seconde, invece, devono essere procedure (e relative strutture) atte a gestire i reclami relativi a violazioni del codice o al modo in cui questo è stato o è attuato da un titolare o un responsabile del trattamento e devono essere resi trasparenti per gli interessati e per il pubblico.

È fatto, inoltre, obbligo ai regolatori privati di prevedere delle misure opportune in caso di violazioni dei codici di condotta da parte di un titolare o di un responsabile del trattamento, che possono includere anche la sospensione o l'esclusione dal codice specificamente violato (art. 41, par. 4 GDPR).

Un'ulteriore valorizzazione della regolamentazione privata è prevista dall'art. 42 GDPR, il quale prevede l'incoraggiamento – ad opera degli Stati membri, delle autorità di controllo e della Commissione europea – all'istituzione di meccanismi di «certificazione» della protezione dei dati nonché di «sigilli e marchi di protezione dei dati» finalizzati a dimostrare il rispetto del GDPR da parte dei titolari o dei responsabili del trattamento[127]. Questi meccanismi rappresentano un'espressione della *private regulation* nella forma di *best*

[126] V. art. 41, par. 2 GDPR.

[127] Per approfondire si vada: E. LACHAUD, *What GDPR Tells about Certification*, 2020, disponibile su SSRN: https://ssrn.com/abstract=3557167

practice e standard di settore, in special modo quelli tecnici[128], e per via di queste caratteristiche sono stati definiti in dottrina[129] come una «forma alternativa di unificazione legislativa», la cui efficacia è stata assimilata agli strumenti di *soft-law*. L'adesione ai suddetti meccanismi è del tutto volontaria e permette di stabilire una presunzione di conformità con le disposizioni del GDPR in capo ai titolari e ai responsabili del trattamento che vi si sottopongono. Per questo motivo essi sono stati assimilati dalla richiamata dottrina[130] ai codici di condotta appena esaminati.

Le certificazioni di cui all'art. 42 GDPR – la cui durata non può eccedere il periodo di tre anni ed è rinnovabile – vengono rilasciate dalle autorità di controllo nazionali ovvero da organismi di certificazione con adeguate competenze ed accreditati secondo quanto previsto dall'art. 43 GDPR. Responsabili dell'accreditamento sono l'autorità di controllo competente o, in alternativa, l'organismo nazionale designato in virtù del regolamento (CE) n. 765/2008[131], conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente. I requisiti generali per ottenere l'accreditamento sono elencati invece nell'art. 43, par. 2 GDPR, mentre i paragrafi successivi disciplinano il relativo procedimento.

Il sistema delle certificazioni di cui agli artt. 42 e 43 GDPR – invero ancora scarsamente utilizzato in Italia – configura quindi un tentativo, da parte del

---

[128] Per l'assimilazione degli standard Iso 27001 a tali meccanismi si vedano: F. PEZZA, *Art. 42 Certificazione*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *op. cit.* n. 117, pp. 380-386; G.M. RICCIO, V. VITI, in MediaLaws.eu, 19 luglio 2017, disponibile al seguente link: https://www.medialaws.eu/le-certificazioni-privacy-ed-il-regolamento-ue/.

[129] F. PEZZA, *op. cit.* n. 128, p. 383.

[130] Idem, p. 384.

[131] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (Testo rilevante ai fini del SEE), apparso in GU L 218 del 13.8.2008, pagg. 30–47. Quanto all'Italia, l'organismo designato è Accredia per l'Italia.

legislatore europeo, di raggiungere un compromesso tra autoregolamentazione privata e controllo da parte dell'autorità pubblica[132]. L'art. 43 GDPR prevede a tal fine un procedimento articolato, in cui si trovano a collaborare diversi attori, sia pubblici che privati, con ruoli differenti. Come nel caso dei codici di condotta, peraltro, si registra una posizione di preminenza, anche formale, dell'attore pubblico, al quale spetta il compito di stabilire le condizioni per l'accreditamento e il controllo sull'operato degli organismi di certificazione. In questo senso, infatti, è previsto che l'autorità di controllo o gli organismi nazionali di accreditamento revochino l'accreditamento in caso di mancato rispetto delle relative condizioni ovvero di violazione delle norme del GDPR da parte di un organismo di certificazione (par. 7). Ulteriore aspetto, quest'ultimo, che vale a distinguere questi sistemi dai semplici incoraggiamenti all'adozione di strumenti di regolamentazione privata precedentemente menzionati e che appare maggiormente in grado di limitare e orientare il potere regolatorio dei privati.

B) La regolamentazione privata nella disciplina sul trasferimento dei dati verso paesi terzi

Un importante ambito in cui il GDPR effettua una valorizzazione della regolamentazione privata è rappresentato dalla disciplina sui trasferimenti di dati personali al di fuori dell'Unione europea[133]. Si tratta di una materia che riveste un'importanza fondamentale nell'impianto del regolamento, che è stata ed è foriera di conflitti regolatori[134] – tuttora irrisolti – tra Unione europea e Stati

---

[132] F. PEZZA, *Art. 43 Organismi di certificazione*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *op. cit.* n. 117, pp. 387-393.

[133] A questo proposito si veda *ex multis*: M. MANTOVANI, *Contractual Obligations as a Tool for International Transfers of Personal Data under the GDPR*, apparso su Eapil.blog, 24 gennaio 2020, disponibile al seguente link: https://eapil.org/2020/01/20/contractual-obligations-as-a-tool-for-international-transfers-of-personal-data/

[134] V. *ex multis*: G. RESTA, *op. cit.* Cap. 1, n. 37; T. CHRISTAKIS, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, in R.

Uniti, nell'ambito dei quali si sono sviluppati importanti filoni giurisprudenziali[135] e si è assistito (e si assiste) a negoziati politici[136] nel tentativo di giungere a soluzioni condivise nel rispetto dei principi e delle condizioni molto stringenti previsti dalla normativa dell'Unione.

Senza pretese di esaustività, vale la pena ricordare come l'obiettivo delle disposizioni del GDPR in materia (ossia il Capo V, artt. 44-50) sia quello di assicurare che, in caso di trasferimenti[137] di dati personali verso un paese terzo o

---

MILCH, S. BENTHALL (a cura di), *Cybersecurity and Privacy in a Globalized World – Building Common Approaches*, New York University School of Law, e-book, 2019. Disponibile su SSRN: https://ssrn.com/abstract=3397047.

[135] Celebre è a questo proposito la saga relativa alla vicenda che ha visti contrapposti lo studente attivista austriaco Max Schrems e Facebook relativa al trasferimento dei dati personali verso gli Stati Uniti e già citata sub Cap. 3, n. 73. Si ricordano qui le due senteze: Per quanto riguarda le due sentenze: CGUE, causa C-362/2014, *Schrems I*; CGUE, causa C-311/18, *Schrems II*.

[136] Si veda in ultimo l'annuncio congiunto della Commissione europea e degli Stati Uniti che, il 25 maggio 2022, hanno annunciato il raggiungimento di un accordo politico su un nuovo quadro per i trasferimenti verso gli Stati Uniti, in sostituzione dello EU-U.S. Privacy Shield annullato con la sentenza *Schrems II*. Qui il testo del comunicato: https://ec.europa.eu/commission/presscorner/detail/it/ip_22_2087. Per un commento dottrinale sui negoziati si veda: T. CHRISTAKIS, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in International Data Privacy Law, Vol. 11, n. 2, pp. 81-106, 2021.

[137] Il GDPR, così come la previgente Direttiva 95/46/CE, non contiene una definizione di «trasferimento». Un chiarimento è tuttavia stato fornito dall'EDPB nelle proprie Linee Guida 5/2021 – *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*. In particolare, a parere del comitato, il trasferimento di dati si configura al ricorrere di tre condizioni: (1) un titolare o un responsabile del trattamento è sottoposto al GDPR per un determinato trattamento; (2) questo titolare o responsabile del trattamento ("esportatore") comunica trasmettendo o rende in qualsiasi altro modo disponibili i dati personali oggetto del suddetto trattamento ad un altro titolare, contitolare o responsabile del trattamento ("esportatore"); (3) questo titolare o responsabile del trattamento si trova in un paese terzo o in una organizzazione, a prescindere dal fatto se questo importatore sia o meno sottoposto al GDPR con riferimento al predetto trattamento ai sensi dell'art. 3 GDPR (v. pag 4, traduzione in italiano dell'autore di questo lavoro).

un'organizzazione internazionale, «il livello di protezione delle persone fisiche garantito dal […] regolamento non sia pregiudicato[138]». Ciò significa, secondo quanto chiarito dalla Corte di Giustizia nella sentenza *Schrems I*[139] e ribadito dal considerando 104 del GDPR, che il paese terzo destinatario dovrebbe offrire garanzie di un adeguato livello di protezione dei dati, che sia cioè «sostanzialmente equivalente» a quello assicurato all'interno dell'Unione. In assenza di tali garanzie, un titolare o un responsabile del trattamento non potrebbe, di regola, procedere al trasferimento dei dati.

È facile intuire come il rispetto di questo principio risulti nella pratica molto complicato per diverse ragioni. In *primis* quelle relative alle profonde differenze[140] esistenti nelle varie legislazioni in materia di protezione dei dati personali a livello mondiale[141], in molti casi spie di approcci e principi fondamentali agli antipodi e collidenti tra i vari ordinamenti giuridici. Si pensi, ad esem-

[138] V. art. 44 GDPR.

[139] CGUE, *Schrems I*, punto 73.

[140] Per approfondire il tema si rimanda *ex multis* a: G. DELLA MORTE, *op. cit.* n. 47 Cap. 1.

[141] Peraltro, non tutti gli ordinamenti giuridici statali o le organizzazioni internazionali sono dotati di legislazioni organiche in materia. Ne sono un esempio gli Stati Uniti, ove manca una legislazione federale sulla protezione dei dati personali, la cui tutela è invece demandata a specifiche norme settoriali, ad esempio in materia di consumatori. Si segnala, peraltro, come recentemente diversi Stati interni si siano dotati di normative organiche, come la California con il California Consumer Privacy Act (CCPA) del 2018, anch'esso peraltro rivolto in via principale ai consumatori.

pio, alla preminenza rispetto alla *data protection* accordata alla libertà di espressione o alla tutela della sicurezza nazionale negli Stati Uniti[142] o, ancora, all'utilizzo della sorveglianza di massa in ordinamenti come la Russia[143] o la Cina[144], all'interno dei quali i dati personali vengono considerati quasi alla stregua di beni nazionali. A complicare ulteriormente le cose sono l'enorme quantità di dati personali continuamente in movimento sulla rete a velocità spesso non controllabile e il dato di fatto per cui la maggior parte delle grandi multinazionali dell'economia digitale, sui cui sistemi gran parte delle imprese e degli individui di tutto il mondo archiviano le proprie informazioni e i propri dati personali, abbiano sede al di fuori dell'Unione, ed in particolare negli Stati Uniti[145].

Ciò posto, le norme del Capo V GDPR stabiliscono delle condizioni molto stringenti per trasferire dati al di fuori dell'Unione. Di regola[146] è infatti necessaria, secondo quanto previsto dall'art. 45 GDPR, la presenza di una decisione formale con cui la Commissione europea abbia ritenuto adeguato il livello di protezione dei dati personali assicurato da un paese terzo, un territorio o uno

---

[142] V. *ex multis*: G. RESTA, *op. cit.* Cap. 1, n. 37; T. CHRISTAKIS, *op. cit.* n. 134; C.M. MARIOTTINI, *Freedom of Speech and Foreign Defamation Judgments:From New York Times v. Sullivan via Ehrenfeld to the 2010 SPEECH Act*, in B. HESS, C.M. MARIOTTINI (a cura di), *Protecting Privacy in Private International and Procedural Law and by Data Protection,* pp. 115-168, Nomos Verlagsgesllschaft, 2015; T. CHRISTAKIS, *National Security, Surveillance and Human Rights*, in R. GEISS, N. MELZER (a cura di), *Oxford Handbook on the International Law of Global Security*, Oxford University Press, 2020, disponibile su SSRN: https://ssrn.com/abstract=3599994.

[143] Si vedano ad esempio gli stringenti requisiti di «*data localisation*» previsti dalla Legge Federale del 21 luglio 2014, n. 242-FZ, un riassunto della quale è accessibile in inglese sul portale www.dataguidance.com

[144] Con riguardo al PIPL, già citato in precedenza nel Cap. 3, n. 200 si veda, *ex multis*: I. CALZADA, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in Smart Cities, Vol. 5, n. 3, pp. 1129-1150, 2022.

[145] Si pensi, ad esempio, all'acronimo GAFA, indicante Google, Amazon, Facebook e Apple, così come ad altri colossi come Microsoft, Oracle, Salesforce, Twitter, tutti facenti capo ad imprese controllanti con sede negli Stati Uniti.

[146] Alcune deroghe tassative sono previste dall'art. 49 GDPR.

o più settori specifici sull'interno di questo, o da una organizzazione internazionale («decisione di adeguatezza»). In mancanza – circostanza tutt'altro che di scuola visto che, allo stato, risultano in vigore soltanto quindici[147] decisioni di adeguatezza – è necessario, ai sensi dell'art. 46 GDPR, che il titolare o il responsabile del trattamento fornisca «garanzie adeguate» sulla protezione dei dati in caso di trasferimento, a condizione, peraltro, che gli interessati dispongano di diritti azionabili e di mezzi di ricorso effettivi.

A questo proposito, l'art. 46, par. 2 e 3 GDPR prevede un elenco di strumenti giuridici in grado di costituire «garanzie adeguate» senza necessità di autorizzazione dell'autorità di controllo. Questo elenco è importante ai nostri fini in quanto, con l'unica eccezione degli strumenti giuridici vincolanti tra autorità pubbliche[148], contiene misure di regolamentazione privata. In particolare, tra le garanzie in questione compaiono i già menzionati codici di condotta[149] di cui all'art. 40 GDPR e i meccanismi di certificazione[150] di cui all'art. 42 GDPR. Accanto a questi vi sono altri due strumenti contraddistinti dall'intreccio tra regolamentazione di fonte pubblica e privata, ossia le «clausole contrattuali tipo» («*standard contractual clauses*» in inglese, note nella prassi con la sigla «SCCs») e le «norme vincolanti d'impresa» («*binding corporate rules*», nella prassi abbreviato in «BCRs»).

---

147 Dopo l'invalidazione dello EU-U.S. Privacy Shield a seguito della sentenza *Schrems II*, risultano in vigore le decisioni di adeguatezza riferite ai seguenti paesi: Regno Unito, Andorra, Argentina, Australia (per quanto riguarda i codici di prenotazione dei passeggeri aerei, "Passenger Name Records – PNR"), Canada, Faer Oer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, Stati Uniti d'America (per quanto riguarda i codici di prenotazione dei passeggeri aerei, "Passenger Name Records – PNR").

148 V. art. 46, par. 2, lett. a) GDPR.

149 V. art. 46, par. 2, lett. e) GDPR.

150 V. art. 46, par. 2, lett. f) GDPR.

Cominciando dalle SCCs, val la pena chiarire come queste costituiscano lo strumento più utilizzato nella prassi[151]. Si tratta, in particolare, di un insieme di clausole contrattuali modello («tipo» come dice la norma) il cui contenuto deve essere previamente approvato dalla Commissione europea[152], ovvero dall'autorità di controllo competente. Le clausole in questione – che, a seguito dell'approvazione, non possono essere modificate dalle parti – devono quindi formare oggetto di un accordo contrattuale tra «esportatore[153]» ed «importatore[154]» dei dati. Un contratto finalizzato a garantire agli interessati – i quali rivestono il ruolo di terzi beneficiari – un livello di protezione dei propri dati adeguato e dei rimedi effettivi in caso di violazione. Si tratta, pertanto, di uno strumento che, pur rivestendo la forma di un accordo privato, è nella sostanza soggetto all'approvazione del regolatore pubblico, ed è in questo senso assimilabile ai codici di condotta.

Va peraltro aggiunto come, proprio per via della loro natura contrattuale, le SCCs risultino idonee a vincolare le parti ma non anche le autorità pubbliche dei paesi terzi di destinazione ed in particolare ad impedire un accesso di queste ai dati. Per tale motivo la Corte di Giustizia, nella sentenza *Schrems II*[155], ha considerato le clausole tipo di per sé[156] non sufficienti a garantire un livello adeguato di protezione agli interessati in caso di trasferimento verso un paese

---

151 V. *ex multis*: G.M. RICCIO, *Art. 46 Trasferimento soggetto a garanzie adeguate*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *op. cit.* n. 117, pp. 404-408.

152 Oggi sono in vigore le *standard contractual clauses* approvate con Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (Testo rilevante ai fini del SEE).

153 Ai sensi della clausola 1 delle SCC di cui al precedente punto 152, per «esportatore» si intende «la o le persone fisiche o giuridiche, la o le autorità pubbliche, lo o gli organismi o altri organi […] che trasferiscono i dati personali […]».

154 Ai sensi della clausola 1 delle SCC di cui al precedente punto 152, per «importatore» si intende «la o le entità di un paese terzo che ricevono i dati personali dall'esportatore, direttamente o indirettamente tramite un'altra entità anch'essa parte delle presenti clausole […]».

155 CGUE, *Schrems II*, punti 133, 134.

156 C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *op. cit.* n. 117 (aggiornamento 2021), p. 171.

terzo. Al contrario, a parere dei Giudici di Lussemburgo[157] è necessario che il titolare del trattamento (o il responsabile), prima di procedere al trasferimento, verifichi, caso per caso, se il diritto del paese di destinazione garantisca una protezione adeguata dei dati personali trasferiti sulla base delle SCCs e, in caso negativo, valuti l'adozione di misure supplementari[158] rispetto a queste. In altre parole, la Corte di Giustizia – facendo leva[159] su quanto previsto dall'art. 46 e dal considerando 109 GDPR – ha in questo modo valorizzato in maniera decisiva il principio dell'«*accountability*[160]» dei titolari e dei responsabili del trattamento (spesso soggetti privati), lasciando in capo ad essi la responsabilità ultima della regolamentazione dei trasferimenti extra UE, comunque nel rispetto delle disposizioni del GDPR.

Venendo all'analisi delle norme vincolanti d'impresa[161], occorre innanzitutto sottolineare come le stesse presentino in maniera più evidente i caratteri degli strumenti di *transnational private regulation*[162]. Si tratta, infatti, di norme di fonte privata – come regole tecniche, strumenti di sicurezza, *policy* di condotta, attività di *training* e *audit*[163] – adottate all'interno di un gruppo di società multinazionale (o anche di una singola impresa) e che, a determinate condizioni, permettono i trasferimenti di dati personali verso paesi terzi, a condizione che

---

[157] CGUE, *Schrems II*, punto 134.
[158] Idem, punti 132-135. Per un chiarimento in merito alle predette misure supplementari si veda: EDPB, *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali*, 18 giugno 2021.
[159] CGUE, *Schrems II*, punto 132.
[160] C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *op. cit.* n. 117 (aggiornamento 2021), p. 171.
[161] Per approfondire si vedano *ex multis*: C. KUNER, *Article 47 Binding Corporate Rules*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 813-824, Oxford University Press, 2020; L. MOEREL, *Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection*, 2011. Accessibile online: https://research.tilburguniversity.edu/en/publications/binding-corporate-rules-fixing-the-regulatory-patchwork-of-data-p
[162] In questo senso v. L. MOEREL, *op. cit.* n. 161, p. 198.
[163] G.M. RICCIO, *Art. 47 Norme vincolanti d'impresa*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *op. cit.* n. 117, pp. 408-413.

questi riguardino soltanto imprese appartenenti al medesimo gruppo. A differenza delle SCCs, le BCRs non erano contemplate dalla precedente direttiva 95/46/CE, anche se, durante la vigenza di quest'ultima, il WP29 le aveva in più occasioni[164] menzionate come strumenti di fonte privata utilizzabili per i trasferimenti dei dati. Il loro inserimento all'interno del GDPR – che dedica ad esse l'intero art. 47 – risponde, peraltro, a modelli già utilizzati dai gruppi multinazionali in altre materie come la salute, l'ambiente o la sicurezza[165].

Anche per quanto riguarda la BCRs, tuttavia, è forte l'influenza del regolatore pubblico sull'attività di quello privato. Infatti, ai sensi dell'art. 47 GDPR, le stesse necessitano dell'approvazione dell'autorità di controllo competente per poter essere utilizzate quale «garanzie appropriate» per i trasferimenti transfrontalieri. L'approvazione in questione – per cui è previsto un articolato procedimento – è subordinata al rispetto di alcune condizioni. In particolare, le BCRs devono essere giuridicamente vincolanti[166] e applicarsi «a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune», nonché ai loro dipendenti, conferire espressamente interessati i diritti azionabili in relazione al trattamento dei loro dati personali e soddisfare alcuni requisiti sostanziali previsti all'art. 47, par. 2 GDPR.

I requisiti in questione rafforzano ulteriormente l'influenza del regolatore pubblico sull'attività regolatoria dei gruppi d'imprese, che si trovano a dover dotare le proprie *binding corporate rules* di contenuti predeterminati dal primo.

---

[164] Per un elenco esaustivo dei documenti del WP29 e dell'EDPB in materia di norme vincolanti d'impresa si rimanda a C. KUNER, *op. cit.* n. 161, p. 823.

[165] V. a questo proposito *ex multis*: L. MOEREL, *op. cit.* n. 161, C. KUNER, *European Data Protection Law: Corporate Compliance and Regulation*, 2a edizione, Oxford University Press, 2007 (in particolare v. p. 217).

[166] Sul punto si veda in particolare C. KUNER, *op. cit.* n. 165, p. 225. In particolare, l'autore cita come strumenti attraverso cui rendere «legalmente vincolanti» le *binding corporate rules* i contratti e l'assunzione di obblighi attraverso dichiarazioni unilaterali.

Quanto a tali contenuti, senza pretesa di esaustività, è opportuno ai nostri fini segnalare come le BCRs debbano presentare alcuni aspetti che valgono a rafforzarne la natura di strumento di *transnational private regulation*, conferendo una dimensione istituzionale al gruppo che decide di dotarsene. In particolare, è previsto che le stesse chiariscano la propria natura giuridicamente vincolante, sia all'interno che all'esterno del gruppo[167], ed esplicitino i compiti dei soggetti incaricati del controllo del rispetto delle BCRs, della formazione e della gestione dei reclami[168], per i quali devono essere previste apposite procedure[169]. Le BCRs devono inoltre stabilire dei meccanismi atti a verificare il rispetto di esse all'interno del gruppo, i quali devono comprendere verifiche sulla protezione dei dati e metodi per assicurare «provvedimenti correttivi» intesi a proteggere i diritti degli interessati[170]. Infine, le norme vincolanti d'imprese devono prevedere i meccanismi per le modifiche delle stesse, nonché la registrazione e comunicazione di queste alle autorità di controllo[171]. Più in generale, le BCRs devono prevedere i meccanismi di cooperazione con le autorità di controllo[172] e per segnalare a queste qualsiasi requisito di legge che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle stesse[173].

3.2.3 Altri elementi distintivi: trasparenza, *accountability*, sanzioni pecuniarie

In chiusura, è opportuno richiamare brevemente alcuni elementi rintracciabili in diversi strumenti normativi in materia di nuove tecnologie e piattaforme digitali già citati nel corso del presente lavoro, che anche suggeriscono come il

[167] Art. 47, par. 2, lett. f) GDPR.
[168] Art. 47, par. 2, lett. h) GDPR.
[169] Art. 47, par. 2, lett. i) GDPR.
[170] Art. 47, par. 2, lett. j) GDPR.
[171] Art. 47, par. 2, lett. k) GDPR.
[172] Art. 47, par. 2, lett. l) GDPR.
[173] Art. 47, par. 2, lett. m) GDPR.

legislatore dell'Unione abbia teso e tenda a considerare in maniera decisiva la «dimensione istituzionale» degli attori della rete (e in particolare delle piattaforme) nello stabilire le regole a questi applicabili.

Il primo di questi elementi è rappresentato dalla valorizzazione del già richiamato principio dell'«*accountability*» e dalla progressiva responsabilizzazione degli *internet service provider* (v. *supra* Cap. 2, par. 2.3, 3.1). Di questo si scorge traccia, oltre che nei già esaminati Regolamento P2B e Direttiva Copyright, tra gli altri anche nel GDPR. In particolare, quest'ultimo menziona[174] l'*accountability* («responsabilizzazione» in italiano) tra i principi fondamentali applicabili ai trattamenti di dati personali. In base a tale principio, il titolare del trattamento deve essere in grado di rispettare in ogni momento le disposizioni del regolamento e di dimostrare la propria conformità ad esso. Simili doveri sono, come vedremo, posti in capo agli *hosting provider* e ai fornitori delle piattaforme online anche dal nuovo Digital Services Act (v. *infra*: Cap. 6).

Altro principio comune a diversi strumenti dell'Unione è quello della trasparenza. Esso è, come abbiamo già notato (v. *supra*: Cap. 2, par. 3.1), uno degli obiettivi del Regolamento P2B ed è presente sia nel GDPR[175] che nel Digital Services Act, oltre che rappresentare uno dei capisaldi su cui si fondano gli strumenti dell'Unione in materia di consumatori[176]. L'utilizzo dello stesso, al pari dell'*accountability*, è funzionale anche ad orientare l'attività degli internet *service provider* al rispetto delle regole stabilite dal legislatore. Ciò vale, come già visto, per il contenuto dei «termini e condizioni» delle piattaforme, che si è sottolineato essere la base delle regole che disciplinano i rapporti afferenti tanto alla «dimensione verticale» quanto alla «dimensione orizzontale» delle stesse, così come per i sistemi di gestione dei reclami istituiti all'interno delle

[174] Art. 5, par. 2 GDPR.
[175] Artt. 12, 13, 14 GDPR.
[176] V. *ex multis*: C. TWIGG-FLESNER, *op. cit*, Cap. 2, n. 56.

piattaforme. Vale, inoltre, per i trattamenti di dati personali effettuati dai gestori delle piattaforme stesse, così come per il funzionamento dei relativi algoritmi[177], alla base dell'attività di *self-enforcement* delle regole delle piattaforme.

In ultimo, è necessario ribadire come una grande importanza nella strategia regolatoria dell'Unione in materia di nuove tecnologie sia ricoperta dalle sanzioni pecuniarie. Tanto il GDPR[178] quanto il Digital Services Act[179] prevedono, infatti, l'irrogazione di sanzioni pecuniarie molto elevate – rispettivamente, sino ad un massimo del 4% e del 6% del fatturato annuo mondiale – volte a disincentivare, con un forte effetto deterrente, le violazioni delle relative disposizioni. Si tratta, quindi, di un tipico meccanismo di «*top-down regulation*», il cui utilizzo appare tuttora necessario per orientare i gestori delle piattaforme – molti dei quali, come detto, stabiliti in paesi terzi – al rispetto della disciplina dell'Unione, anche per quanto riguarda le loro condotte in qualità di regolatori privati.

Le sanzioni in questione appaiono, in senso lato, assimilabili a quelle che sono state definite come «*market destroying measure*» dalla dottrina[180] della c.d. «*market sovereignty*». In particolare, a parere di questa dottrina, un ordinamento giuridico che volesse esercitare i propri poteri sulla rete sarebbe effettivamente in grado di farlo soltanto se riuscisse a precludere l'accesso al proprio mercato ai soggetti che non si conformano al proprio diritto, attraverso l'utilizzo di strumenti sanzionatori (da qui l'espressione «*market destroying measure*»).

---

[177] M. CANTERO GAMITO, *op. cit.* Cap. 1, n. 19.
[178] V. art. 83 GDPR.
[179] V. art. 52 Digital Services Act.
[180] V. D.J. SVANTESSON, *op. cit.*, Cap. 1, n. 62.

È chiaro, peraltro, che l'efficacia di tali strumenti dipenda prima di tutto dalle dimensioni del mercato specificamente considerato. Nel caso dell'Unione europea[181], il Mercato Unico costituisce il secondo mercato a livello mondiale, per quanto riguarda il commercio internazionale[182] e, pertanto, operare all'interno di esso è di grande importanza per gran parte dei gruppi multinazionali cui fanno capo le piattaforme digitali. Di contro, peraltro, l'Unione non può allo stato permettersi di non attirare tali soggetti nella propria economia. In questo quadro, la minaccia di sanzioni pecuniarie elevate – le quali non costituiscono, in senso tecnico, delle «*market destroying measures*» descritte da Svantesson – appare un deterrente efficace per indurre i gestori delle piattaforme a conformarsi e a conformare le proprie condotte da regolatori privati al diritto dell'Unione, ove desiderosi di operare nel Mercato Unico.

Ciò non vale, peraltro, a negare l'assunto per cui il legislatore dell'Unione abbia fondato la propria strategia regolatoria (anche) sulla presa d'atto della «dimensione istituzionale» delle piattaforme e del potere regolatorio dei relativi gestori. Al contrario, proprio alla luce di tale dimensione e delle relative implicazioni, vale a rafforzare – quanto meno in astratto – la preminenza delle norme di fonte pubblica rispetto a quelle di fonte privata.

---

[181] A questo proposito, è appena il caso di ricordare come nella dottrina statunitense sia stata coniata l'espressione «*Brussels Effect*», ad indicare il fenomeno per cui l'Unione sia in grado di influenzare le legislazioni di diversi Stati ed ordinamenti giuridici terzi, oltre che le norme e gli standard di grandi gruppi multinazionali, sfruttando le dimensioni del proprio mercato e regolando unilateralmente diverse materie come la salute, la tutela dell'ambiente o la protezione dei dati personali. Questa influenza, in particolare, darebbe luogo ad un fenomeno di «*race to the top*» verso le regole e gli standard dell'Unione, anche in situazioni e ordinamenti giuridici in cui questi non siano direttamente applicabili. Per approfondire si vedano: A. BRADFORD, *opp. citt.* Cap. 1, n. 48.

[182] Per approfondire si veda la pagine «Fatti e cifre sull'economia dell'Unione europea», consultata in ultimo il 10 novembre 2022: https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/economy_it#:~:text=Il%20valore%20totale%20di%20tutti,14%20500%20miliardi%20di%20euro.

Capitolo 5 – *Focus:* l'autoregolamentazione delle piattaforme nel contrasto alla diffusione di contenuti illeciti sui *social network*

SOMMARIO: 1 Il contrasto alla diffusione di contenuti illeciti sui *social network* tra diritto di fonte pubblica e *private regulation*. – 1.1 Il ruolo centrale dei gestori delle piattaforme nel contrasto alla diffusione di contenuti illeciti e le tensioni con i regolatori pubblici. – 1.2 I tentativi di risoluzione dei conflitti normativi attraverso gli strumenti di autoregolamentazione e co. – 1.2.1 L'autoregolamentazione: dai Santa Clara Principles alle iniziative delle singole piattaforme (rinvio). – 1.2.2 La promozione di meccanismi di coregolamentazione nell'Unione europea: il codice di condotta contro l'odio online e quello di buone pratiche contro la disinformazione. – 1.2.3 Alcuni casi significativi della giurisprudenza italiana sul ruolo delle piattaforme di *social network* nel contrasto ai discorsi d'odio. – 2 Un esempio avanzato di autoregolamentazione: il Facebook Oversight Board. – 2.1 Facebook Oversight Board: genesi e architettura istituzionale. –2.2 I poteri e l'efficacia delle decisioni del Facebook Oversight Board. – 2.3 Il riconoscimento dei limiti del diritto di fonte pubblica nell'Oversight Board Charter. – 2.4 Un esempio pratico di pronuncia del Board: la decisione sulla sospensione del profilo di Donald Trump (cenni).

1. Il contrasto alla diffusione di contenuti illeciti sui *social network* tra diritto di fonte pubblica e *private regulation*

Il potere regolatorio dei gestori delle piattaforme digitali, e segnatamente di quelle di *social network*, si manifesta in forme particolarmente significative nell'azione di contrasto alla diffusione di contenuti ritenuti riprovevoli, come

quelli riconducibili alla categoria dei «discorsi d'odio[1]» («*hate speech*») e delle «notizie false» («*fake news*[2]»), oltre che di altri contenuti illeciti, quali quelli lesivi dei diritti di proprietà intellettuale.

Pur non essendo possibile soffermarsi nel dettaglio su ciascuna di queste tematiche[3], merita, ai fini del presente lavoro, fornire un quadro d'insieme sul tema. L'importanza dei gestori delle piattaforme in materia è, infatti, cresciuta al punto che, negli ultimi anni, sempre più spesso il legislatore dell'Unione ha fatto ricorso agli stessi o ha tentato di orientarne il potere regolatorio – talvolta

---

[1] Per una definizione a rilevanza internazionalistica del fenomeno dell'«*hate speech*» si veda la Raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. (97)/20 del 30 ottobre 1997: «For the purposes of the application of these principles, the term "hate speech" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin». Si veda inoltre l'art. 1, lett. a) della Decisione quadro 2008/913/GAI del Consiglio, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, secondo cui ciascuno Stato membro deve adottare le misure necessarie affinché sia resa punibile «l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica».

[2] Per una definizione del concetto si veda la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final, 26 aprile 2018. Secondo questo documento, in particolare: «Per disinformazione si intende un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico. Il pregiudizio pubblico include 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. La disinformazione non include gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte». Per il relativo codice di condotta e il successivo aggiornamento del 2022 si rimanda a *infra*.

[3] Per approfondire si vedano *ex multis*: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, pp. 229-272; F. ABBONDANTE, *Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in Informatica e diritto, Vol. 26, n. 1-2, pp. 41-68, 2017; C. BUSCH, *Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation*, in UCLA Journal of Law & Technology, Vol. 27, n. 2, pp. 32-79, 2022. P. FALLETTA, *Controlli e responsabilità dei social network sui discorsi d'odio online*, in Media Laws, n. 1, pp. 146-158, 2020, disponibile online: https://www.medialaws.eu/rivista/controlli-e-responsabilita-dei-social-network-sui-discorsi-dodio-online/; O. POLLICINO, G. PITRUZZELLA, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, 2017; O. POLLICINO, G. PITRUZZELLA, *Disinformation and Hate Speech: A European Constitutional Perspective,* Egea, 2021.

tramite strumenti di *soft-law* o di coregolamentazione e talvolta attraverso tradizionali mezzi legislativi – per cercare di raggiungere i propri obiettivi sul punto.

Il tema sarà analizzato dapprima con una panoramica generale, per poi soffermarsi su quello che, probabilmente, costituisce ad oggi l'esempio più avanzati di autoregolamentazione di una piattaforma di *social network*, vale a dire il Facebook Oversight Board (al riguardo v. *infra* par. 2). A livello metodologico, va chiarito come, per semplicità, l'analisi sarà condotta utilizzando l'espressione omnicomprensiva – e per certi versi atecnica – «contenuti illeciti[4]». Con questa formula ci si riferirà, quindi, a tutti quei contenuti – siano essi informazioni, immagini, *file* audio-video o contenuti multimediali di altro genere – condivisi dagli utenti di una piattaforma di *social network* la cui diffusione possa costituire una violazione rilevante ai fini del diritto di fonte pubblica di volta in volta applicabile[5].

1.1 Il ruolo centrale dei gestori delle piattaforme nel contrasto alla diffusione di contenuti illeciti e le tensioni con i regolatori pubblici

Si è già avuto modo di constatare come i regolatori pubblici abbisognino strutturalmente della cooperazione degli *internet service provider* per poter garantire l'applicazione delle proprie regole nel ciberspazio (v. *supra*: Cap. 1, par. 5; Cap. 3, par. 5.3). Di più, abbiamo notato come i gestori delle piattaforme digitali costituiscano, sotto molti punti di vista, i soggetti nella posizione migliore per assumere funzioni regolatorie e para-giurisdizionali all'interno dei propri ambienti virtuali, quanto meno nella forma della coregolamentazione

[4] Per una panoramica si veda: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Lotta ai contenuti illeciti online – Verso una maggiore responsabilizzazione delle piattaforme online*, COM(2017)555 final, 28 settembre 2017.

[5] A questo proposito si pongono, peraltro, inevitabilmente delle questioni internazionalprivatistiche, per le quali si rimanda integralmente agli approfondimenti svolti nel Cap. 3.

(v. *supra*: Cap. 4, par. 3.1.2, 3.1.3) Allo stesso modo, si è già evidenziato (v. *supra*: Cap. 2, par. 2) come la disciplina dell'Unione in materia di *internet service provider* – peraltro di recente revisione a seguito dell'entrata in vigore del Digital Services Act (v. *infra*: Cap. 6) – si fondi in gran parte sulla previsione di diversi regimi di (ir)responsabilità, a seconda del tipo di fornitore coinvolto, per l'illiceità dei contenuti e delle informazioni condivise dagli utenti.

Alla luce del quadro così richiamato, è facile intuire come i gestori delle piattaforme digitali di *social network* rivestano un ruolo centrale ai fini del contrasto alla diffusione di contenuti illeciti all'interno dei propri ambienti. Essi sono, infatti, in primo luogo i soggetti che materialmente hanno il compito di rimuovere i contenuti illeciti dalle piattaforme, o comunque di bloccarne la diffusione, dando così attuazione alla disciplina stabilita dai regolatori pubblici. Inoltre, come è stato notato in dottrina[6], a prescindere dall'esistenza di provvedimenti o ordini delle autorità pubbliche, gli stessi appaiono come i soggetti più adatti a monitorare la diffusione di contenuti illeciti, a dare un riscontro pronto ed efficace alle segnalazioni degli utenti e a gestire i reclami presentati a seguito delle decisioni di rimuovere uno o più contenuti o di disabilitare l'accesso agli stessi.

Si tratta, è appena il caso di ribadirlo, di compiti molto delicati, che implicano il bilanciamento tra diritti e interessi spesso collidenti e vitali per la società e la democrazia occidentale[7], di cui le piattaforme risultano di fatto incaricate. Lo svolgimento di questi compiti solleva inoltre, come già visto, diverse questioni internazionalprivatistiche, strettamente collegate alla natura transnazionale

[6] V. *ex multis*: P. FALLETTA, *op. cit.* n. 3, p. 154; G.M. RUOTOLO, *op. cit.* p. 233, Cap. 3, n. 119; C. GOANTA, P. ORTOLANI, *Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts*, 2021, disponibile su SSRN: https://ssrn.com/abstract=3969360.
[7] V. *ex multis*: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119; O. POLLICINO, G. PITRUZZELLA, *op. cit.* n. 3.

delle piattaforme e alla conseguente necessità per i gestori delle stesse di adeguarsi ad un numero assai elevato di normative spesso in conflitto tra loro e sempre più di impostazione unilateralista, con le criticità che questo comporta anche in termini di «*regulatory overreaching*» (v. *supra*: Cap. 3). A questo proposito, è utile soltanto richiamare una recente sentenza[8] della Corte di Giustizia dell'Unione europea, a mente della quale è possibile, ai sensi dell'art. 15 della Direttiva e-Commerce, per un giudice di uno Stato membro ingiungere ad un *hosting provider* di rimuovere informazioni o di bloccare l'accesso alle medesime a livello mondiale, purché questo avvenga «nell'ambito del diritto internazionale pertinente».

Le tensioni connesse al ruolo dei gestori delle piattaforme discendono inoltre, come già anticipato, dalla sovrapposizione tra regolamentazione privata e normativa di fonte pubblica. A questo proposito, occorre, infatti, sottolineare come non di rado la condivisione di contenuti illeciti secondo il diritto di fonte pubblica costituisca anche una violazione delle norme di *private regulation* che disciplinano i rapporti all'interno della stessa piattaforma – siano esse termini e condizioni, condizioni generali, «*community standard*» o altro tipo di regole – che, come già visto, vengono accettate dall'utente al momento dell'iscrizione (v. *supra*: Cap. 1, par. 2.1). Conseguenza di ciò è che la rimozione dei contenuti illeciti – così come ogni altra sanzione irrogabile dal gestore di una piattaforma a seguito della violazione delle proprie regole, come l'esclusione o la sospensione dell'utente – costituisce, nella maggior parte dei casi, applicazione di entrambe le normative.

È in questo scenario che vi possono essere delle situazioni di conflitto. Infatti, le regole di una piattaforma potrebbero, ad esempio, considerare legittima la

[8] CGUE, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook Ireland Limited*, 3 ottobre 2019 – ECLI:EU:C:2019:821.

condivisione di contenuti vietati dal diritto di fonte pubblica[9]. Allo stesso modo, i termini e le condizioni di una piattaforma potrebbero prevedere delle regole restrittive che finiscano con il considerare illegittime delle condotte perfettamente lecite ai sensi del diritto di fonte pubblica. Questi contrasti assumono rilevanza, in particolare, quando si tratta di effettuare un bilanciamento tra l'esercizio di diritti fondamentali come la partecipazione alla vita politica o la libertà di espressione – per cui i *social network* assumono un'importanza sempre più decisiva – e il contrasto alla diffusione di discorsi d'odio o *fake news* (v. nello specifico *infra*: par. 2). Si consideri, ad esempio, il caso dei disordini verificatisi il 6 gennaio 2021 in occasione dell'assalto al Campidoglio da parte dei sostenitori del Presidente uscente degli Stati Uniti Donald Trump[10] (v. *infra*: par. 2.4 per quanto riguarda la pronuncia del Facebook Oversight Board sulla vicenda). In quel caso, infatti, i *social network* hanno giocato un ruolo decisivo nel compattare il fronte a favore del *tycoon* e solo a seguito degli incidenti la maggior parte delle piattaforme – che sino a quel momento si erano limitate a classificare come «*fake news*» alcune delle esternazioni dello stesso Trump, senza tuttavia impedirne la pubblicazione – ha deciso di sospendere o rimuovere i profili dell'allora Presidente[11].

1.2 I tentativi di risoluzione dei conflitti normativi attraverso gli strumenti di autoregolamentazione e coregolamentazione

Nel tentativo di risolvere le tensioni regolatorie di cui si è appena detto, si è assistito da più parti alla promozione e alla valorizzazione di meccanismi di

[9] Si pensi ad esempio ai diversi standard adottati dalle varie piattaforme di social network in ambiti come la pornografia, talvolta in conflitto con le numerose legislazioni statali in materia. V. *ex multis*: C. GOANTA, P. ORTOLANI, *op. cit.* n. 6, p. 18; F. ABBONDANTE, *op. cit.* n. 3, p. 53.

[10] Per una descrizione puntuale dei fatti si rimanda a: *I social network, Trump e l'attacco al Congresso*, apparso su ilPost.it, 7 gennaio 2021, disponibile online: https://www.ilpost.it/2021/01/07/attacco-congresso-trump-social-network/, consultato in ultimo il 7 dicembre 2022.

[11] V. *ex multis*: C. BUSCH, *op. cit.* n. 3; C. GOANTA, P. ORTOLANI, *op. cit.* n. 6, p. 5.

autoregolamentazione o di coregolamentazione, allo scopo di trovare un punto di equilibrio tra le diverse sensibilità e i vari interessi in gioco.

Si tratta di tendenze registratesi sia nell'ambito dell'Unione europea (su cui si rimanda a *infra*: par. 1.2.2) che in altri ordinamenti giuridici[12] e che si sono concretizzate, principalmente, in strumenti di c.d. «*soft-law*», finalizzati a rafforzare i compiti di sorveglianza degli *internet service provider* attraverso quella che è stata definita in dottrina come una forma di «pressione morbida[13]». A questi si sono affiancate iniziative tipiche di *private regulation* da parte di accademici, esponenti della società civile o delle singole piattaforme. Non è qui possibile soffermarsi nel dettaglio su ciascuno di questi progetti[14], che saranno soltanto brevemente passati in rassegna nelle prossime pagine, rimandando invece alla seconda parte di questa sezione per gli approfondimenti in merito al Facebook Oversight Board (v. *infra*: par. 2).

1.2.1 L'autoregolamentazione: dai Santa Clara Principles alle iniziative delle singole piattaforme (rinvio)

Cominciando delle iniziative di autoregolamentazione, tra le più rilevanti è opportuno menzionare i c.d. «Santa Clara Principles[15]». Si tratta di un progetto intrapreso nel 2018 da un gruppo di accademici, addetti ai lavori e membri

---

[12] Senza alcuna pretesa di esaustività, si vedano ad esempio, a livello internazionale, la Dichiarazione e il Programma d'Azione di Durban, pubblicati al termine della Conferenza mondiali contro il razzismo, la discriminazione razziale, la xenofobia e la relativa intolleranza, tenutasi a Durban tra il 31 agosto e il 7 settembre 2001. Si vedano altresì gli United Nations Guiding Principles on Business and Human Rights (UNGPs), sostenuti ufficialmente dal Consiglio per i diritti umani delle Nazioni Unite nel 2011. Più specificamente rivolti a internet si vedano, inoltre, la Global Network Initiative (GNI) e il *Report on freedom of expression, states and the private sector in the digital age*, A/HRC/32/38, presentato alla 32a sessione del Consiglio per i diritti umani della Nazioni Unite e pubblicato l'11 maggio 2016.

[13] V. in particolare: P. FALLETTA, *op. cit.* n. 3, p. 154; F. ABBONDANTE, *op. cit.* n. 3, p. 64.

[14] Per approfondimenti ed indicazioni bibliografiche si rimanda *ex multis* a G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, pp. 229-272.

[15] The Santa Clara Principles – On Transparency and Accountability in Content Moderation, disponibili online al seguente indirizzo: https://santaclaraprinciples.org/, consultato in ultimo il 21 novembre 2022.

della società civile statunitense e non solo, che hanno redatto un documento di principi comuni relativi al monitoraggio sulla diffusione di contenuti da parte delle piattaforme di *social network*. L'iniziativa ha ricevuto l'adesione di dodici imprese tra le maggiori protagoniste della c.d. *tech-economy*, tra cui Apple, Meta (Facebook e Instagram), Google, Reddit, Twitter e Github[16]. Nel 2021, peraltro, al termine di un percorso di aggiornamento è stata pubblicata una nuova versione del suddetto documento, contenente i Santa Clara Principles 2.0.

Obiettivo dichiarato dei principi è la promozione della libertà d'espressione e dei diritti umani degli utenti di internet. Non appare peraltro casuale che la libertà di espressione assuma un'importanza centrale – rispetto, ad esempio, alla tutela della riservatezza o al contrasto ai discorsi d'odio – in un'iniziativa di questo genere, sorta negli Stati Uniti. Inoltre, va aggiunto come i principi, riconoscendo la dimensione transnazionale della rete, abbiano sì lo scopo di stabilire degli standard comuni a livello internazionale ma, dichiaratamente, non aspirino a divenire un «*template for regulation*» da recepire acriticamente da parte degli ordinamenti giuridici di fonte pubblica.

A livello di contenuto[17], i Santa Clara Principles fanno leva sui già esaminati concetti di trasparenza ed «*accountability*», al centro della strategia regolatoria dell'Unione europea (cfr. Cap. 4, par. 3.2.3). In particolare, viene posta enfasi sul principio del «*due process*» per quanto riguarda le procedure per la segnalazione e la rimozione dei contenuti, che dovrebbero includere anche fasi di impugnazione delle decisioni assunte in prima istanza nei confronti degli utenti. A livello di trasparenza, i principi richiedono ai gestori delle piattaforme, tra le altre cose, di mettere a disposizione in maniera agevole le proprie

[16] Idem.
[17] Per una panoramica si veda *ex multis*: C. BUSCH, *op. cit.* n. 3, pp. 72ss.

regole agli utenti, così come di informare in anticipo («*notice*») ciascun utente della rimozione dei contenuti da questi condivisi, così come della sospensione del proprio account e di qualsiasi altra azione intrapresa a seguito della violazione delle regole della piattaforma stessa, prevedendo altresì dei doveri di motivazione.

In altri casi, la promozione di meccanismi di «*accountability*» e trasparenza è sorta direttamente dall'iniziativa degli stessi gestori delle piattaforme. A questo proposito, si è già ampiamente avuto modo di constatare come i fornitori di piattaforme digitali – così come altri *internet service provider* – siano dotati di poteri regolatori all'interno dei propri ambienti. Una circostanza di cui, come visto, anche il legislatore dell'Unione ha in più occasioni dimostrato di prendere atto (v. *supra* Cap. 4, par. 3).

In questo quadro, allo scopo di gestire le questioni relative al monitoraggio dei contenuti[18], i gestori di alcune piattaforme hanno tentato di conferire alle stesse una dimensione istituzionale sempre più accentuata, stabilendo dei veri e propri organi para-giurisdizionali indipendenti e dotandosi di specifiche regole e procedure per la gestione delle segnalazioni e la rimozione dei contenuti rispettose dei diritti e delle prerogative degli utenti. È il caso, ad esempio, del Twitch Safety Advisory Council[19], costituito nel maggio 2020 «to enhance Twitch's approach to issues of trust and safety». Soprattutto, è il caso paradigmatico[20] del Facebook Oversight Board, che rappresenta oggi la forma più

[18] C. GOANTA, P. ORTOLANI, *op. cit.* n. 6, p. 6.
[19] Per una panoramica si veda il seguente link: https://safety.twitch.tv/s/article/Safety-Advisory-Council?language=en_US#1Overview.
[20] V. *ex multis*: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 265; C. GOANTA, P. ORTOLANI, *op. cit.* n. 6, p. 6.

avanzata[21] di autoregolamentazione di una piattaforma digitale e su cui ci si soffermerà nel dettaglio a breve (v. *infra*: par. 2).

1.2.2 La promozione di meccanismi di coregolamentazione nell'Unione europea: il codice di condotta contro l'odio *online* e quello di buone pratiche contro la disinformazione

Per quanto riguarda i meccanismi di coregolamentazione, nei tempi recenti si è assistito ad un'importante valorizzazione degli stessi ai fini del contrasto alla diffusione di contenuti illeciti da parte dell'Unione europea, anche sulla scia di quanto a più riprese[22] sostenuto dalla Commissione in merito all'importanza di tali sistemi nella disciplina delle piattaforme digitali (v. *supra*: Cap. 4 par. 3.1).

A questo proposito, oltre alla revisione della normativa sulla responsabilità degli *internet service provider* di cui si dirà meglio in seguito (v. *infra*: Cap. 6), negli ultimi anni sono stati adottati dall'Unione alcuni strumenti di «*soft-law*» volti ad indirizzare, mediante la già richiamata tecnica della «pressione morbida», l'attività delle piattaforme. Tra essi rientrano, in particolare, il Codice di condotta[23] contro i discorsi d'odio online del 2016 e il Codice di buone pratiche

[21] F. BASSAN, *op. cit.* Cap, 4, n. 3, p. 89.
[22] V. in particolare: COM(2016) 288 final; COM(2017) 555 final, entrambe *cit.* Cap. 2, n. 7.
[23] Commissione europea, *Codice di condotta per lottare contro le forme illegali di incitamento all'odio online*, maggio 2016. Disponibile online: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_it

contro la disinformazione, adottato per la prima volta[24] nel 2018 dalla Commissione europea e aggiornato in versione «rafforzata[25]» nel 2022, entrambi di seguito analizzati senza pretese di esaustività.

Iniziando dal Codice contro i discorsi d'odio, vale la pena, innanzi tutto, sottolineare come lo stesso recepisca la nozione di «incitamento illegale all'odio online» di cui al già richiamato art. 1, lett. a) della Decisione quadro 2008/913/GAI. Il documento mira ad orientare le attività delle «aziende informatiche[26]» aderenti e a «consentire la condivisione delle migliori pratiche con altre imprese operanti su internet, con le piattaforme e con gli operatori dei media sociali». In questo senso, tali aziende assumono esplicitamente il ruolo di «guida» nella lotta contro la diffusione delle forme illegali di incitamento all'odio online, sottolineando peraltro la necessità di tutelare, nello svolgimento di tale compito, l'esercizio della libertà di espressione.

A livello contenutistico, il Codice stabilisce l'impegno, per le aziende informatiche aderenti, di adottare procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da esse offerti. Tale impegno si collega direttamente a quello di esaminare, entro ventiquattro ore dalla ricezione, la maggior parte delle segnalazioni valide relative a tali contenuti e, se necessario, di rimuoverli ovvero di disabilitare l'accesso

[24] Commissione europea, *Codice di buone pratiche dell'UE sulla disinformazione*, 16 ottobre 2018. Disponibile online al seguente link: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[25] Commissione europea, *Codice di buone pratiche sulla disinformazione rafforzato*, 16 giugno 2022. Disponibile online al seguente link: https://digital-strategy.ec.europa.eu/it/library/2022-strengthened-code-practice-disinformation.

[26] Si tratta della formula utilizzata nella versione italiana del Codice, corrispondente all'inglese «IT Companies». Trattasi di formule atecniche riferite alle imprese che hanno aderito al Codice. Per i fini che qui interessano sembra possibile assimilare la nozione a quella di «*internet service provider*» di cui alla Direttiva *e-Commerce*.

agli stessi. È, altresì, prevista l'adozione di linee-guida indirizzate alla comunità degli utenti della rete, che precisino il divieto di ogni forma di istigazione all'odio e alla violenza.

Anche da questo Codice emerge, inoltre, l'attenzione ai principi della trasparenza e dell'*accountability*. Quanto alla trasparenza, il documento prevede l'impegno a fornire informazioni sulle procedure di trasmissione degli avvisi allo scopo di rendere più rapida ed efficace la comunicazione fra le autorità degli Stati membri e le aziende informatiche, così come l'impegno reciproco di Commissione europea e *internet service provider* a «proseguire le discussioni su modalità idonee a promuovere la trasparenza e ad incoraggiare narrazioni alternative che contrastino l'incitamento all'odio». Quanto all'*accountability*, invece, è opportuno segnalare come le stesse parti firmatarie abbiano convenuto di riesaminare gli impegni previsti dal Codice a cadenze regolari, valutando anche l'impatto degli stessi.

Da quanto sopra emerge come con l'adozione del Codice la Commissione abbia, sostanzialmente, inteso affidare agli *internet service provider* il compito di contrastare, quanto meno in prima istanza, la diffusione di contenuti illegali d'odio[27] in rete attraverso una chiara strategia improntata sulla coregolamentazione, come ribadito dallo stesso Esecutivo nella sua successiva comunicazione[28] sull'argomento. Al momento della sua adozione, il Codice ha registrato l'adesione di Facebook, Twitter, YouTube e Microsoft, a cui negli anni successivi si sono aggiunti Instagram, Snapchat, Dailymotion, Jeuxvideo.com, TikTok, LinkedIn, Rakuten, Viber e Twitch. I risultati empirici disponibili alla ste-

[27] P. FALLETTA, *op. cit.* n. 3, p. 154.
[28] COM(2017) 555 final, *cit.* Cap. 2, n. 7.

sura del presente lavoro suggeriscono, peraltro, come la strategia della Commissione sembri funzionare[29]. Infatti, stando ai dati del sesto monitoraggio[30] sul Codice pubblicati nell'ottobre 2021, le aziende informatiche aderenti sono state in grado di verificate l'81% delle segnalazioni ricevute[31] nell'anno precedente, mentre la percentuale di contenuti rimossi a seguito delle stesse si è attestata sul 62,5%[32].

Venendo al Codice di buone pratiche sulla disinformazione, occorre innanzi tutto ribadire come lo stesso abbia conosciuto di recente un aggiornamento che ne ha cambiato in maniera sensibile l'impostazione[33].

In particolare, nella prima versione del 2018 il Codice costituiva un tipico strumento di autoregolamentazione, elaborato da imprese e associazioni di categoria dell'economia digitale e a cui negli anni avevano aderito sedici firmatari, incluse alcune tra le maggiori piattaforme[34]. Si trattava del primo sistema di norme concordato a livello transnazionale per contrastare la disinformazione online. A livello di contenuti[35], il Codice del 2018 si fondava sugli obiettivi stabiliti dalla già citata[36] comunicazione della Commissione europea in

---

[29] In senso positivo si vedano anche: P. FALLETTA, *op. cit.* n. 3, p. 155; G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 255.

[30] I risultati dei diversi monitoraggi sono disponibili al seguente link: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_it

[31] Seppur alto, il dato è peraltro minore rispetto al 90,4% registrato nel 2020.

[32] Anche questo dato è in calo rispetto ai precedenti (71% di media tra il 2019 e il 2020).

[33] A questo proposito si veda O. POLLICINO, *The Road Towards a Strengthened Code Against Disinformation: About Metaphors in Free Speech and the Need to Handle Them Carefully*, in European Law Institute Newsletter, n. 3, pp. 2-3, 2022. L'autore ha contribuito in maniera decisiva alla redazione del Codice rafforzato del 2022 in qualità di «*honest broker*».

[34] I dati sulle adesioni sono disponibili online: https://digital-strategy.ec.europa.eu/it/library/2018-code-practice-disinformation. Risulta, in particolare, come il codice sia stato firmato nell'ottobre 2018 dalle piattaforme Facebook, Google, Twitter e Mozilla, nonché da inserzionisti e altri operatori del settore pubblicitario. Microsoft ha aderito nel maggio 2019, mentre TikTok nel giugno 2020.

[35] C. BUSCH, *op. cit.* n. 3, p. 66.

[36] V. COM(2018) 236 final, 26 aprile 2018, sub. nota 2.

materia e stabiliva un elenco di ventuno principi cui attenersi per raggiungere tali obiettivi. I principi riguardavano, in particolare, il vaglio delle inserzioni pubblicitarie, la trasparenza della pubblicità politica e tematica, l'integrità dei servizi, la responsabilizzazione dei consumatori e quella dei verificatori di fatti e dei ricercatori, oltre che la misurazione dell'efficacia dello stesso Codice, per cui era previsto un ruolo importante per la Commissione europea.

Proprio i monitoraggi[37] della Commissione hanno evidenziato la necessità, esplicitata dallo stesso Esecutivo nei propri Orientamenti sul rafforzamento del Codice[38], di rivedere e aggiornare lo strumento in commento prevedendo obblighi più stringenti e specifici oltre che maggiori responsabilità per le piattaforme, chiamate non più soltanto a controllare sé stesse ma ad affrontare tutti i rischi sistemici inerenti ai loro servizi. Sulla scia dei richiamati Orientamenti si è, quindi, sviluppato un percorso di revisione sotto l'egida della Commissione, che è culminato con l'adozione del Codice «rafforzato», approvato e sottoscritto da 34 firmatari[39] il 16 giugno 2022.

Come anticipato, con il Codice rafforzato si assiste ad un cambio di approccio rispetto al precedente. In particolare, come altresì sottolineato da autorevole dottrina[40], si passa da uno strumento di autoregolamentazione a un testo che,

---

[37] Si vedano in particolare: Staff Working Document, *Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*, SWD(2020) 180 final, 10 settembre 2020, accessibile online: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement; Programma di monitoraggio della disinformazione sulla Covid-19, i cui dettagli e i report presentati dalle piattaforme aderenti sono accessibili online: https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme.

[38] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*, COM(2021) 262 final, 26 maggio 2021.

[39] L'elenco dei firmatari è disponibile al presente link: https://digital-strategy.ec.europa.eu/it/library/signatories-2022-strengthened-code-practice-disinformation.

[40] O. POLLICINO, *op. cit.* n. 33.

anche in coerenza con il nuovo Digital Services Act, pone al centro della propria strategia normativa la coregolamentazione, quanto meno per ciò che riguarda l'attività delle grandi piattaforme.

A livello di contenuti, in linea con quanto affermato dalla Commissione, il nuovo Codice prevede obblighi più stringenti e specifici in capo alle piattaforme per il contrasto alla disinformazione. Questi obblighi sono condensati in un elenco di 44 impegni e 127 misure specifiche, su cui non è qui possibile soffermarsi in maniera esaustiva[41]. In estrema sintesi, è però possibile individuare come capisaldi del nuovo codice, oltre alla coregolamentazione di cui si è detto: (i) l'impegno ad ampliare la partecipazione all'iniziativa anche ad attori diversi dalle grandi piattaforme; (ii) la c.d. «demonetizzazione» della disinformazione; (iii) l'attenzione verso i comportamenti manipolativi (*account* fasulli, bot o *deep fake* malevoli che diffondono disinformazione); (iv) l'ampliamento e il rafforzamento degli strumenti che consentano agli utenti di individuare e segnalare contenuti falsi o fuorvianti; (v) l'impulso alla verifica dei fatti in tutti i paesi e in tutte le lingue dell'Unione; (vi) la trasparenza della pubblicità politica; (vii) il sostegno ai ricercatori offrendo loro un migliore accesso ai dati delle piattaforme; (viii) la valutazione dell'impatto del Codice attraverso l'istituzione un solido quadro di monitoraggio e comunicazione; (ix)

[41] Per una panoramica sul nuovo strumento, oltre ai primi commenti dottrinali si rimanda alle relative Faq pubblicate sul sito della Commissione europea: https://ec.europa.eu/commission/presscorner/detail/it/QANDA_22_3665, consultato in ultimo il 25 novembre 2022. A livello dottrinale si rimanda a: O. POLLICINO, *op. cit.* n. 33; G.M. RICCIO, *Tre buoni motivi per salutare con favore il Code of Practice on Disinformation*, apparso su MediaLaws.eu, 17 novembre 2022, disponibile online: https://www.medialaws.eu/tre-buoni-motivi-per-salutare-con-favore-il-code-of-practice-on-disinformation/; P. CAVALERI, *The Truth in Fake News: How Disinformation Laws Are Reframing the Concepts*, University of Edinburgh School of Law Working Paper n. 12, 2022. Disponibile su SSRN: https://ssrn.com/abstract=4151908; C. TAN, *Regulating Disinformation on Twitter and Facebook*, in Griffith Law Review Vol. 31, n. 4, pp. 513-536, 2022. Liberamente accessibile online: https://doi.org/10.1080/10383441.2022.2138140.

l'istituzione di un centro per la trasparenza e di una *task force* permanente, allo scopo di mantenere il Codice adeguato ai suoi obiettivi e alle esigenze future.

Questo Codice rafforzato, anche più del suo predecessore, esemplifica in pieno la nuova strategia regolatoria intrapresa dall'Unione[42], tesa a valorizzare ed orientare il potere regolatorio delle piattaforme (e degli altri attori di internet) attraverso strumenti di coregolamentazione, che facciano leva su principi come la trasparenza e l'«*accountability*». Significativo, a questo proposito, il fatto che lo stesso sia stato adottato a seguito del raggiungimento dell'accordo politico provvisorio[43] tra i colegislatori dell'Unione sul Digital Services Act e che, alla lettera (h) del preambolo, affermi esplicitamente che «actions under the Code will complement and be aligned with regulatory requirements and overall objectives in the Digital Services Act (DSA) once it enters into force», ponendo inoltre enfasi sui codici di condotta e sulle misure di coregolamentazione previste dallo stesso regolamento (v. *infra*: Cap. 6, par. 4.4).

1.2.3 Alcuni casi significativi della giurisprudenza italiana sul ruolo delle piattaforme di *social network* nel contrasto ai discorsi d'odio

Svolta questa breve analisi sulle tendenze registratesi negli ultimi anni a livello internazionale e di Unione europea, è utile adesso dare succintamente conto di alcuni recenti sviluppi nella giurisprudenza italiana, allo scopo di verificare come dei giudici interni – per ragioni di prossimità e di sintesi si è scelto di occuparci soltanto del nostro paese – si siano approcciati, nei tempi recenti, alla materia di cui abbiamo sinteticamente appena tracciato l'evolu-

[42] V. a questo proposito: O. POLLICINO, *op. cit.* n. 33; G.M. RICCIO, *op. cit.* n. 41.

[43] L'accordo in questione è stato annunciato con un comunicato stampa del 23 aprile 2022, reperibile online sul sito del Consiglio dell'Unione: https://www.consilium.europa.eu/it/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/.

zione. Dalla giurisprudenza del nostro paese emerge, invero, un quadro piuttosto incerto e lacunoso – soprattutto dal punto di vista internazionalprivatista – composto da provvedimenti[44] di natura cautelare e dagli esiti talvolta incongruenti tra di loro, a partire dai quali non appare possibile individuare una tendenza giurisprudenziale consolidata.

Il primo dei provvedimenti in commento è un'ordinanza del Tribunale di Roma[45], emessa il 12 dicembre 2019 (e confermata[46] dal collegio in sede di reclamo nel maggio 2020) nell'ambito di un ricorso ex art. 700 c.p.c. presentato dal movimento politico italiano di estrema destra CasaPound nei confronti di Facebook Ireland Limited a seguito della disattivazione, da parte del *social network*, della pagina del partito e del profilo del suo fondatore per violazione dei *community standard* di Facebook in materia di messaggi d'odio. L'ordinanza in questione, al di là dei profili relativi al bilanciamento tra la libertà di espressione e il contrasto ai discorsi d'odio[47], è interessante ai nostri fini in quanto, nell'accogliere il ricorso di CasaPound, il Giudice capitolino si è soffermato in

---

[44] Per una panoramica delle pronunce in questione si vedano: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 258; G. DELLA MORTE, *op. cit.* Cap. 3, n. 185, p. 36; P. FALLETTA, *op. cit.* n. 3. Per dei commenti si vedano invece: C. CARUSO, *La libertà di espressione presa sul serio — CasaPound c. Facebook, Atto I*, apparso su SidiBlog.it, 20 gennaio 2020, disponibile online: http://www.sidiblog.org/2020/01/20/la-liberta-di-espressione-presa-sul-serio-casa-pound-c-facebook-atto-i/; M. CASTELLANETA, P. DE SENA, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, apparso su SidiBlog.it, 20 gennaio 2020, disponibile online: http://www.sidiblog.org/2020/01/20/la-liberta-di-espressione-e-le-norme-internazionali-ed-europee-prese-sul-serio-sempre-su-casapound-c-facebook/.

[45] Tribunale di Roma, Sez. Impresa, R.G. 59264/2019, ordinanza del 12 dicembre 2019. Disponibile online su www.ilquotidianogiuridico.it e anche sul sito del Corriere della Sera: https://www.corriere.it/politica/19_dicembre_12/casapound-tribunale-roma-ordina-riattivazione-pagina-facebook-3a5f9a86-1cc9-11ea-9d5e-8159245f62dc.shtml, consultato in ultimo il 27 novembre 2022.

[46] Tribunale di Roma, Sez. XVII Civile, R.G. 80961/19, ordinanza del 29 aprile 2020. Disponibile online su www.ilquotidianogiuridico.it e anche sul sito del Corriere della Sera: https://www.corriere.it/cronache/20_maggio_29/casapound-contro-facebook-l-ordinanza-tribunale-roma-44eb8fae-a1ae-11ea-972c-41555f8ee621.shtml, consultato in ultimo il 27 novembre 2022.

[47] Su questi aspetti si rimanda alla dottrina citata sub nota 44.

maniera decisiva sulla posizione di Facebook nei rapporti con le proprie controparti contrattuali, tracciando di fatto dei limiti ai poteri regolatori del *social network*.

In particolare, pur riconoscendo che tali rapporti – afferenti, come a più riprese ricordato nel presente lavoro, alla «dimensione verticale» delle piattaforme (v. *supra*: Cap. 1, par. 2.1) – siano governati dalle Condizioni d'uso di Facebook, che ne costituiscono il «regolamento contrattuale» e sono accettate dagli utenti al momento della registrazione, il Tribunale di Roma ha chiarito come questi non siano assimilabili «al rapporto tra due soggetti privati qualsiasi», per via della speciale posizione ricoperta da Facebook. Infatti, come osservato dal Giudice, il servizio di Facebook (o di altri *social network* ad esso collegati) riveste oggi un'importanza preminente «con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (49 Cost.), al punto che il soggetto che non è presente su Facebook è di fatto escluso (o fortemente limitato) dal dibattito politico italiano». Ciò comporta, a parere del Tribunale, che Facebook «nella contrattazione con gli utenti, debba strettamente attenersi al rispetto dei principi costituzionali e ordinamentali finché non si dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente». In altre parole, «il rispetto dei principi costituzionali e ordinamentali» costituisce per Facebook condizione e limite nei rapporti con i propri utenti e – aggiungiamo noi – nell'esercizio del proprio potere regolatorio con riguardo agli stessi. Anche per questo, il Giudice capitolino ha considerato illegittima la chiusura della pagina di CasaPound, in quanto violazione del diritto al pluralismo di cui all'art. 49 Cost.

L'ordinanza è stata, come detto, confermata in sede di reclamo nella misura in cui il collegio ha ritenuto illegittima l'esclusione di CasaPound alla luce di

diverse fonti[48], sia di diritto interno che internazionale, e dell'assunto secondo cui la stessa sarebbe un'associazione pienamente lecita secondo l'«ordinamento generale[49]», presente da molti anni nel panorama politico del nostro paese. Senza entrare nel merito degli argomenti alla base di questa decisione, vale la pena ai nostri fini evidenziare come il collegio, nel giungere alle sue conclusioni, sembri, *obiter dictum*, di fatto ridimensionare (se non sconfessare del tutto) gli argomenti del giudice di prime cure in merito alla posizione speciale di Facebook nel rapporto con i propri utenti. Infatti, il collegio ha affermato esplicitamente di ritenere «indubbia la qualificazione del rapporto fra Facebook Ireland e l'utente come un ordinario contratto di diritto civile[50]», rilevando l'assenza, nell'ordinamento giuridico, di norme valevoli a conferire una natura speciale a tali rapporti[51]. Ciò, peraltro, non significa, a parere del collegio, che la disciplina degli stessi sia priva di limiti, essendo al contrario presenti quelli «ordinariamente riconosciuti per l'autonomia privata, riconducibili alle clausole generali dell'ordine pubblico, del buon costume, della buona fede ed al divieto di abuso del diritto, da interpretarsi secondo i principi

[48] In particolare, l'ordinanza in commento cita (al par. 14) quali norme interne: art. 21 Cost; XII disposizione transitoria e finale della Costituzione; legge 20 giugno 1952, n. 645; legge 13 ottobre 1975, n. 654, di ratifica ed esecuzione della convenzione internazionale di New York sull'eliminazione di tutte le forme di discriminazione razziale; D.L. 26 aprile 1993, n. 122 convertito con modificazioni dalla L. 25 giugno 1993, n. 205; artt. 604 bis e 604 ter c.p. Quali «fonti sovranazionali» sono invece citate: Convenzione di New York 1966 sull'eliminazione di tutte le forme di discriminazione razziale; Statuto della Corte Penale Internazionale; Convenzione europea dei diritti dell'uomo e delle libertà fondamentali; Carta dei diritti fondamentali dell'Unione europea. Per una critica in merito alla pertinenza di queste ultime norme (e della stessa espressione «fonti sovranazionali») si veda: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 259.

[49] Ordinanza Trib. Roma 29 aprile 2020, *cit.* sub n. 46, par. 25.

[50] Idem, par. 7.

[51] Idem, par. 8. Sul punto, il Collegio va incontro alle perplessità sollevate da certa dottrina all'indomani dell'ordinanza cautelare del 12 dicembre 2019, relative proprio all'assenza di norme che conferiscano una «posizione speciale» alle piattaforme di *social network*, «pubblicizzando» i servizi da questi offerti, o di contratti di contratti di servizio tra lo Stato e i gestori delle piattaforme stesse. V. in particolare: P. FALLETTA, *op. cit.* n. 3, p. 157.

costituzionali». Allo stesso modo, non sarebbe da escludersi «neanche l'applicazione diretta di parametri costituzionali quale limite all'autonomia privata[52]».

Il secondo provvedimento che vale la pena richiamare è sempre un'ordinanza[53] del medesimo Tribunale di Roma, emessa il 23 febbraio 2020 al termine di un procedimento cautelare del tutto assimilabile a quello poc'anzi esaminato, che ha visto coinvolti il movimento di estrema destra Forza Nuova e Facebook Ireland Limited. Come nel caso di CasaPound, Facebook aveva oscurato la pagina di Forza Nuova e di alcuni militanti della stessa per violazione degli standard della *community* con riferimento alla diffusione di messaggi d'odio. Sorprendentemente, tuttavia, la decisione del Tribunale è stata opposta a quella presa soltanto due mesi prima a seguito del ricorso dell'altro movimento neofascista. Infatti, al termine di una lunga e dettagliata ricapitolazione[54] di fonti giuridiche e di precedenti giurisprudenziali, sia nazionali che sovranazionali, nonché di contenuti e messaggi d'odio diffusi nel tempo da Forza Nuova e da propri esponenti, il Giudice capitolino ha confermato la decisione di Facebook di sospendere gli account dei ricorrenti a seguito di ripetute violazioni delle proprie Condizioni d'uso nelle parti relative alla diffusione di discorsi d'odio.

---

[52] Ordinanza Trib. Roma 29 aprile 2020, *cit.* sub n. 46, par. 8.

[53] Tribunale di Roma, Sez. Diritti della persona e immigrazione civile, R.G. 64894/2019, ordinanza del 23 febbraio 2020. Disponibile online, tra gli altri al seguente link: https://www.questionegiustizia.it/articolo/legittima-la-rimozione-da-parte-di-facebook-delle-pagine-di-forza-nuova-dal-social-network_24-02-2020.php, consultato in ultimo il 27 novembre 2022.

[54] Per una panoramica sulla motivazione del Tribunale e sulle norme da esso si richiamate si vedano: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 260; P. FALLETTA, *op. cit.* n. 3, p. 156; I.M. LO PRESTI, *CasaPound, Forza Nuova e Facebook. Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e social network*, in Forum di Quaderni Costituzionali, fasc. 2, pp. 924-946, 2020, disponibile online: https://www.forumcostituzionale.it/wordpress/?p=14887; O. GRANDINETTI, *Facebook vs. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in Media Laws, n. 1, pp. 173-203, 2021.

Non è qui possibile[55] ripercorrere tutti i passaggi della (lunga) ordinanza del Tribunale di Roma. Ai nostri fini, è opportuno peraltro sottolineare come in essa il Giudice capitolino abbia richiamato le Condizioni d'uso di Facebook e gli standard della *community* in materia di discorso d'odio, limitandosi tuttavia a evidenziare come queste fonti regolino i rapporti contrattuali tra la piattaforma e i propri utenti. A differenza che nel caso di CasaPound, quindi, il Tribunale non ha affermato che i rapporti in questione non possano essere considerati alla stregua di rapporti tra soggetti «qualsiasi[56]»per via della posizione di Facebook che viene, al contrario, considerato come un «soggetto privato, pur svolgendo un'attività di indubbio rilievo sociale[57]». Non è quindi dato scorgere, da questo punto di vista, tracce di quella «pubblicizzazione» della funzione dei *social network* contestata da certa dottrina[58] a seguito della prima ordinanza relativa a CasaPound né, a dire il vero, elementi che valorizzino in maniera decisiva la «dimensione istituzionale» degli stessi.

A questo proposito, è tuttavia degno di nota il fatto che il Tribunale di Roma, tra le diverse fonti normative richiamate, abbia incluso anche il Codice di condotta del 2016 contro l'odio *online* (v. *supra*: par. 1.2.2), sottolineandone l'importanza ai fini del contrasto al fenomeno anche per via della natura transnazionale degli «intermediari informatici[59]». In particolare, a parere del Giudice capitolino, proprio in virtù degli obblighi previsti dal Codice e dalle altre norme richiamate, Facebook aveva il dovere giuridico di risolvere i contratti con gli utenti protagonisti della diffusione dei messaggi d'odio.

---

[55] Per approfondire si rimanda, oltre che all'ordinanza stessa, alla dottrina citata sub nota 54.
[56] Come visto poc'anzi, si tratta dell'espressione utilizzata dal Tribunale di Roma nella prima ordinanza su CasaPound del 12 dicembre 2019, *cit.* sub nota 45.
[57] Trib. Roma, ordinanza 23 febbraio 2020 *cit.* sub nota 53, par. 2.
[58] P FALLETTA, *op. cit.* n. 3, p. 156.
[59] Trib. Roma, ordinanza 23 febbraio 2020 *cit.* sub nota 53, par. 1.3.

Quelli appena esaminati non costituiscono gli unici provvedimenti registratesi negli ultimi anni nella giurisprudenza italiana in tema di discorsi d'odio *online*. Si potrebbero, infatti, citare ulteriori ordinanze come, ad esempio, quella con cui, nel gennaio 2020, il Tribunale di Chieti ha accolto il ricorso ex art. 700 c.p.c. presentato nei confronti di Facebook da un avvocato, già esponente di Forza Nuova, che lamentava la chiusura del proprio profilo a seguito della pubblicazione di una foto di Benito Mussolini[60]. Sempre nel gennaio 2020, in senso opposto si è pronunciato il Tribunale di Siena che, ancora nell'ambito di un procedimento cautelare intentato nei confronti di Facebook, ha confermato la chiusura dei profili dei ricorrenti per violazione degli standard della *community* in materia di discorsi d'odio[61]. Quest'ultima pronuncia, in buona sostanza, si è fondata sui medesimi rilievi di cui all'ordinanza del Tribunale di Roma sul caso di Forza Nuova, per cui Facebook non può essere considerato come un soggetto pubblico e i suoi rapporti con gli utenti vanno trattati alla stregua di «normali» rapporti privatistici, disciplinati dalle Condizioni d'uso del *social network*. Proprio alla luce di queste ultime, secondo il Giudice senese, Facebook avrebbe avuto «il buon diritto, di origine contrattuale, a procedere alla disattivazione della pagina e del profilo» dei ricorrenti.

Come anticipato, dalla giurisprudenza italiana sul punto appare un quadro frammentario e sovente contradditorio, per cui risulta impossibile estrapolare

---

[60] Tribunale di Chieti, R.G. 1489/2019, ordinanza del 29 gennaio 2020. Per un commento si veda G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 260.

[61] Tribunale di Siena, R.G. 2968/2019, ordinanza del 19 gennaio 2020. Disponibile online su: https://dirittodiinternet.it/. Per dei commenti si vedano: P. FALLETTA, *op. cit.* n. 3, p. 158; L. ALBERTINI, *La responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione sul ruolo di gatekeepers della comunicazione)*, apparso su IlCaso.it il 22 settembre 2020, disponibile online al seguente link: https://blog.ilcaso.it/news_996/22-09-20/La_responsabilita_civile_degli_internet_service_provider_per_i_materiali_caricati_dagli_utenti_%28con_qualche_considerazione_sul_ruolo_di_gatekeepers_della_comunicazione%29, consultato in ultimo in data 28 novembre 2022.

dei paradigmi a rilevanza generale. Ciò è probabilmente dovuto anche alla natura cautelare, e quindi a cognizione sommaria, dei procedimenti al termine di cui sono state emesse le pronunce poc'anzi richiamate. Un punto comune alle diverse ordinanze, che merita qui di essere ribadito, è che ciascuna di esse abbia riconosciuto la rilevanza, ai fini della decisione, delle Condizioni d'uso e dei *community standard* di Facebook. Queste ultime, in particolare, sono state considerate nella maggior parte dei casi alla stregua di «normali» contratti, ad eccezione della prima ordinanza sul caso CasaPound, in cui come detto si scorgono elementi di valorizzazione della «dimensione istituzionale» del *social network*, tesi peraltro a limitarne ed orientarne il potere regolatorio. Da sottolineare, non senza perplessità, il fatto che nessuno di questi provvedimenti, pur riguardando situazioni con elementi di transnazionalità – se non altro dati dalla circostanza che Facebook Ireland Limited sia, per l'appunto, una società di diritto irlandese – abbia anche solo minimamente sfiorato le questioni internazionalprivatistiche di cui si è dato conto nel Capitolo 3. Un ulteriore segnale di come, nel nostro paese, ci sia ancora tanta strada da percorrere.

2. Un esempio avanzato di autoregolamentazione: il Facebook Oversight Board

Esaminati i recenti sviluppi normativi e giurisprudenziali in materia di contrasto alla diffusione di contenuti illeciti, tanto a livello interno che internazionale ed europeo, è opportuno adesso soffermarsi su quello che, probabilmente, rappresenta ad oggi l'esempio più avanzato di sistema di autoregolamentazione costituito in seno ad una piattaforma di *social network*. Il riferimento è al già citato Facebook Oversight Board, organo indipendente sorto nel 2020 ad iniziativa della stessa Facebook allo scopo di gestire le segnalazioni e i reclami relativi ai contenuti condivisi dagli utenti in violazione delle condizioni d'uso

e degli standard del *social network*[62]. L'analisi di questo organo e della Facebook Oversight Board Charter – ossia lo strumento di *private regulation* che ne disciplina composizione, competenze e poteri – è importante in quanto esso rappresenta un caso paradigmatico[63], che solleva questioni rilevanti anche per piattaforme non dotate di sistemi di autoregolamentazione così avanzati, in particolare in vista dell'entrata in vigore e della futura piena applicabilità del Digital Services Act (sul quale v. *infra*: Cap. 6).

2.1 Facebook Oversight Board: genesi e architettura istituzionale

La genesi del Facebook Oversight Board può farsi risalire ad un'intervista[64] dell'aprile 2018 in cui Mark Zuckerberg, allora alle prese con lo scandalo Cambridge Analytica, aveva per la prima volta parlato del progetto relativo all'istituzione di «*some sort of structure, almost like a Supreme Court that is made up of independent folks who don't work for Facebook, who ultimately make the final judgment call on what should be acceptable speech in a community that reflects the social norms and values of people all around the world*». A questa prima comunicazione è seguito, sette mesi dopo, l'annuncio ufficiale[65] della creazione di un organo indipendente di *governance* e supervisione che si occupasse di fornire pareri in merito alle *policy* del *social network* e di gestire i reclami presentati dagli utenti in materia di contenuti e che, secondo i piani originari, sarebbe dovuto entrare in funzione entro la fine del 2019.

---

[62] In particolare, la Facebook Oversight Board Charter nella propria introduzione parla esplicitamente di «*authenticity, safety, privacy, and dignity*» quali limiti alla libertà di espressione.
[63] In questo senso si veda anche G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, pag. 265.
[64] E. KLEIN, *Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next*, apparso su Vox.com il 2 aprile 2018, disponibile online: https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge, consultato in ultimo il 1° dicembre 2022.
[65] M. ZUCKERBERG, *A Blueprint for Content Governance and Enforcement*, apparso su Facebook il 15 novembre 2018 e disponibile online al seguente indirizzo: https://www.facebook.com/notes/751449002072082/ – ultima modifica del 5 maggio 2021, consultato in ultimo il 1° dicembre 2022.

Sono questi i primi passaggi del percorso[66] che ha portato all'annuncio[67] relativo all'istituzione del Facebook Oversight Board (talvolta indicato in italiano come «Comitato per il controllo di Facebook[68]»), avvenuto il 17 settembre 2019 assieme alla pubblicazione della Oversight Board Charter («Atto Costitutivo» secondo la dicitura italiana riportata sul sito[69] del Board). Quest'ultima, in particolare, è il documento fondamentale che disciplina la costituzione dell'Oversight Board definendone la composizione, i poteri, la *governance* e le procedure, stabilisce le regole per l'esecuzione delle decisioni del Board da parte di Facebook e quelle per apportare modifiche allo stesso Atto Costitutivo. La Charter è composta da sette articoli e, come sottolineato in dottrina, costituisce una «simil-costituzione[70]», che disciplina a livello strutturale i rapporti tra Facebook, l'Oversight Board e il Trust istituito e finanziato da Facebook allo scopo di facilitare la creazione e la gestione del Board.

All'Atto Costitutivo si affiancano una serie di altri documenti che, tenendo per buona la qualifica di «simil-costituzione» assegnata allo stesso, potremmo definire di rango «simil-primario» e che attuano diversi principi contenuti nella Charter. Si tratta, innanzi tutto, degli Statuti («By-laws» in inglese) e dei

---

[66] Per approfondire si veda in particolare: C. KLONICK, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, in Yale Law Journal, Vol. 129, n. 8, pp. 2418-2499, 2020.

[67] B. HARRIS, *Establishing Structure and Governance for an Independent Oversight Board*, apparso su Facebook newsroom il 17 settembre 2019, disponibile online al seguente link: https://about.fb.com/news/2019/09/oversight-board-structure/, consultato in ultimo il 1° dicembre 2022.

[68] Si veda in particolare: G.C. FERONI, *L'Oversight Board di Facebook: il controllo dei contenuti tra procedure private e norme pubbliche*, Key4Biz, 16 febbraio 2021, disponibile sul sito del Garante per la protezione dei dati personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9542545, consultato in ultimo il il 1° dicembre 2022.

[69] Il documento è consultabile sul sito dell'Oversight Board al seguente link: https://www.oversightboard.com/governance/.

[70] L'espressione ricalca la formula «costitution-like document» utilizzata in dottrina per descrivere il documento. A questo proposito si vedano: C. KLONICK, *op. cit.* n. 66, p. 2457; F. BASSAN, *op. cit.* Cap, 4, n. 3, p. 98.

codici di condotta adottati dei componenti del Board che disciplinano, rispettivamente, le procedure operative dello stesso organo e i comportamenti cui sono tenuti i relativi membri. L'architettura istituzionale è poi completata da altri strumenti di diritto privato, tra cui riveste un'importanza primaria l'atto istitutivo del Trust («Trust Agreement»). Nello svolgimento del proprio mandato, il Trust ha poi costituito, attraverso un apposito atto denominato «LLC Agreement», la società Oversight Board LLC, in cui è incorporato il Board. I rapporti tra questa società e Facebook sono regolati attraverso un apposito contratto di prestazione di servizi («Facebook-LLC Service Provider Contract»).

Da questa breve ricapitolazione si intuisce come l'Oversight Board sia stato concepito in modo da realizzare un sistema a forte connotazione istituzionale, con funzioni effettivamente analoghe a quelle di una sorta di «Corte Suprema», che saranno esaminate a breve. Carattere peculiare di tale organo è inoltre la sua indipendenza dal *social network*, nelle intenzioni dei suoi creatori[71] garantita innanzi tutto dalla circostanza per cui lo stesso non appartenga formalmente a Facebook ma, come visto, ad un Trust da questa separato. L'indipendenza del Board sarebbe inoltre assicurata dai requisiti di competenza – in particolare in materia di contenuti e *governance* digitali, libertà di espressione, dibattito politico, sicurezza, *privacy* e tecnologia – e di assenza di conflitti di interessi previsti dall'art. 1 della Charter per gli aspiranti membri dello stesso. Sempre in quest'ottica, inoltre, l'Atto Costitutivo dispone che i componenti del Board – previsti in un numero non inferiore a undici e non superiore

[71] B. HARRIS, *op. cit.* n. 67. In particolare, nello scritto si legge: «Governance: The majority of people we consulted supported our decision to establish an independent trust. They felt that this could help ensure the board's independence, while also providing a means to provide additional accountability checks. The trust will provide the infrastructure to support and compensate the Board».

a quaranta – siano selezionati attraverso un procedimento speciale che permetta di ridurre, per quanto possibile, l'influenza di Facebook sul punto[72].

2.2 I poteri e l'efficacia delle decisioni del Facebook Oversight Board

Effettuata questa breve digressione sulla genesi dell'Oversight Board e sugli strumenti che ne informano la dimensione istituzionale, ci concentriamo adesso sul contenuto di tali strumenti e quindi, in buona sostanza, sui poteri dello stesso Board e sull'efficacia delle sue decisioni nei confronti di Facebook. L'analisi che ci si appresta a svolgere, certamente non esaustiva, riguarderà in particolare la Charter, rimandando invece ad altre sedi[73] per approfondimenti sugli altri strumenti poc'anzi richiamati.

Come già accennato, la Charter si compone di sette articoli, ciascuno dei quali suddiviso a propria volta in punti. Cominciando dall'art. 1, esso stabilisce la composizione del Board, il numero di membri, i requisiti per poterne far parte (v. *supra* par. 2.1) e ne definisce i poteri in relazione ai «contenuti presentati correttamente allo stesso per l'analisi». A tal proposito, è il successivo art. 2 a chiarire come sia gli utenti (definiti «le persone che usano Facebook») che la stessa Facebook possano sottoporre dei contenuti all'esame del Board. In particolare, quest'ultima norma prevede che sia l'utente che abbia originariamente condiviso il contenuto su Facebook sia altre persone che abbiano in precedenza sottoposto tale contenuto all'esame di Facebook (tramite la c.d. «segnalazione»), possano rivolgersi al Board nel caso in cui non siano d'accordo con una decisione presa da Facebook e a condizione che abbiano esaurito i ricorsi interni messi a disposizione dalla stessa piattaforma. Per quanto riguarda Facebook, essa può sottoporre richieste di analisi al Comitato relative

[72] C. KLONICK, *op. cit.* n. 66, p. 2460.
[73] Idem per approfondire *ex multis*.

al trattamento dei contenuti, anche nei casi in cui ritenga che «un contenuto non debba necessariamente essere rimosso del tutto».

Tornando all'art. 1 e all'analisi dei poteri del Board, importante ai nostri fini è il potere «interpretare gli Standard della community di Facebook e le altre normative rilevanti (definite collettivamente "normative sui contenuti") alla luce dei valori articolati di Facebook[74]». A questo si aggiunge il potere di emettere decisioni vincolanti nei confronti di Facebook, che possono essere di due tipi: indicare a Facebook di consentire o rimuovere contenuti e indicargli di confermare o annullare una decisione già oggetto di esecuzione. Altri due poteri del Board, strettamente collegati a quelli appena richiamati, sono, infine, quello di richiedere a Facebook di fornire le informazioni ragionevolmente necessarie per le proprie deliberazioni in modo tempestivo e trasparente e quello di emettere rapidamente spiegazioni scritte sulle proprie decisioni.

Da questa breve ricognizione emerge quindi un sistema a doppio binario, in cui il Board si trova, nell'ambito dell'ordinamento di *private regulation* di cui è supervisore, sia a ricoprire il ruolo di giudice di ultima istanza[75] sia a svolgere una funzione sostanzialmente «nomofilattica» in relazione alle norme applicabili nel predetto ordinamento. È il caso di osservare come si tratti di funzioni che, negli ordinamenti giuridici tradizionali, sono per lo più tipiche delle corti supreme, il che vale a confermare la natura di simil-Corte suprema[76] (potremmo dire noi di «Corte suprema privata») dell'Oversight Board. Va altresì sottolineato come la circostanza per cui i poteri decisionali e nomofilattici del

[74] FOB Charter, art. 1, punto 4.

[75] Si veda in particolare: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 267, il quale sostiene come l'Oversight Boart costituisca uno dei primi esempi di meccanismi privati di applicazione del principio di *judicial review*, ricondotto da certa dottrina tra i principi di cui all'art. 38, lett. c) dello Statuto della Corte internazionale di giustizia.

[76] In questo senso si vedano: C. KLONICK, *op. cit.* n. 66, p. 2450; G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 267; P. BONINI, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in Federalismi.it, n. 11, pp. 265-281, 2020.

Board riguardino essenzialmente le norme di *private regulation*, stabilite da Facebook e vigenti all'interno della piattaforma, contribuisca in maniera sostanziale a rafforzare la «dimensione istituzionale» del *social network*, dotando lo stesso di una sorta di architettura simil-costituzionale, già teorizzata in dottrina[77] ma rimasta nella pratica inedita sino alla pubblicazione dell'Oversight Board Charter.

Nel quadro della nostra indagine, tralasciando le disposizioni relative alle procedure di analisi dei reclami presentati al Board[78], è bene inoltre soffermarsi sul valore delle decisioni e dei pareri emessi dallo stesso.

Si è già detto, in particolare, che il Comitato ha il potere di emettere decisioni «vincolanti» nei confronti di Facebook. Si aggiunge ora che, ai sensi dell'art. 2 della Charter, le decisioni in questione hanno valore di «precedente» e dovrebbero essere considerate «altamente persuasiv[e]» nell'ipotesi di fattispecie simili portate all'attenzione della Corte. Si tratta di un'evidente eco dei sistemi di Common Law, che vale peraltro a rafforzare in maniera notevole il ruolo del Comitato. Per quanto riguarda l'esecuzione di tali decisioni, l'art. 4 prevede che Facebook debba attuarle tempestivamente a meno che «l'attuazione di una risoluzione possa violare la legge» (su questo aspetto v. *infra*: par. 2.3). La stessa norma, anche in virtù dello *stare decisis* di cui si è appena detto, dispone che nei casi in cui Facebook noti che un contenuto identico a uno su cui il Board si sia già pronunciato continui ad essere presente sulla piattaforma, debba agire analizzando se sia tecnicamente e operativamente possibile applicare la decisione del Comitato anche a quel contenuto.

---

[77] V. *ex multis*: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 268; C. KLONICK, *op. cit.* n. 66, p. 2477; A. CHANDER, *Facebookistan*, in Southern California Law Review, Vol. 86, n. 1, pp. 1808-1842 – UC Davis Legal Studies Research Paper Series, Research Paper No. 295, 2012, disponibile su SSRN: http://ssrn.com/abstract=2061300.

[78] La norma della Charter al riguardo rilevante è l'art. 3. Per approfondire si vedano *ex multis*: C. KLONICK, *op. cit.* n. 66, p. 2464; G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 268.

Detto del carattere vincolante delle decisioni del Comitato, occorre aggiungere come tale carattere non sia, peraltro, proprio di tutte le pronunce dello stesso, in quanto fanno eccezione quelle contenenti soltanto linee guida o pareri consultivi in merito alle norme di *private regulation* su cui il Board esercita la propria funzione nomofilattica. Si tratta non di decisioni emesse a valle di procedimenti iniziati a seguito di reclami presentati con riguardo a determinate fattispecie – e, quindi, di comandi specifici e concreti – ma di indicazioni a valenza generale fornite su richiesta di Facebook. Per queste pronunce è stata preferita una soluzione fondata non sull'autorità del Board ma sulla sua forza persuasiva e sulla sua influenza indiretta sull'attività regolatoria di Facebook, in capo al quale sono comunque posti degli obblighi di trasparenza. In particolare, l'art. 4 della Charter richiede a Facebook soltanto di intraprendere, a seguito dell'emissione di un parere o di linee guida da parte del Board, ulteriori azioni «analizzando le procedure operative necessarie per attuare le indicazioni del Comitato, considerandole nel processo formale di sviluppo delle proprie regole e comunicando in modo trasparente le azioni intraprese di conseguenza».

2.3 Il riconoscimento dei limiti del diritto di fonte pubblica nell'Oversight Board Charter

Continuando, per quanto qui di interesse, con l'analisi della Oversight Board Charter, occorre adesso soffermarsi sugli intrecci tra questa e il diritto di fonte pubblica. A tal proposito, si è già avuto modo di notare come l'intero sistema dell'Oversight Board si basi su strumenti di diritto privato, come tali disciplinati da norme di fonte pubblica e a proposito dei quali si pongono anche questioni internazionalprivatistiche già esaminate (v. *supra*: par. 2.1, Cap. 3). Non è però di questi aspetti che ci si occuperà adesso, in quanto ci si concentrerà piuttosto sull'influenza del diritto di fonte pubblica e sui limiti dallo stesso

posti all'attività dell'Oversight Board. Infatti, la Charter riconosce in più occasioni il diritto di fonte pubblica quale limite ai poteri ed alle attività del Board, ammettendo come il sistema di *private regulation* a cui il Comitato è preposto non possa essere considerato come totalmente avulso dalla realtà giuridica del mondo fisico ma debba, al contrario, rapportarcisi.

Venendo all'analisi delle disposizioni ai nostri fini rilevanti, occorre innanzi tutto richiamare il già citato art. 2 (v. *supra*, par. 2.2), ai sensi del quale il Board decide le questioni sottoposte alla propria attenzione sulla base delle regole di Facebook. La stessa norma, tuttavia, al punto 2 chiarisce come, nel prendere una decisione, il Comitato dovrà porre particolare attenzione all'impatto della rimozione dei contenuti oggetto della pronuncia, «alla luce delle norme sui diritti umani che proteggono la libertà di espressione». In altre parole, la Charter richiede al Board di prendere in considerazione queste ultime norme di fonte pubblica in fase decisionale, pur dovendosi esso pronunciare sulla base delle regole private di Facebook. Altri limiti discendono dal già citato art. 4 (v. *infra*: par. 2.2) ed in particolare dal passaggio secondo cui Facebook è obbligata all'esecuzione delle decisioni del Board, a meno che la suddetta esecuzione possa «violare la legge».

Rilevante ai nostri fini è poi l'art. 7 dell'Atto Costitutivo, rubricato proprio «Compliance with law». Tale norma dispone, per prima cosa, che nulla della Charter o di altri documenti che compongono il sistema giuridico del Board possa essere interpretato in maniera da «comportare una violazione della legge da parte di Facebook, del trust, del comitato o di qualsiasi altra entità associata». Si tratta, quindi, di un limite cha riguarda anche l'attività nomofilattica del Board, oltre che quella decisionale. Lo stesso articolo chiude poi affermando che «il comitato non pretenderà di applicare la legge locale», con ciò

chiarendo che tra i compiti del Board non rientra quello di decidere controversie regolate (esclusivamente) dal diritto di fonte pubblica e non dalle regole private di Facebook.

I limiti in questione appaiono in realtà piuttosto ampi e non di semplicissimo inquadramento. Da una prima lettura delle disposizioni appena richiamate sembrerebbe, infatti, che la Charter consideri le regole private di Facebook generalmente subordinate al diritto di fonte pubblica. Il rischio di violazioni di quest'ultimo, in particolare, non consentirebbe di eseguire decisioni assunte dal Board sulla base delle norme del *social network*, anche nel caso in cui queste, in ipotesi, legittimassero condotte vietate da quelle di fonte pubblica (v. *supra* par. 1.1). Simili motivi, come si è visto, proibirebbero inoltre al Board di interpretare le regole della Charter e degli altri documenti ad essa collegati in maniera difforme rispetto alla legge, influendo quindi anche sulla funzione nomofilattica del Comitato oltre che su quella decisionale.

Gli aspetti problematici sorgono, tuttavia, nel provare a delineare i confini esatti dei suddetti limiti. A questo proposito, se è vero che lo stesso art. 7 chiarisce come tra i compiti del Board non rientri quello di «applicare la legge locale», è anche vero che l'art. 2, si è notato, imponga allo stesso Comitato di prendere in considerazione alcune disposizioni di fonte pubblica a tutela dei «diritti umani» e della «libertà di espressione». È chiaro quindi come, avendo a riguardo questa disposizione, il diritto di fonte pubblica finisca per ricoprire comunque un ruolo ai fini delle decisioni e dei pareri del Board.

Altre criticità sorgono dalla circostanza, già ampiamente discussa nel presente lavoro, per cui l'ambiente del *social network* sia lambito da molteplici diritti di fonte pubblica, facenti capo ad ordinamenti giuridici diversi, ciascuno

dei quali desideroso di estendere la propria sovranità sulla rete[79]. Da ciò conseguirebbe infatti che, laddove la Charter faccia riferimento genericamente alla «legge», occorrerebbe in realtà considerare che una stessa condotta possa essere vietata dal diritto di un ordinamento giuridico e, allo stesso tempo, essere perfettamente legittima ai sensi del diritto di un diverso ordinamento. In altre parole, a seconda della fattispecie considerata, sarebbe necessario determinare *ex ante* la legge ad essa applicabile per poi valutare la conformità alla stessa delle decisioni o delle interpretazioni fornite dal Board. Non sembra, peraltro, che gli estensori della Charter abbiamo tenuto in debita considerazione la problematica, posto che l'unica disposizione che sembra tangenzialmente occuparsene è l'art. 7 nel passaggio in cui si riferisce all'assenza, in capo al Board, di pretese di applicare la «legge locale».

Al contrario, infatti, in una delle interviste già citate[80], Mark Zuckerberg aveva chiarito come l'obiettivo della sua iniziativa fosse quello di stabilire un organo indipendente che fungesse da giudice di ultima istanza «on what should be acceptable speech in a community that reflects the social norms and values of people all around the world». Come evidenziato in dottrina[81], il fondatore di Facebook sembrava quindi alludere ad un insieme di norme e valori universali che, tuttavia, a livello globale semplicemente non esiste. Invece, le soli norme uniformi per gli utenti di Facebook sarebbero proprio le regole della piattaforma, le quali devono però confrontarsi con un numero indefinito di diritti di fonte pubblica. È chiaro quindi che, da questo punto di vista, l'obiettivo indicato da Mark Zuckerberg appare chimerico.

Nonostante le menzionate criticità, l'iniziativa dell'Oversight Board resta comunque importante in quanto costituisce un interessante tentativo di stabilire

[79] Sul punto si veda C. KLONICK, *op. cit.* n. 66, p. 2474.
[80] E. KLEIN, *op. cit.* n. 64.
[81] C. KLONICK, *op. cit.* n. 66, p. 2474.

una autorità indipendente – pur con le perplessità a tal proposito rilevate in dottrina[82] – cui gli utenti di una piattaforma possano presentare i propri reclami e, in generale, di «costituzionalizzare[83]» il sistema di *private regulation* sotteso ad una piattaforma digitale. Da questo punto di vista, i plurimi riferimenti alla legge e l'enfasi posta dalla Charter sulla trasparenza segnalano, se non altro, la possibilità che tale iniziativa possa rappresentare un punto di partenza ed un modello di cooperazione tra regolatori pubblici e privati nell'ambito delle piattaforme[84]. A questo proposito, peraltro, è opportuno dare conto di quella dottrina[85] secondo cui le norme della Charter – pensate, come visto, per riflettere valori invocati come «universali» – non siano in realtà neutre ma sembrino, al contrario, riflettere valori tipici dell'ordinamento statunitense, in quanto collocherebbero la libertà di espressione in una posizione di primazia rispetto a beni e valori quali sicurezza, *privacy*, decoro e autenticità[86].

2.4 Un esempio pratico di pronuncia del Board: la decisione sulla sospensione del profilo di Donald Trump (cenni)

A conclusione di questo breve approfondimento sull'Oversight Board, pare opportuno ai nostri fini dare conto, senza pretesa di esaustività[87], di una della

---

[82] V. *ex multis*: C. KLONICK, *op. cit.* n. 66, p. 2481; F. BASSAN, *op. cit.* Cap, 4, n. 3, p. 99; G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 267.
[83] V. dottrina cit. sub nota 70.
[84] C. KLONICK, *op. cit.* n. 66, p. 2474.
[85] Idem, p. 2475.
[86] FOB Charter, introduzione, cit. sub nota 62.
[87] Per approfondire si rimanda a: F. PAOLUCCI, *L'Oversight Board di Facebook conferma la sospensione degli account di Trump*, apparso su Iusinitinere.it il 5 maggio 2021, disponibile online: https://www.iusinitinere.it/loversight-board-di-facebook-conferma-la-sospensione-degli-account-di-trump-38521; O. POLLICINO, M. BASSINI, G. DE GREGORIO, *Trump's Indefinite Ban – Shifting the Facebook Oversight Board away from the First Amendment Doctrine*, apparso su Verfassungsblog.de, l'11 maggio 2021, disponibile online: https://verfassungsblog.de/fob-trump-2/; A. GEROSA, *La tutela della libertà di manifestazione del pensiero nella rete tra Independent Oversight Board e ruolo dei pubblici poteri. Commenti a margine della decisione n. 2021-001-FB-FBR*, in Forum di Quaderni Costituzionali, fasc. 2, pp. 427-440, 2021, disponibile online: https://www.forumcostituzionale.it/wordpress/?p=16395.

più note decisioni emesse dal Comitato sin dalla sua fondazione. Si tratta, in particolare, della decisione[88] relativa alla sospensione degli account dell'ex presidente degli Stati Uniti Donald Trump, decisa da Facebook il 7 gennaio 2021 a seguito degli assalti a Capitol Hill del giorno precedente[89], su cui i contenuti e i messaggi condivisi su Facebook dall'allora inquilino della Casa Bianca avevano avuto un'influenza decisiva.

Ai nostri fini, preme in particolare evidenziare come il Comitato, nel giungere alla propria decisione, abbia più volte fatto riferimento al «diritto internazionale», ai «diritti umani» e al «diritto umanitario» allo scopo di definire i limiti entro cui le regole di Facebook possano limitare la libertà di espressione a tutela di valori riconosciuti e tutelati da strumenti appartenenti ai predetti ambiti del diritto di fonte pubblica. Un accenno è stato fatto anche al Primo Emendamento della Costituzione degli Stati Uniti, seppure lo stesso non sia stato incluso esplicitamente tra gli standard in materia di diritti umani considerati dal Board per effettuare le proprie valutazioni[90].

---

[88] FOB, Decisione 2021-001-FB-FBR, *Sospensione dell'ex Presidente degli Stati Uniti Trump*, accessibile online: https://www.oversightboard.com/decision/FB-691QAMHJ, consultata in ultimo il 7 dicembre 2022.

[89] Per approfondire i fatti v. nota 10

[90] Idem, si veda in particolare il par. 4 («Relevant standards»), punto III. («Human rights standards»), ove, oltre agli United Nations Guiding Principles on Business and Human Rights (UNGPs), sono elencati testualmente: «[…] The right to freedom of expression: International Covenant on Civil and Political Rights (ICCPR), Articles 19 and 20; as interpreted in General Comment No. 34, Human Rights Committee (2011) (General Comment 34); the Rabat Plan of Action, OHCHR, (2012); UN Special Rapporteur on freedom of opinion and expression report A/HRC/38/35 (2018); Joint Statement of international freedom of expression monitors on COVID-19 (March, 2020). […] The right to life: ICCPR Article 6. […] The right to security of person: ICCPR Article 9, para. 1. […] The right to non-discrimination: ICCPR Articles 2 and 26; International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), Articles 1 and 4. […] Participation in public affairs and the right to vote: ICCPR Article 25. […] The right to remedy: ICCPR Article 2; General Comment No. 31, Human Rights Committee (2004) (General Comment 31); UNGPs, Principle 22».

Quanto al merito della decisione, è opportuno segnalare come il Board abbia ritenuto giustificata la decisione di Facebook di sospendere l'account del *tycoon*. Tuttavia, il Comitato ha aggiunto che la sanzione formalmente comminata da Facebook, ossia la «sospensione a tempo indeterminato», non fosse corretta in quanto non rientrante tra le sanzioni previste dalle regole del *social network*. Pertanto, il Comitato ha assegnato a Facebook un termine di sei mesi per riesaminare la questione ed irrogare una diversa sanzione in linea con quelle applicabili a tutti gli utenti della piattaforma. Inoltre, anche facendo leva sul principio di trasparenza che abbiamo visto essere presente nella Charter (v. *supra*: par. 2.2, 2.3) e che il Board ha ritenuto violato da parte di Facebook nel caso di specie, il Comitato ha formulato una serie di raccomandazioni alla piattaforma, da implementare «sviluppando normative chiare, necessarie e proporzionate che promuovano la sicurezza pubblica e il rispetto della libertà di espressione[91]».

[91] Idem, v. in particolare il riepilogo del caso per il virgolettato e per una sintesi delle raccomandazioni del Board.

Capitolo 6 – Ultimi sviluppi e prospettive future: il Digital Services Act europeo

SOMMARIO: 1 Il Digital Services Act: genesi, obiettivi e struttura del regolamento. – 2. Ambito di applicazione del regolamento: un approccio unilateralista. – 2.1 I «servizi intermediari» disciplinati dal Digital Services Act e le nozioni di «piattaforma online» e «motore di ricerca». – 2.2 Ambito di applicazione territoriale: tra «*targeting approach*» e necessità di un «collegamento sostanziale» con l'Unione. – 3 La responsabilità degli intermediari nel Digital Services Act: conferme ed evoluzioni rispetto alla Direttiva e-Commerce. – 4 I doveri di diligenza dei *provider*: tra approccio «a strati», trasparenza e *private regulation*. – 4.1 Gli obblighi relativi alle «condizioni generali» e alla trasparenza applicabili a tutti i *provider*. – 4.2 Gli obblighi applicabili agli *hosting provider* (piattaforme incluse): i sistemi di «*notice and action*». – 4.3 Gli obblighi per le piattaforme online: tra dimensione istituzionale, autoregolamentazione e trasparenza. – 4.3.1 La gestione dei reclami interni alle piattaforme e gli strumenti di risoluzione extragiudiziale delle controversie. – 4.3.2 Il rafforzamento dei doveri di trasparenza e dell'accountability delle piattaforme. – 4.3.3 Gli obblighi supplementari a carico dei fornitori di piattaforme online di dimensioni molto grandi. – 4.4 La promozione di strumenti di autoregolamentazione e coregolamentazione: standard di settore, codici di condotta, protocolli di crisi. – 5 Attuazione, cooperazione, sanzioni, esecuzione (cenni).

1 Il Digital Services Act: genesi, obiettivi e struttura del regolamento

A conclusione della nostra indagine, e con uno sguardo inevitabilmente rivolto al futuro, ci si occuperà in questo ultimo capitolo del Digital Services

Act[1] (talvolta anche abbreviato in «DSA»), il più volte citato nuovo regolamento dell'Unione europea sui servizi digitali (v. *supra* Cap. 1, par. 4).

L'analisi di questo strumento è per noi rilevante in quanto lo stesso, piuttosto che costituire di per sé una rivoluzione[2], sviluppa ulteriormente le tendenze relative alle strategie regolatorie dell'Unione europea in materia di piattaforme digitali esaminate nel presente lavoro. Nelle pagine successive si cercherà quindi di mostrare[3] come il nuovo regolamento contribuisca a rafforzare le evidenze da noi raccolte, sia dal punto di vista del diritto materiale che di quello internazionalprivatista, oltre che per ciò che riguarda il rapporto tra regolamentazione di fonte pubblica e di fonte privata nell'ambito delle piattaforme digitali.

Come già notato, il percorso di approvazione del Digital Services Act aveva preso l'avvio dalla proposta legislativa presentata dalla Commissione europea nel dicembre 2020, contenuta nel «pacchetto sui servizi digitali» («Digital Services Act Package»). Questa proposta si basava, in particolare, sui principi fondamentali della Direttiva e-Commerce – che erano nell'occasione stati ritenuti

---

[1] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (Testo rilevante ai fini del SEE), apparso in *GU L 277 del 27.10.2022, pagg. 1-102.*

[2] In questo senso v. G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 263.

[3] Tra i commenti relativi alla proposta ed al testo definitivo del regolamento si vedano *ex multis*: H. RICHTER, M. STRAUB, E. TUCHTFELD (a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021, disponibile su SSRN: https://ssrn.com/abstract=3932809; C. CAUFFMAN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in European Journal of Risk Regulation, Vol. 12, n. 4, pp. 758-774, 2021; I. BURI, J. VAN HOBOKEN, *The Digital Services Act (DSA) Proposal: A Critical Overview*, DSA Observatory – Discussion paper, 28 ottobre 2021; T. RODRÍGUEZ DE LAS HERAS BALLELL, *The background of the Digital Services Act: Looking Towards a Platform Economy*, in ERA Forum, Vol. 22, n. 1, pp. 75-86, 2021; S.F. SCHWEMER, *Liability Exemptions of Non-hosting Intermediaries: Sideshow in the Digital Services Act?*, in Oslo Law Review, Vol. 8, n. 1, pp. 4-29, 2021; A.R. LODDER, J. MORAIS CARVALHO, *Online Platforms: Towards an Information Tsunami with New Requirements on Moderation, Ranking, and Traceability*, in European Business Law, Vol. 33, n. 4, pp. 537-556, 2022.

validi dall'Esecutivo, pur proponendo lo stesso la revisione della richiamata direttiva – e sugli obiettivi già anticipati nella comunicazione «Plasmare il futuro digitale dell'Europa[4]». Dopo il raggiungimento dell'accordo politico provvisorio[5] nell'aprile 2022, il testo finale del DSA è stato, quindi, approvato dai colegislatori il 19 ottobre 2022 ed è entrato in vigore il successivo 16 novembre[6]. Tuttavia, con poche eccezioni[7], esso non sarà applicabile prima del 17 febbraio 2024[8].

Obiettivo dichiarato del Digital Services Act è quello di contribuire al corretto funzionamento del mercato interno dei «servizi intermediari» *online* (sulla cui nozione v. *infra*: par. 2), stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile, che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta di Nizza siano tutelati in modo effettivo[9], contrastando la diffusione di contenuti illegali online e i rischi per la società che la diffusione della disinformazione o di altri contenuti può generare[10].

[4] COM(2020) 67 final, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Plasmare il futuro digitale dell'Europa*, 19 febbraio 2020.
[5] V. sub. nota 43, Cap. 5.
[6] Ai sensi dell'art. 93 il Digital Services Act è entrato in vigore venti giorni dopo la sua pubblicazione sulla Gazzetta ufficiale dell'Unione, avvenuta il 27 ottobre 2022 (GU L 277 del 27.10.2022, pagg. 1-102).
[7] Si veda a questo proposito l'art. 92 DSA, secondo cui: «Il presente regolamento si applica ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi designati a norma dell'articolo 33, paragrafo 4, a decorrere da quattro mesi dalla notifica al fornitore interessato di cui all'articolo 33, paragrafo 6, qualora tale data sia anteriore al 17 febbraio 2024». Si veda altresì l'art. 93, par. 2 DSA, secondo cui «[…] l'articolo 24, paragrafi 2, 3 e 6, l'articolo 33, paragrafi da 3 a 6, l'articolo 37, paragrafo 7, l'articolo 40, paragrafo 13, l'articolo 43 e il capo IV, sezioni 4, 5 e 6, si applicano a decorrere dal 16 novembre 2022».
[8] Art. 93, par. 2 DSA.
[9] Art. 1, par. 1 DSA.
[10] Considerando 10 DSA.

A tal fine, il regolamento si muove in una triplice direzione[11]. In primo luogo, esso interviene modificando e aggiornando la disciplina relativa alla responsabilità degli *internet service provider* di cui alla Direttiva e-Commerce (v. *supra*: Cap. 2, par. 2.1 e 2.2; v. *infra*: par. 3). In secondo luogo, il DSA impone specifici obblighi di diligenza, trasparenza e «*accountability*» in capo ai «prestatori di servizi intermediari», variamente gradati a seconda delle diverse categorie di *provider* individuate dal regolamento (v. *infra*: par. 4). Infine, il regolamento stabilisce un sistema di norme relative alla propria attuazione ed esecuzione prevedendo, a tal fine, dei meccanismi di cooperazione e coordinamento tra le «autorità competenti[12]» appositamente designate dagli Stati membri, nonché tra queste e i *provider*[13] (v. *infra*, par. 5).

Gli obiettivi del legislatore si riflettono sulla struttura stessa del Digital Services Act. In particolare, il regolamento si compone di cinque capi. Il Capo I contiene le disposizioni generali, il Capo II le norme relative alla responsabilità dei prestatori di servizi intermediari, il Capo III gli obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro, il Capo IV le norme sull'attuazione, la cooperazione, le sanzioni e l'esecuzione del regolamento, il Capo V le disposizioni finali.

2 Ambito di applicazione del regolamento: un approccio unilateralista

Iniziando con l'analisi delle disposizioni per noi rilevanti, occorre subito notare come, al pari di altri strumenti esaminati nel corso del precedente lavoro (v. Cap. 3, par. 5), anche il Digital Services Act contenga al proprio interno una

[11] Art. 1, par. 2 DSA.

[12] V. art. 49 DSA: «[…] Gli Stati membri designano una o più autorità competenti incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del presente regolamento ("autorità competenti")».

[13] In questo senso S. PELLERITI, *La governance privata di Facebook e la presa di coscienza del regolatore europeo: qualcosa sta cambiando?*, in Rivista della Regolazione dei mercati, fasc. 2, pp. 429-444, 2021. V. in particolare p. 441.

norma di chiara impostazione unilateralista, che ne determina autonomamente la «gittata» prescindendo dalle norme di conflitto. Si tratta, in particolare, dell'art. 2, che riguarda sia l'ambito di applicazione materiale che quello territoriale del regolamento.

A tal fine, la norma dispone, al par. 1, che il regolamento «si applica ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari[14]». Il par. 2 aggiunge, quindi, che il regolamento «non si applica ai servizi che non sono servizi intermediari né alle prescrizioni imposte in relazione a tali servizi, indipendentemente dal fatto che i servizi siano prestati facendo ricorso a servizi intermediari».

2.1 I «servizi intermediari» disciplinati dal Digital Services Act e le nozioni di «piattaforma online» e «motore di ricerca»

Per quanto riguarda l'ambito di applicazione materiale, centrale è l'aspetto relativo alla nozione di «servizi intermediari» richiamati dall'art. 2.

Si stratta, secondo la definizione[15] fornita dal regolamento, dei medesimi servizi della società dell'informazione di semplice trasporto («*mere conduit*»), memorizzazione temporanea («*caching*») e memorizzazione di informazioni («*hosting*») considerati dalla Direttiva e-Commerce (v. *supra*: Cap. 2, par. 2.1). Solo questi servizi ricadono, quindi, nella gittata del Digital Services Act, rimanendo di contro esclusi quelli di altro genere. Di conseguenza, per definire la portata del nuovo regolamento assumono un'importanza decisiva le questioni qualificatorie da noi già esaminate (v. *supra*: Cap. 2, par. 4).

[14] Art. 2, par. 1 DSA.

[15] V. art. 3, lett. g) DSA per la definizione di «servizio intermediario» rilevante ai fini del Digital Services Act.

A tal proposito, occorre sottolineare come il considerando 6 DSA specifichi che il regolamento non riguarda i «servizi che possono o non possono essere prestati per via elettronica, come servizi di trasporto ricettivi o di consegna» e che, in pratica, vengono forniti *online* grazie all'intermediazione dei prestatori di servizi intermediari. Si tratta di quelli che altrove abbiamo definito come «servizi sottostanti» (v. *supra*: Cap. 2, par. 4), che rimangono quindi al di fuori del perimetro del regolamento. Il medesimo considerando aggiunge, inoltre, che il Digital Services Act non si applica nemmeno a «quelle situazioni nelle quali il servizio intermediario costituisce parte integrante di un altro servizio che non è un servizio intermediario come riconosciuto dalla giurisprudenza della Corte di giustizia dell'Unione europea». Si tratta di un chiaro riferimento alle pronunce relative ai casi *Uber* e *Airbnb* (v. *supra*: Cap. 2, par. 4), da cui si ricava che soltanto i servizi offerti dal secondo rientrerebbero nella gittata del nuovo regolamento[16].

Un altro aspetto che preme qui evidenziare – e che costituisce un'innovazione rispetto al regime della Direttiva e-Commerce – è quello per cui il nuovo regolamento introduce all'interno dell'ordinamento giuridico dell'Unione due definizioni relative a due categorie di «servizi intermediari» che rivestono un'importanza sempre più crescente nell'economia digitale. Si tratta, in particolare, delle nozioni di «piattaforma online» e di «motore di ricerca online». Queste due nozioni, come si è avuto modo di constatare (v. *supra*: Cap. 2, par. 3.1), erano già state utilizzate dal legislatore nell'ambito di altri strumenti come il Regolamento P2B senza che, tuttavia, fossero mai state fornite delle definizioni di esse. Colmando le lacune in questione, il Digital Services Act definisce innanzi tutto la «piattaforma online» come una speciale categoria di *hosting provider* che, su richiesta di un destinatario del servizio, «memorizza e

[16] C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 764.

diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento[17]». Il «motore di ricerca online» è invece definito come «un servizio intermediario che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto[18]».

Le definizioni in questione sono particolarmente importanti in quanto, oltre a colmare le lacune sistemiche di cui si è detto, il Digital Services Act, come vedremo meglio a breve (v. *infra*: par. 4), disciplina gli obblighi dei vari prestatori di servizi intermediari utilizzando un approccio «a strati[19]» e ponendo in capo ai fornitori di piattaforme online e dei motori di ricerca obblighi più penetranti rispetto a quelli previsti per gli altri intermediari. Doveri ancora più incisivi sono poi posti in capo ai fornitori di piattaforme o di motori di ricerca «di dimensioni molto grandi[20]», ossia che hanno un numero medio mensile di destinatari attivi dei servizi[21] da essi forniti nell'Unione pari o superiore a 45

---

[17] Art. 3, lett. i) DSA.
[18] Art. 3, lett. j) DSA.
[19] In questo senso si veda: T.A. MADIEGA, *Digital Services Act*, EPRS – European Parliamentary Research Service, PE 689.357, novembre 2022, disponibile online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689357. Si veda altresì I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 18, ove si parla di «*tiered approach*».
[20] Art. 33 DSA.
[21] Per le definizioni di «destinatario del servizio», «destinatario attivo di una piattaforma online» e «destinatario attivo di un motore di ricerca online» si vedano, rispettivamente: art. 3, lett. b), p), q) DSA.

milioni e che siano stati designati come tali dalla Commissione europea secondo quanto previsto dall'art. 33, par. 4 DSA[22].

2.2 Ambito di applicazione territoriale: tra «*targeting approach*» e necessità di un «collegamento sostanziale» con l'Unione

Con riferimento all'ambito di applicazione territoriale, va notato come l'art. 2, par. 1 DSA faccia utilizzo della già menzionata tecnica del «*targeting approach*» (v. *supra*: Cap. 3, par. 2.4.3, 5.1) e conferisca rilevanza alla circostanza per cui un *provider*, eventualmente anche stabilito in uno Stato terzo[23], offra i propri servizi intermediari a destinatari stabiliti ovvero ubicati all'interno dell'Unione. Da questo punto di vista, la norma ricorda l'art. 3 GDPR (v. Cap. 3, par. 5.1) e, al pari di quest'ultimo, pare configurare una sorta di applicazione extraterritoriale del nuovo regolamento[24].

Inoltre, analogamente allo stesso art. 3 GDPR e ad altre norme di matrice unilateralista già richiamate, l'art. 2 DSA appare, *prima facie*, suscettibile di estendere l'ambito di applicazione del nuovo regolamento in maniera troppo

[22] In particolare, l'art. 33, par. 4 DSA prevede: «La Commissione, previa consultazione dello Stato membro di stabilimento o tenuto conto delle informazioni fornite dal coordinatore dei servizi digitali del luogo di stabilimento a norma dell'articolo 24, paragrafo 4, adotta una decisione che designa come piattaforma online di dimensioni molto grandi o motore di ricerca online di dimensioni molto grandi ai fini del presente regolamento la piattaforma online o il motore di ricerca online con un numero medio mensile di destinatari attivi del servizio pari o superiore al numero di cui al paragrafo 1 del presente articolo [45 milioni]. La Commissione adotta la propria decisione sulla base dei dati comunicati dal fornitore della piattaforma online o del motore di ricerca online a norma dell'articolo 24, paragrafo 2, o delle informazioni richieste a norma dell'articolo 24, paragrafo 3, e di qualsiasi altra informazione a sua disposizione».

[23] A questo proposito, occorre chiarire come, a differenza dell'art. 27 GDPR, l'art. 13 DSA non obblighi ma lasci soltanto la facoltà ai *provider* stabiliti in paesi terzi di designare un proprio rappresentante legale in uno degli Stati membri in cui offrono i propri servizi.

[24] In questo senso si veda: J. VAN HOBOKEN, I. BURI, J.P. QUINTAIS, R. FAHY, N. APPELMAN, *The DSA Has Been Published – Now the Difficult Bit Begins*, apparso su Verfassungsblog.de, il 31 ottobre 2022, disponibile online: https://verfassungsblog.de/dsa-published/.

ampia, dando così luogo al fenomeno del «*regulatory overreaching*». Questo rischio sembra tuttavia mitigato da quanto previsto dai considerando 7 e 8, che merita qui richiamare.

Il primo di essi, in particolare, chiarisce come la circostanza per cui dei prestatori di servizi intermediari offrano servizi nell'Unione debba essere dimostrata da un «collegamento sostanziale» con la stessa Unione. A specificazione del precedente, il considerando 8 DSA afferma come tale collegamento dovrebbe considerarsi presente, oltre che nel caso in cui il *provider* sia stabilito nell'Unione, in due distinte ipotesi.

La prima riguarda la presenza di un numero di destinatari del servizio in uno o più Stati membri «significativo in relazione alla rispettiva popolazione». Non è chiaro, peraltro, cosa si intenda con la suddetta formula e, in attesa di delucidazioni, si può soltanto intuire come l'applicazione del regolamento debba escludersi nei casi in cui un *provider* offra i propri servizi soltanto a un numero esiguo di destinatari stabiliti nell'Unione.

La seconda ipotesi, propria del «*targeting approach*», individua la presenza di un collegamento sostanziale «sulla base dell'orientamento delle attività verso uno o più Stati membri». A tal proposito, il considerando 8 DSA continua con l'elencare una serie di criteri in base ai quali stabilire se un *provider* stia orientando o meno le proprie attività verso uno o più determinati Stati. In particolare, la disposizione afferma come l'orientamento in questione possa essere determinato «sulla base di tutte le circostanze del caso», indicando, a titolo esemplificativo, fattori quali «l'uso di una lingua o di una moneta generalmente utilizzata nello Stato membro in questione, la possibilità di ordinare prodotti o servizi oppure l'utilizzo di un pertinente dominio di primo livello». Continuando con l'elenco, l'orientamento delle attività verso uno Stato membro potrebbe anche desumersi «dalla disponibilità di un'applicazione nell'ap-

posito negozio online (app store) nazionale, dalla fornitura di pubblicità a livello locale o in una lingua usata nello Stato membro in questione o dalla gestione dei rapporti con la clientela, ad esempio la fornitura di assistenza alla clientela in una lingua generalmente parlata in tale Stato membro».

Occorre notare come i criteri appena richiamati ricalchino in parte quelli considerati dalla Corte di Giustizia nella sentenza *Pammer* per stabilire se un professionista diriga o meno le proprie attività verso uno Stato membro ai fini dell'applicazione dei regimi protettivi in materia di consumatori previsti dalle norme dell'Unione sulla competenza giurisdizionale e sulla legge applicabile (v. *supra* Cap. 3, par. 2.4.3, lett. A)). A tal proposito, è significativo il fatto che lo stesso considerando 8 DSA richiami esplicitamente tali regole, affermando come un collegamento sostanziale dovrebbe ritenersi presunto anche quando le attività di un *provider* sono dirette verso uno o più Stati membri ai sensi dell'art. 17, par. 1, lett. c) Regolamento Bruxelles I*bis*[25].

Ricalca ancora le regole di diritto internazionale privato dell'Unione a tutela dei consumatori[26], così come interpretate dalla Corte di Giustizia nella sentenza *Pammer*[27], l'ulteriore specifica del considerando 8 DSA secondo cui «la mera accessibilità tecnica di un sito web dall'Unione non possa, di per sé, essere considerata come costitutiva di un collegamento sostanziale con l'Unione». Un chiarimento anch'esso funzionale ad evitare di estendere in maniera eccessiva l'ambito di applicazione territoriale del nuovo regolamento.

---

[25] Art. 17, par. 1, lett. c) Regolamento Bruxelles I*bis*: «1. Fatto salvo quanto previsto dall'articolo 6 e dall'articolo 7, punto 5, la competenza in materia di contratti conclusi da una persona, il consumatore, per un uso che possa essere considerato estraneo alla sua attività professionale è regolata dalla presente sezione: […] c) in tutti gli altri casi, qualora il contratto sia stato concluso con una persona le cui attività commerciali o professionali si svolgono nello Stato membro in cui è domiciliato il consumatore o sono dirette, con qualsiasi mezzo, verso tale Stato membro o verso una pluralità di Stati che comprende tale Stato membro, purché il contratto rientri nell'ambito di dette attività.

[26] V. in particolare considerando 24 Regolamento Roma I.

[27] CGUE, *Pammer e Alpenhof*, punti 67-73, 94.

Va infine aggiunto come l'art. 2, par. 4, lett. h) affermi che il Digital Services Act non pregiudica, tra le altre[28], le norme del diritto dell'Unione nel settore della cooperazione giudiziaria in materia civile, in particolare il Regolamento Bruxelles I*bis* o qualsiasi atto giuridico dell'Unione che stabilisca norme relative alla legge applicabile alle obbligazioni contrattuali ed extracontrattuali. Quest'ultimo riferimento è, innanzi tutto, ai regolamenti Roma I e II, che sono quindi fatti salvi dal Digital Services Act. Ciò non vale, peraltro, ad escludere la natura unilateralista di quest'ultimo, che dovrebbe applicarsi alle materie e nei casi da esso previsti a prescindere dal funzionamento delle norme di conflitto. Questa affermazione appare sostenuta anche dalla specifica di cui al considerando 10 DSA, il quale chiarisce che, nella misura in cui gli atti giuridici dell'Unione fatti salvi dal Digital Services Act perseguono i medesimi obiettivi dello stesso, le norme del nuovo regolamento «si dovrebbero applicare in relazione alle questioni che non sono affrontate o non sono pienamente affrontate da tali altri atti giuridici».

3 La responsabilità degli intermediari nel Digital Services Act: conferme ed evoluzioni rispetto alla Direttiva e-Commerce

Venendo all'analisi delle norme materiali del Digital Services Act, occorre partire da quelle relative alla responsabilità dei prestatori di servizi intermediari per le informazioni fornite dai propri utenti (definiti «destinatari del servizio[29]» dall'art. 2, lett. b) DSA). Come abbiamo già visto, la materia era stata per la prima volta disciplinata dalla Direttiva e-Commerce, la quale prevedeva

[28] Per le altre norme dell'Unione fatte salve dal DSA si vedano il considerando 10 e l'art. 2, par. 4 DSA.

[29] «Destinatario del servizio»: «qualsiasi persona fisica o giuridica che utilizza un servizio intermediario, in particolare per ricercare informazioni o renderle accessibili» (art. 2, lett. b) DSA).

un generale regime di irresponsabilità per gli *internet service provider*, progressivamente erososi per via giurisprudenziale attraverso la creazione della figura dell'*hosting provider* attivo (v. Cap. 2, par. 2). Il nuovo regolamento interviene sul punto non apportando rivoluzioni radicali[30] ma mantenendo fermi i principi della Direttiva e-Commerce, positivizzando le indicazioni della richiamata giurisprudenza e chiarendo meglio il ruolo dei prestatori di servizi intermediari nella prevenzione e nel contrasto alla diffusione di «contenuti illegali[31]». A questo proposito, va subito aggiunto come il regolamento preveda norme uniformi soltanto per stabilire i casi in cui i *provider* possano andare esenti da responsabilità per i contenuti illegali forniti dai propri utenti, mentre la sussistenza di eventuali responsabilità in capo agli stessi deve essere determinata in base alle altre norme applicabili del diritto dell'Unione o nazionale[32].

Nell'intervenire sulla materia, il Digital Services Act, in primo luogo, abroga le disposizioni di cui artt. 12-15 della Direttiva e-Commerce, riproducendole al proprio interno, con qualche piccola modifica, agli artt. 4, 5, 6, 8 DSA[33]. Quanto al contenuto, il regolamento continua quindi a prevedere, come regime ordinario, l'irresponsabilità dei prestatori di servizi intermediari di cui alla previgente normativa (c.d. «*safe harbour*»).

Come anticipato, le novità attengono, innanzi tutto, al recepimento delle indicazioni della Corte di Giustizia relative alla figura dell'*hosting provider* attivo. A questo proposito, norma chiave è il considerando 18 DSA, il quale chiarisce

---

[30] In questo senso si vedano *ex multis*: G.M. RUOTOLO, *op. cit.* Cap. 3, n. 119, p. 263
C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 764; I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 14.

[31] Ai sensi dell'art. 2, lett. h) con «contenuto illegale» si intende «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto».

[32] V. considerando 17 DSA.

[33] Si veda in particolare l'art. 89 DSA,secondo cui: « 1. Gli articoli da 12 a 15 della direttiva 2000/31/CE sono soppressi. 2. I riferimenti agli articoli da 12 a 15 della direttiva 2000/31/CE si intendono fatti rispettivamente agli articoli 4, 5, 6 e 8 del presente regolamento».

come le esenzioni di responsabilità stabilite nel regolamento non dovrebbero applicarsi nei casi in cui un prestatore di servizi intermediario, «anziché limitarsi a una fornitura neutra dei servizi mediante un trattamento puramente tecnico e automatico delle informazioni fornite dal destinatario del servizio, svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni». Il medesimo considerando specifica poi che le esenzioni non dovrebbero applicarsi qualora in cui le informazioni siano fornite non dall'utente ma dallo stesso *provider*, anche nel caso di informazioni elaborate sotto la responsabilità editoriale di quest'ultimo. Aggiunta che, secondo alcuni commentatori[34], sarebbe suscettibile di restringere, in concreto, l'area della responsabilità degli *hosting provider* attivi che emerge dal regolamento.

Ulteriore disposizione che, innovando rispetto alla Direttiva e-Commerce, restringe l'applicazione del regime di «*safe harbour*» per alcuni prestatori di servizi intermediari è l'art. 6, par. 3 DSA, rivolto proprio alle piattaforme online. Secondo questa norma, infatti, le esenzioni stabilite a favore degli *hosting provider* non si applicano in relazione alla responsabilità prevista dalla normativa in materia di protezione dei consumatori per le piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali. Ciò, peraltro, a condizione che tali piattaforme agiscano «in modo tale da indurre un consumatore medio a ritenere che le informazioni, o il prodotto o il servizio oggetto dell'operazione, siano forniti dalla piattaforma stessa o da un destinatario del servizio che agisce sotto la sua autorità o il suo controllo». Si tratta di una norma pensata, teoricamente, a tutela dei consumatori[35] per i casi in cui questi effettuino acquisti attraverso piattaforme rite-

[34] C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 765.
[35] In questo senso v. considerando 24 DSA e I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 15.

nendo, poiché indotti in inganno dagli elementi di fatto, che i fornitori di queste siano le proprie controparti contrattuali. Anche questa disposizione, peraltro, ha sollevato alcune perplessità in dottrina[36], in particolare da parte di chi ha evidenziato le incertezze relative all'effettivo significato da assegnare alle espressioni «consumatore medio» e «sotto la sua autorità e suo controllo». Incertezze che sarebbero, a parere della citata dottrina, in grado di limitare, in concreto, la protezione offerta dal DSA ai consumatori.

Un altro aspetto su cui il Digital Services Act porta dei chiarimenti rispetto alla Direttiva e-Commerce è quello relativo ai doveri di sorveglianza dei prestatori di servizi intermediari. A questo proposito, innanzi tutto, l'art. 8 DSA conferma l'assenza, in capo ai *provider*, di obblighi generali di sorveglianza sulle informazioni da essi trasmesse o memorizzate, già prevista dalla Direttiva e-Commerce (v. *supra*: Cap. 2, par. 2.1). La novità è rappresentata invece dall'art. 7 DSA, ai sensi del quale i prestatori di servizi intermediari non perdono il beneficio del «*safe harbour*» per il solo fatto di svolgere, in buona fede e in modo diligente, indagini volontarie di propria iniziativa o di adottare altre misure volte a individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi. Analogamente, ai *provider* non è preclusa l'esenzione di responsabilità per aver adottato misure necessarie per conformarsi al diritto dell'Unione (compreso lo stesso Digital Services Act) o al diritto nazionale a questo conforme. In sostanza, la norma incentiva i *provider* ad attivarsi per contrastare la diffusione di contenuti illegali senza temere, per questo fatto solo, di perdere il beneficio dell'esenzione accordato loro dal Digital Services Act[37]. In questo senso, si tratta di un'innovazione da salutare con favore, posto che, come abbiamo avuto modo di vedere (v. Cap. 5, par. 1.2.2), in sempre più

[36] C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, pp. 766-767.
[37] I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 16

occasioni negli ultimi anni il legislatore dell'Unione ha fatto ricorso alla collaborazione delle piattaforme e a strumenti di coregolamentazione ai fini del contrasto alla diffusione di contenuti illegali online.

A proposito di collaborazione tra autorità competenti e *provider* per il contrasto alla diffusione di contenuti illegali, va infine aggiunto come gli artt. 4, 5, 6 DSA, al pari delle norme corrispondenti della Direttiva e-Commerce, lascino impregiudicata la possibilità che un'autorità giudiziaria o amministrativa ordini al prestatore di impedire o porre fine a una violazione conformemente all'ordinamento giuridico di uno Stato membro. Su questo aspetto, il Digital Services Act è innovativo rispetto alla normativa previgente in quanto specifica nel dettaglio, all'art. 9 DSA, le caratteristiche che dovrebbe avere un simile ordine. Tra queste, è opportuno ai nostri fini menzionare l'indicazione dell'ambito di applicazione territoriale dell'ordine, «in base alle norme del diritto dell'Unione e nazionale applicabili, compresa la Carta, e, se del caso, ai principi generali del diritto internazionale». Si tratta di una formulazione, quest'ultima, che richiama alla mente quanto disposto dalla Corte di Giustizia nella citata sentenza *Glawischnig-Piesczek* (v. Cap. 5, par. 1.1) e che va letta in correlazione con l'ulteriore requisito previsto dall'art. 9 DSA, secondo cui l'ambito dell'ordine dovrebbe limitarsi a quanto strettamente necessario per conseguire l'obiettivo dello stesso. Da aggiungere come siano simili le previsioni di cui all'art. 10 DSA in merito agli ordini di informazioni specifiche su uno o più singoli destinatari del servizio.

Dalle analisi appena svolte si deduce come il Digital Services Act, pur mantenendo fermi i principi generali di cui alla Direttiva e-Commerce, dovrebbe, quanto meno nelle intenzioni del legislatore, contribuire alla responsabilizzazione delle piattaforme ai fini del contrasto alla diffusione di contenuti illegali su internet, incentivando gli interventi diretti da parte delle stesse e restringendo l'ambito di applicazione dell'esenzione del «*safe harbour*». Ciò si pone

in continuità rispetto al percorso di evoluzione della materia di cui si è dato conto nel corso del presente lavoro e costituisce un naturale punto di arrivo dello stesso.

4 I doveri di diligenza dei *provider*: tra approccio «a strati», trasparenza e *private regulation*

Oltre a rivedere il regime della Direttiva e-Commerce, il Digital Services Act introduce, come anticipato, un nuovo sistema di norme relative ai doveri di diligenza («*due diligence*» nella versione in inglese) dei *provider*, allo scopo di garantire la sicurezza e la trasparenza degli ambienti digitali da questi gestiti.

Le regole in questione, previste al Capo III, costituiscono la parte più consistente ed articolata del nuovo regolamento. Ai nostri fini, è opportuno evidenziare come le stesse rispecchino le tendenze emerse nel corso del presente lavoro a proposito delle strategie regolatorie del legislatore dell'Unione nei confronti di internet e delle piattaforme digitali. Tali norme si fondano, infatti, sui principi della trasparenza e dell'*accountability* dei *provider*, in capo ai quali sono posti doveri sempre più penetranti per garantire la sicurezza del mondo digitale e contrastare la diffusione di contenuti illegali. Centrale è, inoltre, la valorizzazione del potere regolatorio degli stessi fornitori e della dimensione istituzionale degli ambienti da questi gestiti[38], anche attraverso la promozione di strumenti di autoregolamentazione e di coregolamentazione[39] che saranno illustrati a breve (v. *infra*: par. 4.4).

[38] In questo senso v. C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 767, ove si parla esplicitamente di «outsourcing solutions to private entities» da parte del legislatore dell'Unione.

[39] Per una critica nei confronti di questo approccio si vada: R. NIRO, *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive,* in Osservatorio sulle fonti, fasc. 3, pp. 1369-1391, 2021. Disponibile online su: www.osservatoriosullefonti.it

Prima di addentrarci nell'analisi nelle norme per noi rilevanti, occorre ribadire come i doveri di diligenza previsti dal Digital Services Act non siano identici per tutti i prestatori ma vengano, al contrario, gradati in base alle categorie e alle dimensioni di questi ultimi, secondo quello che abbiamo già avuto modo di definire come approccio «a strati[40]» (v. *supra*: par. 2.1). Nello specifico, accanto ad obblighi relativi a tutti i tipi di intermediari (artt. 11-15 DSA), ve ne sono alcuni applicabili, rispettivamente, soltanto agli *hosting provider*, inclusi i fornitori di piattaforme (artt. 16-18 DSA), ai fornitori di piattaforme (artt. 19-28 DSA), ai fornitori di piattaforme che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (artt. 29-32 DSA) e ai fornitori di piattaforme e di motori di ricerca di dimensioni molto grandi (artt. 34-38 DSA).

4.1 Gli obblighi relativi alle «condizioni generali» e alla trasparenza applicabili a tutti i *provider*

Cominciando dagli obblighi applicabili a tutti i *provider*, occorre porre l'accento su quelli relativi alle «condizioni generali[41]» previsti dall'art. 14 DSA[42], la cui rubrica utilizza l'espressione «termini e condizioni» già presente nel Regolamento P2B (v. *supra*: Cap. 2, par. 3.1).

---

[40] Per una sintesi delle posizioni critiche in merito a questo approccio si veda: I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 18.

[41] Per la definizione si veda l'art. 3, lett. u) DSA, secondo cui con «condizioni generali» si intendono «tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio».

[42] Per un'analisi di tale norma, seppur nella versione contenuta nella proposta della Commissione europea, ove corrispondeva all'art. 12, si veda: N. APPELMAN, J.P. QUINTAIS, R. FAHY, *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?*, apparso su Dsaobservatory.eu, il 31 maggio 2021, disponibile online: https://dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions.

Analogamente a quest'ultimo, anche il Digital Services Act richiede ai fornitori di inserire determinate informazioni nelle condizioni generali che disciplinano i rapporti contrattuali con i propri utenti. In particolare, l'art. 14, par. 1 DSA obbliga i *provider* a includere nelle stesse informazioni sulle proprie pratiche di «moderazione dei contenuti» («*content moderation*» in inglese), definite[43] come le attività, automatizzate o meno, da questi svolte allo scopo di «individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali» forniti dagli utenti. Più nel dettaglio, la norma richiede ai fornitori di indicare i motivi per cui essi potrebbero limitare la prestazione dei propri servizi ad uno o più utenti a seguito della condivisione di contenuti che violino il diritto dell'Unione o di uno Stato membro o le loro condizioni generali. Le informazioni in questione devono riguardare, tra le altre cose: «le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché le regole procedurali del loro sistema interno di gestione dei reclami».

A questo proposito, occorre notare come la norma non specifichi le caratteristiche che devono avere «le politiche, le procedure, le misure e gli strumenti» citati, limitandosi a richiederne l'indicazione – con un linguaggio chiaro e in

[43] V. art. 3, lett. t) DSA, secondo cui con «moderazione di contenuti» si intende «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le 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 informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio».

forma accessibile[44] – nelle condizioni generali per ragioni di trasparenza[45]. Da questo punto di vista, l'influenza dell'art. 14, par. 1 DSA sulla conformazione delle condizioni generali dei *provider* – e quindi, in buona sostanza, sulla loro attività regolatoria – risulta soltanto indiretta. La norma, infatti, pur prevedendo un vincolo alla libertà contrattuale dei fornitori[46] – e, di riflesso, al loro potere regolatorio – lascia la definizione delle politiche di moderazione dei contenuti pressocché totalmente in mano a questi ultimi. Ciò vale anche per i «sistemi interni di gestione dei reclami» che l'art. 14, par. 1 DSA richiede di istituire e di dotare di determinate procedure, senza tuttavia fornire alcuna indicazione in merito al contenuto e al funzionamento degli stessi. Analogamente, la norma non contiene nessuna indicazione circa i processi decisionali algoritmici da essa menzionati[47].

---

[44] V. a questo proposito l'art. 14, par. 1 DSA, ultimo periodo, secondo cui le condizioni generali devono essere «redatte in un linguaggio chiaro, semplice, comprensibile, facilmente fruibile e privo di ambiguità e sono disponibili al pubblico in un formato facilmente accessibile e leggibile meccanicamente».

[45] Le ragioni di trasparenza perseguite dal legislatore dell'Unione emergono anche dai successivi art. 14, par. 2, 3, 5, 6, secondo cui: «2. I prestatori di servizi intermediari informano i destinatari del servizio in merito a qualsiasi modifica significativa delle condizioni generali. 3. Se un servizio intermediario è principalmente destinato a minori o è utilizzato in prevalenza da questi, il prestatore di tale servizio intermediario spiega in modo comprensibile per i minori le condizioni e le restrizioni che si applicano all'utilizzo del servizio. […] 5. I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi forniscono ai destinatari dei servizi una sintesi concisa delle condizioni generali, di facile accesso e leggibile meccanicamente, compresi le misure correttive e i mezzi di ricorso disponibili, in un linguaggio chiaro e privo di ambiguità. 6. Le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi ai sensi dell'articolo 33 pubblicano le loro condizioni generali nelle lingue ufficiali di tutti gli Stati membri in cui offrono i loro servizi».

[46] V. considerando 46 DSA.

[47] Va ricordato come la disposizione in commento avesse attirato, in fase di discussione della proposta, le preoccupazioni dello European Data Protection Supervisor (EDPS) e di parte della dottrina per via dei rischi in termini di protezione dei dati personali connessi ai processi algoritmici e, in generale, alle politiche di moderazione dei contenuti dei *provider*. Si veda in particolare: EDPS, *Opinion 1/2021 on the European Commission's proposal for a Digital Services Act*, 10 febbraio 2021, disponibile online: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en. A livello dottrinale si veda: I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 20.

Un limite al potere regolatorio dei *provider* viene, quanto meno apparentemente, stabilito dall'art. 14, par. 4 DSA. Ai sensi di questa norma, ai fornitori è fatto obbligo di agire in «in modo diligente, obiettivo e proporzionato» nell'applicare le proprie politiche di moderazione dei contenuti, «tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio, quali la libertà di espressione, la libertà e il pluralismo dei media, e altri diritti e libertà fondamentali» sanciti dalla Carta di Nizza.

L'esatta portata di questa disposizione ha dato adito, prima dell'approvazione del regolamento, a diverse perplessità in dottrina[48], rimaste peraltro attuali dal momento che la stessa riproduce integralmente il contenuto dell'art. 12, par. 2 della proposta, oggetto delle richiamate perplessità. In particolare, è stato sottolineato come la disposizione non chiarisca se e con quale intensità i diritti fondamentali riconosciuti dalla Carta di Nizza siano direttamente applicabili ai rapporti tra i *provider* e gli utenti[49] e, di conseguenza, come incidano concretamente sulle decisioni dei fornitori basate sulle proprie condizioni generali. Si tratta di problematiche simili a quelle incontrate nel corso della nostra indagine in merito al funzionamento del Facebook Oversight Board (v. Cap. 5, par. 2.3 e 2.4) e che la nuova disposizione non sembra, quanto meno

---

[48] V. in particolare: I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 20; N. APPELMAN, J.P. QUINTAIS, R. FAHY, *op. cit.* n. 43; N. APPELMAN, J.P. QUINTAIS, R. FAHY, *Using Terms and Conditions to apply Fundamental Rights to Content Moderation*, in H. RICHTER, M. STRAUB, E. TUCHTFELD (a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, pp. 29-37, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021; I. BURI, J. VAN HOBOKEN, *The DSA Proposal's Impact on Digital Dominance*, in H. RICHTER, M. STRAUB, E. TUCHTFELD (a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, pp. 10-16, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021.

[49] Da notare come la dottrina richiamata alla nota 48 precedente si riferisca a tali rapporti con la formula «horizontal relationship», indicando che si tratta di rapporti tra soggetti privati in contrapposizione con le relazioni tra Stati e privati. Ai fini del presente lavoro, tali rapporti sono invece stati ricondotti alla «dimensione verticale» delle piattaforme, in contrapposizione con i rapporti tra utenti afferenti alla «dimensione orizzontale» (v. Cap. 1, par. 2.1).

nel contesto dell'Unione, aver risolto. Il rischio principale evidenziato in dottrina è quindi quello per cui, nell'attesa di indicazioni giurisprudenziali, la stessa possa risultare, all'atto pratico, poco più che una petizione di principio[50].

Sempre in materia di «*content moderation*», va menzionato l'art. 15 DSA, il quale stabilisce che tutti i *provider* debbano pubblicare, almeno una volta all'anno, in un formato leggibile meccanicamente e in modo facilmente accessibile, delle «relazioni chiare e facilmente comprensibili sulle attività di moderazione dei contenuti svolte nel periodo di riferimento». Le relazioni in questione devono contenere informazioni variamente gradate a seconda dei tipi di *provider* considerati dal regolamento, come ad esempio il numero di ordini ricevuti dalle autorità degli Stati membri (applicabile a tutti i fornitori), il numero di segnalazioni ricevute attraverso gli appositi meccanismi stabiliti ai sensi dell'art. 16 DSA (obbligo che si applica soltanto agli *hosting provider* e su cui v. *infra*: par. 4.2) o il numero di reclami ricevuti attraverso gli appositi sistemi interni di gestione stabiliti dai fornitori di piattaforme online ai sensi dell'art. 20 DSA (su cui v. *infra*: par. 4.3.1). Si tratta di obblighi che, come da rubrica dello stesso art. 15 DSA, perseguono l'obiettivo della trasparenza delle attività di moderazione dei contenuti dei *provider* e che non si applicano a quei fornitori che si qualificano come «microimprese» o «piccole imprese» ai sensi della raccomandazione 2003/361/CE[51] e che non sono piattaforme online di dimensioni molto grandi ai sensi dell'art. 33 DSA.

---

[50] V. in particolare N. APPELMAN, J.P. QUINTAIS, R. FAHY, *op. cit.* n. 43, ai sensi dei quali la norma, in assenza di chiarimenti giurisprudenziali, rischia di rimanere soltanto una «paper tiger».

[51] Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (Testo rilevante ai fini del SEE) [notificata con il numero C(2003) 1422], apparsa su *GU L 124, 20.5.2003, p. 36–41*. In particolare, l'art. 2 di tale raccomandazione stabilisce: «1. La categoria delle microimprese delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43

4.2 Gli obblighi applicabili agli *hosting provider* (piattaforme incluse): i sistemi di «*notice and action*»

I successivi artt. 16-18 DSA stabiliscono obblighi aggiuntivi per gli *hosting provider*, valorizzando in maniera più decisa il potere regolatorio di questi e la dimensione istituzionale degli ambienti da essi gestiti.

Questa valorizzazione emerge, in primo luogo, dall'art. 16 DSA, che impone a tutti gli *hosting provider*, fornitori di piattaforme inclusi, di istituire dei meccanismi di «segnalazione e azione» («*notice and action*[52]» in inglese), attraverso cui sia possibile segnalare agli *hosting provider* la presenza di contenuti illegali all'interno dei servizi da questi forniti, in modo che i fornitori possano procedere all'analisi degli stessi e alla loro eventuale rimozione. Si tratta di meccanismi già noti al diritto dell'Unione, la cui istituzione era stata incoraggiata dalla Commissione europea nella propria Raccomandazione del 2018 sulle misure per contrastare efficacemente i contenuti illegali online[53] e, come abbiamo avuto modo di vedere, è prevista anche dalla Direttiva Copyright per quanto riguarda i contenuti in violazione delle norme sul diritto d'autore (v. Cap. 2, par. 2.3).

In continuità con questi strumenti, ed in particolare con la raccomandazione della Commissione, l'art. 16 DSA chiede agli *hosting provider* di stabilire dei meccanismi che consentano a «qualsiasi persona o ente» – e quindi non soltanto agli utenti «destinatari del servizio» – di inviare loro segnalazioni «sufficientemente precise e adeguatamente motivate», che contengano una serie di

milioni di EUR. 2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.3. Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR».

[52] In questo senso: I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 21.

[53] Raccomandazione (UE) 2018/334 della Commissione, del 1° marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online, apparsa su *GU L 63, 6.3.2018, p. 50–61*.

elementi indicati dalla norma stessa[54]. La ricezione di segnalazioni che consentano ad un *hosting provider* «diligente[55]» di avvedersi del carattere illegale delle informazioni o delle attività oggetto delle stesse fa scattare la presunzione della conoscenza delle stesse da parte del fornitore.

Conseguenze di tale presunzione sono la perdita del beneficio del *safe harbour* da parte degli *hosting provider* e il sorgere dell'obbligo, per questi ultimi, di trattare le segnalazioni ricevute e di adottare le proprie decisioni «in modo tempestivo, diligente, non arbitrario e obiettivo». Si tratta di funzioni sostanzialmente para-giurisdizionali, in quanto i *provider* si ritrovano a dover valutare la legittimità dei contenuti condivisi dai propri utenti, avendo anche l'obbligo di prendere decisioni vincolanti nei confronti degli stessi. A questo proposito, va però notato come ai fornitori non sia richiesto di compiere accertamenti approfonditi in punto di diritto, sorgendo la presunzione di cui si è detto a fronte di segnalazioni che permettano di appurare «senza un esame giuridico dettagliato» – e quindi con giudizio meramente sommario – il carattere illecito delle informazioni e delle attività oggetto di queste.

I provvedimenti che gli *hosting provider* possono prendere variano a seconda della natura delle informazioni e delle attività segnalate e possono includere, ad esempio, la rimozione, la restrizione all'accesso o la modifica del posizionamento dei contenuti sugli spazi gestiti dagli *hosting provider*. In ogni caso, i

---

[54] V. art. 16, par. 2, secondo cui le segnalazioni devono contenere: «a) una spiegazione sufficientemente motivata dei motivi per cui la persona o l'ente presume che le informazioni in questione costituiscano contenuti illegali; b) una chiara indicazione dell'ubicazione elettronica esatta di tali informazioni, quali l'indirizzo o gli indirizzi URL esatti e, se necessario, informazioni supplementari che consentano di individuare il contenuto illegale adeguato al tipo di contenuto e al tipo specifico di servizio di memorizzazione di informazioni; c) il nome e l'indirizzo di posta elettronica della persona o dell'ente che presenta la segnalazione, tranne nel caso di informazioni che si ritiene riguardino uno dei reati di cui agli articoli da 3 a 7 della direttiva 2011/93/UE; d) una dichiarazione con cui la persona o l'ente che presenta la segnalazione conferma la propria convinzione in buona fede circa l'esattezza e la completezza delle informazioni e delle dichiarazioni ivi contenute.

[55] Art. 16, par. 3 DSA.

fornitori sono obbligati ad avvisare i segnalatori senza indebito ritardo sulle decisioni da essi assunte, fornendo informazioni in merito ai ricorsi esperibili contro le stesse (art. 16, par. 5 DSA).

Inoltre, analogamente a quanto previsto dal Regolamento P2B (v. *supra*: Cap. 2, par. 3.1), l'art. 17 DSA obbliga gli *hosting provider* a fornire agli utenti una motivazione chiara e specifica a sostegno di determinati provvedimenti[56] da questi assunti a seguito della condivisione di contenuti illegali o incompatibili con le loro condizioni generali. Sotto il profilo contenutistico, la motivazione in questione deve contenere, quanto meno, una serie dettagliata di informazioni elencate all'art. 17, par. 3 DSA. In particolare, vanno, in primo luogo, indicate le misure[57] contenute nella decisione adottata e, ove opportuno, la portata territoriale della stessa e la sua durata. A ciò si aggiungono i fatti e le circostanze su cui si basa la decisione, compresa la specifica sul se essa si fondi su una segnalazione ai sensi dell'art. 16 DSA o su indagini volontarie nonché, ove strettamente necessario, l'identità del segnalante[58]. In terzo luogo, ove opportuno, vanno fornite informazioni sugli eventuali strumenti automatizzati utilizzati ai fini della decisione[59]. Importante, ai nostri fini, l'obbligo di cui all'art. 17, par. 1, lett. d) DSA, ai sensi del quale, in caso di decisioni relative a

[56] Ai sensi dell'art. 17, par. 1 DSA le motivazioni sono obbligatorie nel caso in cui vengano adottate le seguenti restrizioni: « (a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; (b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; (c) la sospensione o la cessazione totale o parziale della prestazione del servizio; (d) la sospensione o la chiusura dell'account del destinatario del servizio».

[57] Ai sensi dell'art. 17, par. 3, lett. a), la motivazione deve contenere: «l'informazione che indichi se la decisione comporti la rimozione delle informazioni, la disabilitazione dell'accesso alle stesse, la retrocessione o la limitazione della visibilità delle informazioni oppure la sospensione o la cessazione dei pagamenti in denaro relativi a tali informazioni o imponga altre misure di cui al paragrafo 1 in relazione alle informazioni, e, ove opportuno, la portata territoriale della decisione e la sua durata»;

[58] Art. 17, par. 3, lett. b) DSA.

[59] Art. 17, par. 3, lett. c) DSA.

presunti «contenuti illegali», la motivazione deve contenere un riferimento alla base giuridica invocata e una spiegazione delle ragioni per cui il fornitore ha considerato l'informazione come contenuto illegale in applicazione della stessa.

Un analogo obbligo è previsto dalla successiva lett. e) per il caso in cui la decisione si basi sulla presunta incompatibilità delle informazioni con le condizioni generali dell'*hosting provider*: in questa ipotesi, la motivazione deve contenere un riferimento alla clausola contrattuale invocata e una spiegazione delle ragioni per cui le informazioni sono state ritenute incompatibili la stessa. Infine, è obbligatorio per l'*hosting provider* fornire informazioni chiare e di facile comprensione sui mezzi di ricorso a disposizione dell'utente contro la decisione presa nei propri confronti, in particolare, se del caso, attraverso i meccanismi interni di gestione dei reclami, la risoluzione extragiudiziale delle controversie e il ricorso per via giudiziaria (su cui v. *infra*: par. 4.3).

L'obbligo di fornire motivazioni così dettagliate, oltre a perseguire obiettivi di responsabilizzazione degli *hosting provider*, conferma come il Digital Services Act incarichi questi ultimi di svolgere, quanto meno per ciò che riguarda la moderazione dei contenuti all'interno degli ambienti da essi gestiti, funzioni di tipo para-giurisdizionale[60]. Ciò vale, in particolare, per gli obblighi relativi all'indicazione delle norme di legge o delle condizioni generali violate, della durata e dell'ambito di applicazione territoriale dei provvedimenti adottati[61] e, soprattutto, dei mezzi di ricorso che gli utenti hanno a disposizione per contestare le decisioni subite (su cui v. *infra*: par. 5). Peraltro, la circostanza che la cognizione degli *hosting provider* in merito all'illiceità delle informazioni segnalate debba essere sommaria e quella per cui, a prescindere, agli utenti siano

[60] C. GOANTA, P. ORTOLANI, *op. cit.* Cap. 5, n. 6.

[61] Dovere, quest'ultimo, che richiama le problematiche affrontate dalla Corte di Giustizia nella citata sentenza *Glawischnig-Piesczek* (v. *supra*: Cap. 5, par. 1.1 e Cap. 6, par. 3).

garantiti strumenti di ricorso per via giudiziaria, dimostrano come, anche in questo caso, il regolatore pubblico non conferisca una delega in bianco a favore del regolatore privato, ma si limiti ad attribuire funzioni a quest'ultimo, vista la sua capacità di contrastare in maniera autonoma e più celere la diffusione di contenuti illegali, mantenendo per sé i poteri decisori finali. Significativo è, a questo proposito, anche quanto previsto dall'art. 18 DSA, il quale impone agli *hosting provider* di informare senza indugio le autorità giudiziarie o le forze di polizia degli Stati membri interessati in caso di sospetti di reati che comportino una minaccia per la vita o la sicurezza di una o più persone. Il contrasto alle attività criminali resta, quindi, prerogativa del regolatore pubblico.

4.3 Gli obblighi per le piattaforme online: tra dimensione istituzionale, autoregolamentazione e trasparenza

Oltre alle norme destinate a tutti gli *hosting provider*, il Digital Services Act prevede, come già anticipato, un apposito regime (artt. 19-28 DSA) dedicato a quella particolare categoria di prestatori di servizi di memorizzazione di informazioni costituita dai fornitori di piattaforme online[62] (per la relativa nozione v. *supra*: par. 2.1). Accanto a queste ulteriori regole, compaiono poi delle disposizioni aggiuntive applicabili ai fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali (artt. 29-32 DSA) e delle norme che stabiliscono obblighi supplementari a carico dei fornitori di piattaforme online e di motori di ricerca online

[62] Va peraltro chiarito come, ai sensi dell'art. 19 DSA, le norme di cui agli artt. 19-28 DSA, ad eccezione dell'art. 24, par. 3 DSA, non si applicano ai fornitori di piattaforme online che si qualificano come microimprese o piccole imprese quali definite nella raccomandazione 2003/361/CE o a quelli che si sono precedentemente qualificati come tali nel corso dei 12 mesi successivi alla perdita di tale qualifica. Il medesimo articolo aggiunge come le norme in questione si applichino, in ogni caso, ai fornitori di piattaforme online di dimensioni molto grandi a norma dell'articolo 33, indipendentemente dal fatto che essi si qualifichino come microimprese o piccole imprese.

di dimensioni molto grandi per la gestione dei rischi sistemici (artt. 29-32 DSA).

Le disposizioni in commento, in coerenza con l'approccio «a strati» che permea l'intero Digital Services Act e viste le caratteristiche dei servizi offerti da questi fornitori[63], stabiliscono per gli stessi degli obblighi più penetranti rispetto a quelli validi per tutti gli *hosting provider*, anche dal punto di vista della valorizzazione della dimensione istituzionale e dell'autoregolamentazione delle piattaforme.

4.3.1 La gestione dei reclami interni alle piattaforme e gli strumenti di risoluzione extragiudiziale delle controversie

Conformemente a questo *modus operandi*, l'art. 20 DSA impone ai fornitori delle piattaforme digitali di istituire dei sistemi interni attraverso cui gli utenti e i segnalatori possano presentare – gratuitamente, in via elettronica e entro un termine non inferiore a sei mesi dalla decisione[64] – dei reclami contro le decisioni adottate dai fornitori a seguito delle segnalazioni di cui all'art. 16 DSA (v. *supra*: par. 4.2) o contro alcuni tipi di decisioni prese a motivo dell'illegalità delle informazioni oggetto della segnalazione o della loro incompatibilità con le condizioni generali di un fornitore.

In particolare, i reclami possono essere presentati contro le decisioni che indicano se rimuovere le informazioni, disabilitare l'accesso alle stesse o limitarne la visibilità, contro quelle relative alla sospensione o all'interruzione della prestazione del servizio a favore di un utente, così come contro quelle relative all'account di quest'ultimo o contro la sospensione, cessazione o limitazione della capacità di monetizzare le informazioni fornite. Tali meccanismi

[63] Considerando 41 DSA.

[64] Ai sensi dell'art. 20, par. 3 DSA, il termine in questione decorre dal momento in cui il destinatario del servizio è stato informato della decisione ai sensi dell'art. 16, par. 5 o dell'art. 17 DSA.

non prevedono, peraltro, una rivalutazione *ex novo* in merito all'illegalità dei contenuti segnalati, ma soltanto una revisione delle decisioni inizialmente assunte fondata sui motivi esposti dai reclamanti[65]. Si tratta, quindi, di sistemi assimilabili a mezzi d'impugnazione a critica libera, oltre che a modelli di *private regulation* già esaminati, come quelli del Facebook Oversight Board[66] (v. *supra*: Cap. 5, par. 2).

La previsione di questi meccanismi costituisce un ulteriore riconoscimento della dimensione istituzionale e dell'autoregolamentazione delle piattaforme digitali da parte del legislatore dell'Unione, il quale rafforza e specifica in questo modo le funzioni para-giurisdizionali attribuite ai fornitori in materia di «*content moderation*».

A tutela degli utenti, l'art. 20, par. 3 DSA dispone che i sistemi di gestione dei reclami siano facilmente accessibili ed utilizzabili, consentendo e agevolando la presentazione di reclami «sufficientemente precisi e adeguatamente motivati». Il successivo art. 20, par. 4 DSA impone invece ai *provider* di gestire i reclami «in modo tempestivo, non discriminatorio, diligente e non arbitrario», allo scopo di assicurare l'imparzialità del giudizio. La stessa norma aggiunge che nel caso di reclami fondati su «motivi sufficienti», tali da indurre il fornitore a rivedere una propria decisione, questi debba procedere all'annullamento della stessa «senza indebito ritardo». Viceversa, in caso di reclami non sufficientemente fondati si dovrebbe arrivare a decisioni di rigetto[67]. Infine, si pone a garanzia dei destinatari dei servizi e della correttezza dei giudizi dei fornitori la disposizione di cui all'art. 20, par. 6 DSA, secondo cui le decisioni

[65] C. GOANTA, P. ORTOLANI, *op. cit.* Cap. 5, n. 6, p. 22.
[66] Idem, p. 23.
[67] Idem.

sui reclami devono essere prese «con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati».

Oltre a questi reclami interni, il Digital Services Act prevede – muovendosi anche da questo punto di vista in analogia con il Regolamento P2B (v. Cap. 2, par. 3.1) – altri strumenti attraverso cui contestare, al di fuori delle piattaforme, le decisioni relative ai contenuti condivisi dagli utenti. Si tratta, in particolare, dei sistemi di risoluzione extragiudiziale delle controversie, disciplinati dall'art. 21 DSA. Questa norma consente, infatti, agli utenti (inclusi i segnalatori) di rivolgersi a degli organismi certificati dai «coordinatori dei servizi digitali[68]» dai relativi Stati membri di stabilimento per risolvere, in via stragiudiziale, le controversie relative alle decisioni adottate dai fornitori a seguito dei reclami interni di cui all'art. 20 DSA.

A differenza di quanto previsto nella proposta di regolamento del dicembre 2020[69], gli organismi in questione non hanno il potere di adottare decisioni vincolanti per le parti ma possono essere aditi al solo scopo di favorire il raggiungimento, in buona fede, di una risoluzione extragiudiziale delle controversie portate alla propria attenzione. Peraltro, i fornitori delle piattaforme possono

[68] V. art. 49, par. 2 DSA: «Gli Stati membri designano una delle autorità competenti come coordinatore dei servizi digitali. Il coordinatore dei servizi digitali è responsabile di tutte le questioni relative alla vigilanza e all'applicazione del presente regolamento in tale Stato membro, a meno che lo Stato membro interessato non abbia assegnato determinati compiti o settori specifici ad altre autorità competenti. Il coordinatore dei servizi digitali è comunque responsabile di garantire il coordinamento a livello nazionale in relazione a tali questioni e di contribuire alla vigilanza e all'applicazione efficaci e coerenti del presente regolamento in tutta l'Unione […]».

[69] V. art. 18 della proposta, corrispondente all'art. 21 DSA. Per dei commenti a riguardo si vedano: C. GOANTA, P. ORTOLANI, *op. cit.* Cap. 5, n. 6, p. 23; I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 22; D. HOLZNAGEL, *The Digital Services Act wants you to "sue" Facebook over content decisions in private de facto courts*, apparso su Verfassungsblog.de, il 24 giugno 2021, disponibile online: https://verfassungsblog.de/dsa-art-18/.

rifiutarsi di aderire ai tentativi di risoluzione nel caso in cui esistano delle precedenti controversie già risolte relative alle medesime informazioni o agli stessi motivi[70]. Anche questa previsione, che appare suscettibile di disincentivare il ricorso a questi strumenti, non era contenuta nella proposta originaria della Commissione europea.

Tra le caratteristiche che devono avere gli organismi di risoluzione per poter essere certificati vi sono, innanzi tutto, l'imparzialità e l'indipendenza, anche sul piano finanziario, sia rispetto ai fornitori delle piattaforme[71] che rispetto agli utenti e ai segnalatori. A queste si aggiungono la sussistenza delle competenze necessarie in materia di moderazione di contenuti e la circostanza per cui i membri di tali organismi non siano retribuiti in base all'esito delle procedure alla loro attenzione. Inoltre, gli organismi in questione devono garantire la facile accessibilità ai meccanismi di risoluzione attraverso mezzi elettronici e devono essere in grado di risolvere le controversie «in modo rapido, efficiente ed efficace sotto il profilo dei costi e in almeno una delle lingue ufficiali delle istituzioni dell'Unione». Infine, è richiesto che le risoluzioni delle controversie avvengano secondo regole procedurali «chiare ed eque», che siano «facilmente e pubblicamente accessibili e conformi al diritto applicabile». L'art. 21 DSA contiene poi ulteriori disposizioni relative agli obblighi di relazione delle proprie attività da parte degli organismi certificati[72], ai tempi[73] e alla ripartizione dei costi[74] dei procedimenti, nonché al ruolo dei coordinatori dei servizi digitali, su cui non è qui possibile soffermarsi nel dettaglio[75].

[70] Art. 21, par. 2, comma 2 DSA.
[71] Art. 21, par. 3, lett. a) DSA.
[72] Art. 21, par. 4 DSA.
[73] Idem.
[74] Art. 21, par. 5 DSA.
[75] Art. 21, par. 4, 7, 8 DSA.

La previsione e le caratteristiche di questi organismi evidenziano ancora una volta come il legislatore dell'Unione non abbia conferito una delega bianco ai fornitori ai fini della regolamentazione delle piattaforme da essi gestiti e della risoluzione delle controversie sorte all'interno delle stesse. Al contrario, infatti, il regolatore pubblico continua a mantenersi in una posizione di (quantomeno formale) preminenza rispetto a quello privato, come esemplificato anche dalla necessità per gli organismi – i quali, peraltro, potranno essere istituiti direttamente dagli Stati membri[76] – di ottenere una certificazione dalle competenti autorità pubbliche per poter operare. L'esistenza di questi organismi dovrebbe, inoltre, fornire agli utenti una tutela maggiore rispetto a quella garantita dei sistemi di presentazione dei reclami interni alle piattaforme. Occorrerà, tuttavia, osservare attentamente il fenomeno nella pratica per comprenderne la reale utilità a tal fine, tenendo a mente le diverse perplessità sollevate sul punto in dottrina[77], soprattutto per quanto riguarda la praticità dei meccanismi in questione. Quanto all'imparzialità e all'indipendenza degli organismi – anch'esse fonti di preoccupazioni in dottrina[78] – si confida che le stesse possano essere garantite dall'attività dei coordinatori dei servizi digitali, tenendo anche conto degli obblighi di relazionare agli stessi imposti agli organismi dalla disposizione in commento.

Infine, è il caso di sottolineare come l'art. 21, par. 1, comma 3 DSA faccia in ogni caso esplicitamente salva la possibilità per gli utenti di intentare, in qualsiasi momento e senza alcuna preclusione o rapporto di alternativa rispetto ai meccanismi di risoluzione extragiudiziale appena esaminati, dei procedimenti dinnanzi alle competenti autorità giurisdizionali allo scopo di contestare le decisioni dei fornitori delle piattaforme (sul punto v. anche *infra*: par. 5). Ciò ad

[76] Art. 21, par. 6 DSA.
[77] D. HOLZNAGEL, *op. cit.* n. 69.
[78] Idem.

ulteriore tutela dei diritti dei «destinatari dei servizi» e a riprova della preminenza, quantomeno formale, del regolatore pubblico su quello privato.

4.3.2 Il rafforzamento dei doveri di trasparenza e dell'*accountability* delle piattaforme

Sintomatiche dell'approccio del legislatore sono anche le altre disposizioni rivolte alle piattaforme online. Le norme in questione, su cui non è qui possibile soffermarsi con pretesa di esaustività[79], infatti, rafforzano sensibilmente gli obblighi di trasparenza e di *accountability* dei fornitori, facendo in più occasioni leva sul loro potere regolatorio e sulla dimensione istituzionale delle piattaforme da essi gestite.

Ad esempio, diversi ulteriori obblighi di trasparenza – sia nei confronti degli utenti che nei confronti della Commissione europea e dei coordinatori dei servizi digitali – sono stabiliti dall'art. 24 DSA. Tra questi, vale la pena ricordare quelli di includere ulteriori informazioni[80] nelle relazioni di cui all'art. 15 DSA (v. *supra*: par. 4.2). Obiettivi di trasparenza sono perseguiti anche dalle norme sulla progettazione e sull'organizzazione delle interfacce online (art. 25 DSA), sulla pubblicità sulle piattaforme online (art. 26 DSA), sulla trasparenza dei sistemi di raccomandazione (art. 27 DSA) e sulla protezione online dei minori (art. 28 DSA). Infine, specifici obblighi informativi, anch'essi funzionali alla

[79] Per approfondire v. dottrina cit. sub nota n. 3.

[80] «1. Oltre alle informazioni di cui all'articolo 15, i fornitori di piattaforme online includono nelle relazioni di cui a tale articolo informazioni sui seguenti elementi: a) il numero di controversie sottoposte agli organismi di risoluzione extragiudiziale delle controversie di cui all'articolo 21, i risultati della risoluzione delle controversie, il tempo mediano necessario per completare le procedure di risoluzione delle controversie nonché la percentuale di controversie per le quali il fornitore della piattaforma online ha attuato le decisioni dell'organismo; b) il numero di sospensioni imposte a norma dell'articolo 23, operando una distinzione tra le sospensioni messe in atto in risposta alla fornitura di contenuti manifestamente illegali, alla presentazione di segnalazioni manifestamente infondate e alla presentazione di reclami manifestamente infondati (art. 24, par. 1 DSA).

trasparenza, sono posti in capo ai fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con operatori commerciali (art. 32 DSA).

Sotto il profilo della responsabilizzazione vanno invece citati gli artt. 22 e 23 DSA. Il primo impone ai fornitori di piattaforme online di adottare le misure tecniche e organizzative necessarie affinché venga data priorità alle segnalazioni presentate dai «segnalatori attendibili» («*trusted flaggers*» in inglese), le quali devono essere trattate e decise «senza indebito ritardo». Da sottolineare come la qualifica di «segnalatori attendibili» possa essere riconosciuta a qualsiasi ente che ne faccia richiesta da parte del coordinatore dei servizi digitali dello Stato membro in cui il richiedente è stabilito, purché questo dimostri di soddisfare delle condizioni[81] elencate dall'art. 22, par. 2 DSA. Peraltro, agli stessi segnalatori sono imposti dal medesimo articolo diversi obblighi di trasparenza e di collaborazione con le autorità pubbliche.

L'art. 23 DSA prevede, invece, una disciplina particolare relativa alle misure da adottare da parte dei fornitori per contrastare i comportamenti abusivi, sia degli utenti che dei segnalatori. In primo luogo, dopo aver emesso un avviso preventivo, i fornitori sono tenuti a sospendere «per un periodo di tempo ragionevole» la prestazione dei propri servizi agli utenti che con frequenza forniscono contenuti manifestamente illegali (art. 23, par. 1 DSA). Analogamente, sempre previo avviso, i fornitori sospendono «per un periodo ragionevole» anche il trattamento delle segnalazioni ex art. 16 DSA e dei reclami ex art. 20 DSA presentati da persone o enti che con frequenza presentano segnalazioni o reclami manifestamente infondati. Entrambe le sospensioni vanno decise

[81] Le condizioni previste dall'art. 22, par. 2 DSA sono le seguenti: «a) dispone di capacità e competenze particolari ai fini dell'individuazione, dell'identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo».

«caso per caso e in modo tempestivo, diligente e obiettivo», tenendo conto di una serie di circostanze[82] elencate dall'art. 23, par. 3 DSA. Si tratta, anche in questo caso, di obblighi che intervengono direttamente sul potere regolatorio dei fornitori delle piattaforme, orientando le funzioni para-giurisdizionali ad essi conferite dal legislatore dell'Unione. Ciò vale anche per l'ulteriore obbligo, previsto dall'art. 23, par. 4 DSA, di indicare nelle condizioni generali, in modo chiaro e dettagliato, le politiche relative agli abusi appena esaminati, fornendo altresì degli esempi dei fatti e delle circostanze di cui i fornitori tengono conto ai fini delle proprie valutazioni sul punto.

4.3.3 Gli obblighi supplementari a carico dei fornitori di piattaforme online di dimensioni molto grandi

Come abbiamo già avuto modo di anticipare, il Digital Services Act pone ulteriori doveri di trasparenza e di *accountability* in capo ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi (per le relative nozioni v. *supra*: par. 2.1). Le norme in questione (artt. 33-43 DSA) sono finalizzate alla gestione dei «rischi sistemici[83]» connessi alle caratteristiche e alle dimensioni di queste piattaforme, le quali hanno «una portata più ampia[84]» rispetto alle altre e «un impatto maggiore nell'influenzare il modo in cui i destinatari dei servizi ottengono informazioni e comunicano online[85]». Caratteristiche che, a parere del legislatore

[82] In particolare, ai sensi dell'art. 23, par. 3 DSA le circostanze comprendono almeno: «a) il numero, in termini assoluti, di contenuti manifestamente illegali o di segnalazioni o reclami manifestamente infondati presentati entro un determinato arco temporale; b) la relativa proporzione rispetto al numero totale di informazioni fornite o di segnalazioni presentate entro un determinato arco temporale; c) la gravità degli abusi, compresa la natura dei contenuti illegali, e delle relative conseguenze; d) ove sia possibile identificarla, l'intenzione del destinatario del servizio, della persona, dell'ente o del reclamante».

[83] Per una panoramica dei relativi rischi v. art. 34 DSA.

[84] V. considerando 57 DSA.

[85] Idem.

dell'Unione, giustificano l'imposizione di obblighi supplementari in capo ai relativi fornitori.

Disposizioni chiave[86] di questo specifico regime normativo sono gli artt. 34-35 DSA. L'art. 34 DSA, in particolare, richiede ai *provider* di svolgere delle apposite valutazioni dei rischi sistemici nell'Unione derivanti dalla progettazione, dal funzionamento o dall'uso delle piattaforme da essi gestiti, nonché dai relativi sistemi, inclusi i sistemi algoritmici. Le analisi in questioni devono essere svolte entro termini specifici[87] e vanno rinnovate almeno una volta all'anno e, in ogni caso, prima di introdurre funzionalità che possano avere un impatto critico sui rischi individuati dal medesimo art. 34 DSA. Con una formulazione simile a quanto previsto da diverse disposizioni del GDPR[88], la norma richiede di svolgere una valutazione specifica e proporzionata ai rischi sistemici, «tenendo in considerazione la loro gravità e la loro probabilità». Tale

[86] I. BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 33.

[87] Ai sensi dell'art. 34, par. 1, comma 2 DSA, in particolare, le valutazioni dei rischi devono essere effettuate entro la data di applicazione di cui all'art. 33, par. 6, secondo comma DSA. L'art. 33, par. 6 DSA dispone, a propria volta: «6. La Commissione notifica senza indebito ritardo le sue decisioni a norma dei paragrafi 4 e 5 al fornitore della piattaforma online o del motore di ricerca online in questione, al comitato e al coordinatore dei servizi digitali del luogo di stabilimento. La Commissione provvede affinché l'elenco delle piattaforme online designate di dimensioni molto grandi o dei motori di ricerca online designati di dimensioni molto grandi sia pubblicato nella *Gazzetta ufficiale dell'Unione europea* e provvede all'aggiornamento di tale elenco. Gli obblighi di cui alla presente sezione si applicano, o cessano di applicarsi, alle piattaforme online di dimensioni molto grandi interessate e ai motori di ricerca online di dimensioni molto grandi decorsi quattro mesi dalla notifica al fornitore interessato di cui al primo comma».

[88] Artt. 24, 25, 32, 35 GDPR.

valutazione deve comprendere alcuni rischi sistemici specificamente individuati dall'art. 34, par. 1, secondo comma DSA[89] e deve tenere conto delle modalità con cui alcuni fattori[90] relativi alle piattaforme e alle politiche dei fornitori elencati dalla norma in commento possano influire sugli stessi. Per ragioni di *accountability* i fornitori sono, inoltre, obbligati a conservare i documenti giustificativi delle valutazioni dei rischi per almeno tre anni e, su richiesta, devono comunicarli alla Commissione europea e al coordinatore dei servizi digitali del luogo di stabilimento.

A valle di queste valutazioni, il successivo art. 35 DSA impone ai fornitori di piattaforme di dimensioni molto grandi di adottare misure di attenuazione

---

[89] V. in particolare art. 34, par. 1, comma secondo DSA, ai sensi di cui: « […] La valutazione del rischio deve essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità, e deve comprendere i seguenti rischi sistemici: a) la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'articolo 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'articolo 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta; c) eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona». Per un approfondimento sul punto si veda: BURI, J. VAN HOBOKEN, *op. cit*. n. 3, pp. 32ss.

[90] V. in particolare art. 34, par. 2 DSA, secondo cui: «Nello svolgimento delle valutazioni dei rischi, i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi tengono conto, in particolare, dell'eventualità e del modo in cui i seguenti fattori influenzano uno dei rischi sistemici di cui al paragrafo 1: a) la progettazione dei loro sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente; b) i loro sistemi di moderazione dei contenuti; c) le condizioni generali applicabili e la loro applicazione; d) i sistemi di selezione e presentazione delle pubblicità; e) le pratiche del fornitore relative ai dati. Le valutazioni analizzano inoltre se e in che modo i rischi di cui al paragrafo 1 siano influenzati dalla manipolazione intenzionale del loro servizio, anche mediante l'uso non autentico o lo sfruttamento automatizzato del servizio, nonché l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali. La valutazione tiene conto di specifici aspetti regionali o linguistici, anche laddove siano specifici di uno Stato membro».

«ragionevoli, proporzionate ed efficaci» per contrastare i rischi individuati attraverso le stesse, ponendo particolare attenzione nei confronti degli effetti di tali misure sui diritti fondamentali. Lo stesso articolo fornisce un elenco esemplificativo[91] di misure potenzialmente adottabili, le quali riguardano – direttamente o indirettamente – il potere regolatorio dei fornitori delle piattaforme, sia sotto il profilo delle regole e degli standard tecnici che di quello delle condizioni generali o di altre regole di condotta di tipo contrattuale. Tra queste, vale qui la pena menzionare: l'adeguamento della progettazione, delle caratteristiche o del funzionamento delle piattaforme e delle loro interfacce online (art. 35, par. 1, lett. a) DSA); l'adeguamento delle condizioni generali e la loro applicazione (art. 35, par. 1, lett. b) DSA); l'adeguamento delle procedure di moderazione dei contenuti[92] (art. 35, par. 1, lett. c) DSA); la sperimentazione e l'adeguamento dei sistemi algoritmici, compresi i sistemi di raccomandazione (art. 35, par. 1, lett. d) DSA); l'avvio o l'adeguamento della cooperazione con altri fornitori di piattaforme online o di motori di ricerca online attraverso i codici di condotta e i protocolli di crisi di cui agli artt. 45 e 48 DSA (art. 35, par. 1, lett. h) DSA – v. *infra*: par. 4.4).

Come evidenziato da certa dottrina[93], la circostanza per cui la valutazione dei rischi sistemici e l'individuazione delle misure adatte a farvi fronte siano demandate ai fornitori delle piattaforme costituisce un ulteriore riconoscimento e valorizzazione del potere regolatorio di questi ultimi, ai quali il legislatore si affida per il raggiungimento dei propri obiettivi. La scelta di conferire questi

[91] Per l'elenco completo v. art. 35, par. 1 DSA.

[92] «[…] compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare in relazione all'incitamento illegale all'odio e alla violenza online, nonché l'adeguamento di tutti i processi decisionali pertinenti e delle risorse dedicate alla moderazione dei contenuti […]» (art. 35, par. 1, lett. c) DSA).

[93] C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 770.

compiti ai fornitori delle piattaforme appare condivisibile sulla scorta delle già richiamate ragioni a sostegno dell'autoregolamentazione o della coregolamentazione delle piattaforme (v. *supra*: Cap. 4, par. 3.1.2, 3.1.3). Infatti, i fornitori costituiscono, per ragioni di prossimità nonché per l'enorme mole di dati e informazioni in proprio possesso, i soggetti più adatti a riconoscere i problemi delle piattaforme da essi gestiti, inclusi i rischi per gli utenti, e a trovarne le soluzioni[94].

Anche in questo caso, tuttavia, non si assiste ad una delega in bianco da parte del regolatore pubblico a favore del privato. Al contrario, infatti, oltre ai vincoli di cui agli artt. 34-35 DSA che abbiamo appena esaminato, il Digital Services Act stabilisce diversi strumenti attraverso cui controllare le attività dei fornitori delle piattaforme di dimensioni molto grandi.

In primo luogo, infatti, l'art. 36 DSA attribuisce alla Commissione europea dei poteri significativi da esercitare nei confronti dei fornitori nel caso di crisi, ossia qualora si verifichino «circostanze eccezionali che comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative di essa[95]». In particolare, su raccomandazione del comitato europeo per i servizi digitali di cui all'art. 61 DSA (su cui v. *infra*: par. 5), l'Esecutivo può adottare delle decisioni che impongano ai fornitori una o più azioni volte a prevenire o contrastare tali situazioni, le quali vanno ad incidere, limitandolo, sul potere regolatorio degli stessi *provider*[96].

---

[94] In questo senso v. anche: C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 770.

[95] Art. 36, par. 2 DSA.

[96] Le azioni che possono essere richieste ai fornitori di piattaforme di dimensioni molto grandi ai sensi dell'art. 36, par. 1 DSA sono: «[…] a) la valutazione sull'eventualità e, in caso affermativo, sulla relativa portata e sul modo in cui il funzionamento e l'uso dei loro servizi contribuiscano, o possano contribuire, in maniera significativa a una minaccia grave […]; b) l'individuazione e l'applicazione di misure specifiche, efficaci e proporzionate, quali quelle di cui all'articolo 35, paragrafo 1, o all'articolo 48, paragrafo 2, per prevenire, eliminare o limitare tale contributo alla grave minaccia individuata a norma della lettera a) del presente paragrafo; c) una relazione alla Commissione, entro una certa data o a intervalli regolari specificati nella

Ai sensi dell'art. 37 DSA, inoltre, i fornitori devono sottoporsi, a proprie spese e almeno una volta all'anno, a revisioni indipendenti volte a valutare il rispetto delle norme sui doveri di diligenza di cui al Capo III del Digital Services Act e degli impegni assunti attraverso i codici di condotta di cui agli artt. 45 e 46 DSA e i protocolli di crisi di cui all'art. 48 DSA. Le revisioni in questione sono effettuate da organizzazioni indipendenti e che non devono presentare conflitti di interesse né con i fornitori né con persone giuridiche a questi connesse (art. 37, par. 3, lett. a) DSA). Queste organizzazioni, inoltre, devono essere dotate di «comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche[97]» oltre che di «comprovata obiettività e deontologia professionale, basata in particolare sull'adesione a codici di condotta o standard appropriati[98]». Si tratta, quindi, di revisori privati, le cui caratteristiche si fondano, anch'esse, su strumenti di *private regulation*, ed in particolare i codici di condotta, i migliori standard o le *best practice* dei settori di loro pertinenza.

Il carattere privato di queste organizzazioni aveva portato certa dottrina[99] a sollevare – in occasione dei commenti alla proposta del dicembre 2020 – alcune preoccupazioni in merito alle garanzie circa la loro effettiva indipendenza, in particolare per via della mancanza di sistemi di vigilanza sull'operato delle stesse («*auditing the auditors*[100]») all'interno della predetta proposta. La versione finale del Digital Services Act continua a non contemplare sistemi del

decisione, in merito alle valutazioni di cui alla lettera a), sul contenuto preciso, l'attuazione e l'impatto qualitativo e quantitativo delle misure specifiche adottate a norma della lettera b) e su qualsiasi altra questione connessa a tali valutazioni o misure, come specificato nella decisione».

[97] Art. 37, par. 3, lett. b) DSA.

[98] Art. 37, par. 3, lett. c) DSA.

[99] V. a questo proposito: CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 771; BURI, J. VAN HOBOKEN, *op. cit.* n. 3, p. 37.

[100] CAUFFMAN, C. GOANTA, *op. ult cit.*, idem.

genere ma contiene un nuovo art. 37, par 7 DSA, che conferisce alla Commissione europea il potere di adottare atti delegati allo scopo di integrare il regolamento stabilendo le norme necessarie per lo svolgimento delle revisioni in commento, in particolare per quanto riguarda «la regolamentazione necessaria per le fasi procedurali, le metodologie di revisione e i modelli di comunicazione delle revisioni» effettuate a norma del medesimo art. 37 DSA. Gli atti delegati devono, inoltre, tenere conto di eventuali standard di revisione volontari a norma dell'art. 44, par. 1, lett. e) DSA (su cui v. *infra*: par. 4.4). Occorrerà attendere l'adozione di tali atti delegati e la piena applicabilità del Digital Services Act, con la conseguente operatività delle organizzazioni revisori, per verificare la reale indipendenza e il funzionamento delle stesse.

Oltre a questi meccanismi di revisione gestiti da soggetti privati, il Digital Services Act, allo scopo di facilitare il controllo delle attività dei fornitori di piattaforme online di dimensioni molto grandi da parte delle autorità pubblica, prevede che gli stessi siano obbligati a fornire al coordinatore dei servizi digitali del proprio luogo di stabilimento o alla Commissione europea, su richiesta degli stessi, l'accesso ai dati necessari per monitorare e valutare la loro conformità al regolamento (art. 40, par. 1 DSA). I termini e le modalità con cui possono essere presentate queste richieste, così come gli obblighi di collaborazione con le autorità che sorgono in capo ai fornitori delle piattaforme in conseguenza delle stesse, sono disciplinati nel dettaglio dall'art. 40 DSA. Anche su questo, peraltro, l'art. 40, par. 13 DSA attribuisce alla Commissione il potere di adottare atti delegati stabilendo le condizioni tecniche alle quali i fornitori devono condividere i dati richiesti e le finalità per cui questi ultimi possono essere utilizzati.

Per concludere l'analisi delle disposizioni relative ai fornitori di piattaforme online di dimensioni molto grandi, occorre evidenziare come esse impongano

ai propri destinatari ulteriori obblighi di trasparenza, sia per quanto riguarda la pubblicità online (art. 39 DSA) che per quanto riguarda il contenuto delle relazioni di cui all'art. 15 DSA (art. 42 DSA). Sotto il profilo della responsabilizzazione va, infine, citato l'art. 41 DSA, ai sensi del quale i fornitori di piattaforme online di dimensioni molto grandi sono obbligati ad istituire al proprio interno una funzione di controllo sulla conformità alle norme del regolamento («*compliance function*» in inglese) indipendente dalle funzioni operative e composta da uno o più responsabili della conformità («*compliance officer*»). I compiti di questa funzione – la quale deve essere dotata dall'autorità, lo status e le risorse sufficienti, nonché avere accesso all'organo di gestione dei fornitori – sono descritti nel dettaglio dall'art. 41 DSA e paiono assimilabili a quelli della figura del responsabile per la protezione dei dati («*data protection officer*» o «DPO») di cui all'art. 37 GDPR.

4.4 La promozione di strumenti di autoregolamentazione e coregolamentazione: standard di settore, codici di condotta, protocolli di crisi

Il Capo III relativo alle regole sui doveri di diligenza dei prestatori di servizi intermediari si conclude con alcune norme (art. 44-48 DSA) che, analogamente a quanto avviene in altri testi normativi dell'Unione come il Regolamento P2B (v. *supra*: Cap. 2, par. 3.1) o il GDPR (v. *supra*: Cap. 4, par. 3.2.1, 3.2.2), promuovono lo sviluppo di strumenti tipici di autoregolamentazione o di coregolamentazione[101] per favorire il rispetto del Digital Services Act e orientare il potere regolatorio dei *provider*.

I primi di questi strumenti, considerati dall'art. 44 DSA, sono gli standard di settore (indicati con l'espressione «norme volontarie» nella versione italiana del regolamento) stabiliti dai competenti organismi di standardizzazione (o

[101]Diversi riferimenti espliciti alle nozioni di «autoregolamentazione» e «coregolamentazione» sono contenuti nel Digital Services Act, ed in particolare nei considerando 88, 89, 104 e 106.

«normazione» secondo la dicitura del medesimo art. 44, par. 1 DSA) internazionali o europei[102]. In particolare, l'art. 44 DSA prevede che la Commissione europea, previa consultazione con il comitato di cui all'art. 61 DSA, promuova e sostenenga «lo sviluppo e l'attuazione» di tali standard con lo scopo primario di agevolare il rispetto degli obblighi del regolamento la cui attuazione può richiedere l'utilizzo di mezzi tecnologici[103]. Al tal fine, la norma elenca alcune materie a proposito delle quali dovrebbero concentrarsi gli sforzi della Commissione[104]. Tra queste, val la pena menzionare la presentazione in via elettronica delle segnalazioni ex art. 16 DSA (v. *supra*: par. 4.2), la comunicazione con gli utenti in merito alle restrizioni previste dalle condizioni generali dei fornitori, le attività di revisione delle piattaforme di dimensioni molto grandi di cui all'art. 37 DSA (v. *supra*: par. 4.3.3). Ad esse si aggiungono la pubblicità online, i sistemi di raccomandazione, l'accessibilità e la protezione dei minori online. Va segnalata, peraltro, la mancanza della presentazione dei reclami contro le decisioni dei fornitori ai sensi dell'art. 20 DSA, criticata in dottrina[105].

L'adozione di questi standard da parte dei *provider*, che il legislatore ribadisce essere facoltativa, non garantisce la conformità con il regolamento, anche se viene indicata come utile allo scopo, soprattutto per i fornitori di piccole dimensioni[106]. È importante, inoltre, sottolineare come lo sviluppo e l'attuazione di tali norme, così come il loro aggiornamento alla luce degli sviluppi tecnologici e dei comportamenti degli utenti, debbano essere soltanto soste-

[102] Il Digital Services Act non fornisce alcuna esemplificazione relativa a questi organismi. Appare tuttavia possibile ricondurre tra gli stessi l'Iso e simili organizzazioni da noi già menzionate in occasione dell'analisi del fenomeno del *transnational private regulation* e del ruolo dei meta-regolatori (v. *supra*: Cap. 4, par. 1.3.1).
[103] Considerando 101 DSA.
[104] V. art. 44, par. 1 DSA per il relativo elenco.
[105] C. GOANTA, P. ORTOLANI, *op. cit.* Cap. 5, n. 6, p. 23, i quali parlano di «*missed opportunity*».
[106] Considerando 101 DSA.

nuti e promossi dalla Commissione e non richiedano, a differenza di altri strumenti di *private regulation* previsti dal GDPR (v. Cap. 4, par. 3.2.2), un'approvazione formale da parte dell'autorità pubblica. L'influenza del regolatore pubblico sulla produzione e sul contenuto di questi standard è quindi soltanto meramente indiretta.

Altri strumenti di autoregolamentazione (o, a seconda dei casi, di coregolamentazione[107]) sono i più volte citati codici di condotta (v. *supra*: Cap. 2, par. 3.1; Cap. 4, par. 3.2.1, 3.2.2; Cap. 5, par. 1.2.2), che il Digital Services considera agli artt. 45-47.

In primo luogo, l'art. 45, par. 1 DSA, con una formulazione analoga all'art. 17 Regolamento P2B, stabilisce che la Commissione e il comitato ex art. 61 DSA incoraggino e agevolino l'elaborazione di «codici di condotta volontari a livello di Unione» per contribuire alla corretta applicazione del Digital Services Act. La norma prosegue poi aggiungendo che i codici in questione debbano tenere conto della «sfide» connesse alla lotta alla diffusione di contenuti illegali in rete e ai rischi sistemici, in conformità con il diritto dell'Unione e, in particolare, con le norme in materia di concorrenza e protezione dei dati personali. Più specifico è l'art. 45, par. 2 DSA secondo cui, nel caso di rischi sistemici significativi di cui all'art. 34, par. 1 DSA e che riguardano diverse piattaforme (o motori di ricerca) di dimensioni molto grandi, la Commissione può invitare i fornitori di queste e di altre, nonché i *provider* di servizi diversi e, se opportuno, le autorità competenti, a partecipare all'elaborazione dei codici di condotta, anche stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un quadro di comunicazione periodica sulle misure adottate e sui relativi risultati.

[107] V. considerando 104 DSA.

Le disposizioni richiamate, pur non prevedendo un procedimento di formale approvazione da parte dell'autorità pubblica, configurano una situazione differente rispetto al mero incoraggiamento previsto dall'art. 44 DSA per gli standard di *private regulation* o dall'art. 17 Regolamento P2B. In esse, infatti, il regolatore pubblico riveste un ruolo più incisivo, in quanto stabilisce *ex ante* i parametri a cui i codici di condotta dovrebbero adeguarsi, individua dei limiti precisi nel diritto dell'Unione e, nel caso delle piattaforme di dimensioni molto grandi, può assumere esso stesso un ruolo di iniziativa ai fini dell'elaborazione di questi strumenti. In altre parole, sulla scorta anche delle esperienze dei codici contro la disinformazione e contro l'odio online esplicitamente richiamate dal nuovo regolamento[108], i codici di cui all'art. 45 DSA assumono le sembianze di strumenti di coregolamentazione piuttosto che di autoregolamentazione pura, rimanendo comunque fermo il loro carattere volontario[109].

Ciò appare confermato anche da quanto disposto dai paragrafi 3 e 4 del medesimo articolo, che conferiscono ulteriori compiti alla Commissione e al comitato ex art. 61 DSA, chiamati ad orientare e vigilare ulteriormente l'attività regolatoria delle piattaforme[110]. Tali compiti riguardano, innanzi tutto, l'impe-

---

[108] Si veda a questo proposito il considerando 106 DSA: «Le norme sui codici di condotta ai sensi del presente regolamento potrebbero fungere da base per le iniziative di autoregolamentazione già stabilite a livello dell'Unione, tra cui l'impegno per la sicurezza dei prodotti, il protocollo d'intesa sulla vendita di merci contraffatte via internet, il codice di condotta per lottare contro le forme illegali di incitamento all'odio online nonché il codice di buone pratiche sulla disinformazione. In particolare, tale codice di buone pratiche sulla disinformazione è stato rafforzato, seguendo gli orientamenti della Commissione, come annunciato nel piano d'azione per la democrazia europea».

[109] V. in questo senso: C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 768.

[110] V. in questo senso considerando 103 DSA, secondo cui: «[…] l'attuazione dei codici di condotta dovrebbe essere misurabile e soggetta a controllo pubblico, tuttavia ciò non dovrebbe pregiudicare il carattere volontario di tali codici e la libertà delle parti interessate di decidere se aderirvi […]».

gno affinché i codici di condotta definiscano chiaramente i propri obiettivi specifici, contengano indicatori chiave di prestazione[111] per misurare il conseguimento di tali obiettivi e tengano debitamente conto delle esigenze e degli interessi di tutte le parti interessate, in particolare dei cittadini, a livello di Unione. A questi impegni si affiancano quelli di garantire che i partecipanti alle iniziative di regolamentazione riferiscano periodicamente alla Commissione e ai coordinatori dei servizi digitali dei relativi luoghi di stabilimento in merito a tutte le misure adottate e ai relativi risultati. Infine, alla Commissione e al comitato spetta il compito di valutare se i codici rispondano alle finalità perseguite dalle disposizioni in commento, così come quello di monitorare e valutare periodicamente il conseguimento degli obiettivi degli stessi. A tale scopo, la Commissione e il comitato incoraggiano e agevolano anche il riesame e l'adattamento periodico dei codici di condotta e, in caso di inottemperanza sistematica agli stessi, possono invitare i firmatari dei codici di condotta a adottare le misure ritenute necessarie.

Sulla stessa scia dell'art. 45 si collocano i successivi artt. 46 e 47 DSA relativi, rispettivamente, ai codici di condotta per la pubblicità online e a quelli per l'accessibilità. Per entrambi è, infatti, previsto che la Commissione ne incoraggi e ne faciliti l'elaborazione a livello di Unione, con l'indicazione anche dei

[111] Il terzo period dell'art. 45, par. 3 DSA specifica: «Gli indicatori chiave di prestazione e gli obblighi di comunicazione tengono conto delle differenze esistenti tra i diversi partecipanti in termini di dimensioni e capacità».

soggetti che devono prendere parte[112] o essere coinvolti[113] nei relativi procedimenti di elaborazione. Tra questi, vale la pena menzionare, in quanto spia dell'approccio del legislatore improntato alla coregolamentazione, organizzazioni private come quelle che rappresentano gli utenti e quelle della società civile nonché, ove opportuno, le autorità (pubbliche) competenti. Entrambe le norme specificano, inoltre, le finalità perseguite dall'adozione dei codici da esse considerati, nonché il contenuto e gli obiettivi che queste dovrebbero perseguire. Sono previsti, altresì, i medesimi termini temporali entro cui elaborare e applicare entrambi i codici[114]. Anche su questi particolari strumenti, pertanto, il regolatore pubblico esercita un'influenza significativa, non limitata ad un mero incoraggiamento.

Gli ultimi strumenti considerati dalle norme in commento (ed in particolare dall'art. 48 DSA) sono i protocolli di crisi volontari per affrontare situazioni di crisi, ossia situazioni «strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica e sulla salute pubblica[115]». Si tratta di strumenti di coregolamentazione rivolti ai fornitori di piattaforme online e di motori di ricerca online di dimensioni molto grandi nonché, ove opportuno, a quelli delle piattaforme e dei motori di ricerca di tipo diverso. È previsto che l'elaborazione di questi protocolli venga effettuata congiuntamente dalla

[112] Art. 46, par. 1 DSA: «La Commissione incoraggia e agevola l'elaborazione di codici di condotta volontari a livello di Unione da parte dei fornitori di piattaforme online e altri fornitori di servizi interessati, quali i fornitori di servizi intermediari per la pubblicità online, altri soggetti coinvolti nella catena del valore della pubblicità programmatica, o le organizzazioni che rappresentano i destinatari del servizio e le organizzazioni della società civile o le autorità competenti […]».

[113] Art. 47, par. 1 DSA: «La Commissione incoraggia e facilita l'elaborazione di codici di condotta a livello dell'Unione con il coinvolgimento dei fornitori di piattaforme online e altri fornitori di servizi interessati, delle organizzazioni che rappresentano i destinatari del servizio e delle organizzazioni della società civile o delle autorità competenti […]».

[114] Si tratta, rispettivamente, del 18 febbraio 2025 per l'elaborazione e del 18 agosto 2025 per l'applicazione.

[115] Art. 48, par. 1 DSA.

Commissione europea – eventualmente a seguito della raccomandazione del Comitato – e dai *provider*, con il coinvolgimento, ove ritenuto opportuno dall'Esecutivo, delle autorità degli Stati membri, delle istituzioni, gli organi e gli organismi dell'Unione e delle «organizzazioni della società civile o altre organizzazioni competenti nell'elaborazione dei protocolli di crisi».

Il ruolo della Commissione nell'elaborazione e nell'applicazione di questi protocolli risulta molto incisivo. Infatti, oltre ad avere potere d'impulso e a stabilire i soggetti che devono prendere parte alle procedure di elaborazione, la stessa è incaricata di provvedere affinché tali protocolli contengano una o più misure ed elementi specificamente indicati, rispettivamente, ai paragrafi 2 e 4 dell'art. 48 DSA. Ciò ad ulteriore riprova di come la promozione di meccanismi di coregolamentazione e di autoregolamentazioni da parte del Digital Services Act non valga a mettere in dubbio la preminenza del regolatore pubblico rispetto a quello privato.

5 Attuazione, cooperazione, sanzioni, esecuzione (cenni)

Dopo la disciplina in materia di responsabilità dei *provider* e quella relativa ai doveri di diligenza di questi ultimi, il Digital Services Act si chiude con un articolato capo IV (di ben quarantasette articoli: artt. 49-86 DSA) dedicato all'attuazione e all'esecuzione del regolamento, anche per quanto riguarda la cooperazione e il coordinamento tra le autorità competenti, nonché l'irrogazione di sanzioni pecuniarie e di penalità di mora. Si tratta di aspetti che sono stati condensati da certa dottrina con l'espressione «*digital enforcement*[116]» e dei quali, non essendo possibile soffermarsi su di essi con pretese di esaustività, si tenterà qui in chiusura di tracciare soltanto un quadro di massima.

Soggetti chiave di queste attività di *enforcement* sono le «autorità competenti», incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione

[116] C. CAUFFMAN, C. GOANTA, *op. cit.* n. 3, p. 772.

del regolamento all'interno degli Stati membri (artt. 49-55 DSA). Tra queste ricoprono un'importanza fondamentale i già citati «coordinatori dei servizi digitali», che ciascuno Stato membro ha l'obbligo di designare tra le proprie autorità competenti e che sono responsabili di tutte le questioni relative alla vigilanza e all'applicazione del regolamento all'interno dei propri paesi, oltre che di garantire il coordinamento a livello nazionale in relazione a tali questioni e di contribuire alla vigilanza e all'applicazione efficaci e coerenti del Digitali Services Act in tutta l'Unione (art. 49 DSA). I coordinatori dei servizi digitali hanno diversi poteri elencati all'art. 51 DSA, tra cui rientrano i poteri d'indagine in merito alla condotta dei fornitori che ricadono nella competenza del loro Stato membro (art. 51 e 56 DSA – su cui v. *infra*). A questi si aggiungono diversi poteri interdittivi o correttivi, il potere di imporre sanzioni pecuniarie o penalità di mora e quello di adottare misure provvisorie, ciascuno dei quali può essere esercitato direttamente oppure mediante richiesta che ogni coordinatore può presentare all'autorità giudiziaria del proprio Stato membro.

Quanto al contenuto di questi poteri, l'art. 52 DSA prevede che ciascuno Stato membro adotti le norme relative alle sanzioni applicabili in caso di violazione del regolamento e adotti le misure necessarie per assicurarne l'applicazione. Le sanzioni in questioni devono arrivare, nel massimo, al 6% del fatturato annuo mondiale del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente. Si tratta di un importo molto elevato, che fa di tali sanzioni un elemento fondamentale nell'impianto del Digital Services Act e rende le stesse ascrivibili al filone delle «*market destroying measure*» da noi già richiamato, al pari di quelle previste da altri strumenti come il GDPR (Cap. 4, par. 3.2.3). Alle sanzioni si affiancano le penalità di mora, il cui importo massimo giornaliero deve essere pari al 5% del fatturato giornaliero medio mondiale o del reddito del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente (art. 52, par. 4 DSA).

Il successivo art. 53 DSA chiarisce che ciascun destinatario del servizio[117] ha il diritto di presentare un reclamo contro i fornitori di servizi intermediari in merito alla violazione del regolamento presso il coordinatore dei servizi digitali dello Stato membro in cui egli è situato o è stabilito. Il coordinatore in questione valuta il reclamo e, se del caso, lo trasmette a quello del luogo di stabilimento del *provider*, accompagnato, ove ritenuto appropriato, da un parere. Sempre a tutela dei destinatari dei servizi, l'art. 54 DSA chiarisce come gli stessi abbiano anche il diritto di chiedere *ai provider*, in conformità con il diritto dell'Unione e nazionale, il risarcimento dei danni o delle perdite subite a seguito di una violazione degli obblighi stabiliti dal regolamento da parte degli stessi.

Quanto alla competenza, l'art. 56, par. 1 DSA stabilisce che lo «Stato membro» in cui è situato lo «stabilimento principale[118]» del fornitore di servizi intermediari coinvolto dispone di poteri esclusivi per la vigilanza e l'applicazione del regolamento, fatti salvi i poteri attribuiti alla Commissione europea dai paragrafi 2, 3 e 4 del medesimo articolo. Di conseguenza, i poteri in questione possono essere esercitati soltanto dalle autorità competenti di tale Stato, il cui coordinatore dei servizi digitali è l'unico a poter decidere sui reclami presentanti dagli utenti nei confronti dello specifico fornitore. Nel caso di *provider* stabilit0 al di fuori dell'Unione ma ricadente nell'ambito di applicazione del Digital Services Act secondo le regole unilateraliste da noi ricordate (v. *supra*: par. 2), la competenza spetta, di norma, allo Stato membro in cui questi ha nominato il proprio legale rappresentante[119]. Nell'ipotesi in cui un fornitore

[117] Il diritto in questione è attribuito, oltre che ai destinatari dei servii anche agli «organismi, le organizzazioni o le associazioni incaricati di esercitare per loro conto i diritti conferiti dal […] regolamento» (art. 53, par. 1 DSA).

[118] Ai sensi del considerando 123 DSA, si tratta dello Stato membro «in cui il prestatore ha la sua sede principale o sociale nella quale sono esercitate le principali funzioni finanziarie e il controllo operativo».

[119] V. nota 23.

non abbia provveduto alla nomina è previsto, nell'interesse dell'efficace applicazione del regolamento[120], che tutti gli Stati membri – o, nel caso di fornitori di piattaforme (o di motori di ricerca) online di dimensioni molto grandi, la Commissione europea – dispongono dei poteri di vigilanza e di applicazione appena richiamati.

Da segnalare, a questo proposito, come il Digital Services Act non contenga norme relative alla competenza giurisdizionale, nonostante i coordinatori dei servizi digitali possano, come si è visto, rivolgersi all'autorità giudiziaria dei loro Stati membri per esercitare i propri poteri e nonostante l'art. 54 DSA riconosca il diritto al risarcimento dei danni a favore di ciascun utente. Al contrario, come già notato (v. *supra*: par. 2.2), il regolamento fa salve le norme dell'Unione europea in materia di competenza giurisdizionale, ed in particolare il Regolamento Bruxelles I*bis*. Di conseguenza, la risoluzione dei conflitti di giurisdizione nelle controversie relative alla violazione delle norme del Digital Services Act, incluse quelle sul risarcimento dei danni ex art. 54 DSA, dovrebbe avvenire in base ad esse.

Sempre in tema di competenze delle autorità, gli artt. 57-60 DSA prevedono diverse disposizioni relative all'assistenza reciproca (art. 57 DSA), la cooperazione transfrontaliera tra coordinatori dei servizi digitali (art. 58 DSA) e lo svolgimento di indagini comuni da parte degli stessi (art. 60 DSA), funzionali a garantire la collaborazione tra le varie autorità competenti nel caso di situazioni transfrontaliere, assai comuni in materia di servizi digitali.

Nell'ottica di favorire la cooperazione tra le attività competenti, va menzionato, inoltre, l'art. 61 DSA, il quale prevede la costituzione del già citato «comitato europeo per i servizi digitali» (o più semplicemente «comitato» – v. *su-*

[120] V. considerando 123 DSA.

pra: par. 4.3.3), quale gruppo consultivo indipendente composto dai coordinatori dei servizi digitali di ciascuno Stato membro[121]. Tale organismo fornisce consulenza alla Commissione europea e ai coordinatori dei servizi digitali al fine di raggiungere determinati obiettivi[122] relativi all'applicazione coerente del regolamento, alla promozione della cooperazione efficace tra autorità competenti e all'assistenza nella vigilanza sulle piattaforme online di dimensioni molto grandi. Oltre alla consulenza, ove necessario per il raggiungimento dei predetti obiettivi, l'art. 62 DSA attribuisce al comitato il compito di sostenere il coordinamento delle indagini congiunte, assistere le autorità competenti nell'analisi delle relazioni e dei risultati delle revisioni di piattaforme online (o di motori di ricerca) di dimensioni molto grandi e quello di sostenere e promuovere l'elaborazione e l'attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei in cooperazione con i relativi portatori di interessi nonché l'individuazione di questioni emergenti in relazione alle materie disciplinate dal regolamento. In altre parole, il comitato viene a ricoprire un ruolo importante ai fini dell'elaborazione degli strumenti di autoregolamentazione e coregolamentazione esaminati in precedenza (v. *supra*: par. 4.4).

A livello contenutistico, occorre aggiungere come il Capo IV in commento dedichi un'intera sezione (la 4, artt. 64-83 DSA) alla vigilanza, le indagini e il monitoraggio relativi ai fornitori di piattaforme online (e di motori di ricerca) di dimensioni molto grandi. In essa, un ruolo preminente viene assunto dalla Commissione europea, a cui sono attribuiti dettagliati poteri ispettivi, istruttori e sanzionatori, oltre che di vigilanza e monitoraggio in merito al rispetto

[121] V. art. 62 DSA per la struttura del comitato stesso.
[122] Nel dettaglio v. art. 61, par. 2 DSA.

del regolamento. Tra questi, va menzionata l'irrogazione di sanzioni pecuniarie (art. 74 DSA) o di penalità di mora (art. 76 DSA) che soggiacciono ai medesimi limiti previsti per le sanzioni applicabili agli altri *provider*.

In conclusione, si può affermare che la previsione di un regime così articolato dimostri l'importanza attribuita dal legislatore dell'Unione all'attività delle autorità pubbliche nell'impianto Digital Services Act. Questo nonostante la valorizzazione del potere regolatorio dei *provider* operata dallo stesso regolamento e il bisogno strutturale del regolatore pubblico della collaborazione dei medesimi fornitori per il concreto svolgimento delle menzionate attività di *enforcement* (v. *supra*: Cap. 3, par. 5.3). Come nel caso del GDPR, appare a tal proposito significativa la previsione di sanzioni pecuniarie elevate, volte a garantire il rispetto dei principi e delle regole del Digital Services Act da parte dei *provider* anche svolgendo la funzione di «*market destroying measure*» (Cap. 4, par. 3.2.3). Si tratta dell'ennesimo indizio emerso nel corso del presente lavoro a sostegno della tesi per cui il regolatore pubblico, pur prendendo atto della necessità di rapportarsi e di collaborare con il regolatore privato, o anche soltanto di riconoscerne il potere regolatorio, ai fini della regolamentazione delle piattaforme digitali, non rinunci a collocarsi su un livello, quanto meno formalmente, superiore allo stesso.

Conclusioni

L'indagine svolta ha messo in luce le ragioni che inducono a tenere in debita considerazione, nella regolamentazione delle piattaforme digitali, il potere regolatorio dei gestori delle stesse. Ciò vale per la disciplina dei rapporti riconducibili tanto alla «dimensione verticale» della vita di relazione che si svolge nelle piattaforme, quanto alla «dimensione orizzontale» della stessa (v. Cap. 1, par. 2).

L'asserzione che precede è confermata dalle tendenze normative e giurisprudenziali registratesi negli ultimi decenni all'interno dell'Unione europea, su cui si è concentrato il presente lavoro.

In particolare, dal punto di vista del diritto materiale, si è avuto modo di osservare come si sia passati da un regime fondato sull'irresponsabilità degli *internet service provider* per le informazioni condivise dai propri utenti – pur con le differenze di cui si è dato conto (v. Cap. 2, par. 2.1) – ad una progressiva responsabilizzazione («*accountability*») di tali soggetti, tra cui rientrano, al netto dei problemi qualificatori affrontati (v. Cap. 2, par. 4), i gestori delle piattaforme digitali.

I segnali più evidenti di questa evoluzione si ritrovano, innanzi tutto, nella giurisprudenza della Corte di Giustizia relativa all'interpretazione dell'art. 15 della *e-Commerce Directive* e alla creazione della figura del c.d. «*hosting provider* attivo» (v. Cap. 2, par. 2.2). La tendenza si può, inoltre, rintracciare in diversi strumenti normativi in materia di piattaforme digitali adottati dall'Unione europea negli ultimi anni. Tra questi, abbiamo visto la Direttiva Copyright (v. Cap. 2, par. 2.3), il Regolamento P2B (v. Cap. 2, par. 3.1) e il recentemente approvato Digital Services Act (v. Cap. 6). Quest'ultimo, tra le altre cose, ha modificato il regime di (ir)responsabilità degli *internet service provider* di cui alla

Direttiva e-Commerce, recependo le indicazioni della Corte di Giustizia sull'*hosting provider* attivo (v. Cap. 6, par. 3) e prevedendo ulteriori obblighi per specifici tipi di piattaforme.

In linea con le strategie delineate dalla Commissione europea (v. Cap. 4, par. 3.1) gli strumenti richiamati, accanto alla tradizionale «*top-down regulation*», valorizzano il potere regolatorio dei gestori delle piattaforme facendo utilizzo della tecnica della coregolamentazione.

In più occasioni, infatti, il legislatore dell'Unione è sembrato riconoscere come i gestori delle piattaforme si trovino in una posizione migliore per regolare determinate materie o fattispecie – tra cui abbiamo sottolineato, in particolare, il contrasto alla diffusione di contenuti illeciti (v. Cap. 5) – e financo per esercitare, all'interno dei propri ambienti, funzioni para-giurisdizionali (v. Cap. 2, par. 2.3, 3.1; Cap. 6, par. 4.2, 4.3.1, 4.3.3). Su questa premessa, il legislatore dell'Unione, piuttosto che cercare di soffocare il potere regolatorio dei gestori, ha tentato di controllarlo, orientandolo al raggiungimento degli obiettivi da esso stabiliti (v. Cap. 4, par. 3.2).

Vari sono gli strumenti a tal fine utilizzati dal legislatore. Tra questi abbiamo citato i codici di condotta, la cui elaborazione e adozione da parte dei regolatori privati sono in alcune occasioni incoraggiate dal diritto dell'Unione, come nel caso del Regolamento P2B (v. Cap. 2, par. 3.1) o del Digital Services Act (v. Cap. 6, par. 4.4), mentre in altre soggiacciono a procedimenti di approvazione formale da parte delle autorità competenti, come avviene nel GDPR (v. Cap. 4, par. 3.2.2). Esempi di codici di condotta sono quello contro l'odio online e quello di buone pratiche contro la disinformazione, entrambi adottati dalla Commissione europea e da diversi attori di primo piano dell'economia digitale, inclusi alcuni tra i gestori delle maggiori piattaforme (v. Cap. 5, par. 1.2.2).

Nell'ambito della medesima strategia, il legislatore dell'Unione è in più occasioni intervenuto in maniera più incisiva, tentando di plasmare esso stesso

il contenuto delle norme stabilite dai regolatori privati e ponendo enfasi sulla trasparenza e sull'«*accountability*» di questi ultimi. A tal riguardo, abbiamo visto, ad esempio, come sia la Direttiva Copyright (v. Cap. 2, par. 2.3), che il Regolamento P2B (v. Cap. 2, par. 3.1) o il Digital Services Act (v. Cap. 6, par. 4.1) impongano ai gestori delle piattaforme l'obbligo di conformare in determinati modi le regole da essi stabilite per disciplinare i loro rapporti contrattuali gli utenti, siano tali regole denominate «condizioni generali», «termini e condizioni» o in altro modo.

Vi è di più. Gli strumenti citati impongono, infatti, ai rispettivi destinatari di istituire dei sistemi di gestione dei reclami presentanti dagli utenti con riferimento a determinate controversie sorte nell'ambito delle piattaforme. In altre parole, in questi casi, il legislatore finisce con il conferire funzioni para-giurisdizionali ai gestori delle piattaforme, seppur nei limiti delineati dai testi normativi richiamati. A ben vedere, peraltro, non si tratta di un conferimento vero e proprio quanto piuttosto di un riconoscimento, a cui si lega il tentativo di orientare anche le suddette funzioni. Infatti, la presenza di meccanismi interni di gestione dei reclami caratterizzava diversi sistemi di autoregolamentazione sorti nell'ambito di piattaforme digitali già prima dell'intervento del legislatore dell'Unione. Tra i meccanismi in questione, abbiamo qui abbiamo sottolineato il Facebook Oversight Board, che ne costituisce l'esempio più avanzato (v. Cap. 5, par. 2).

Da quanto sopra, emerge come il legislatore dell'Unione, nei vari tentativi di disciplinare le piattaforme digitali susseguitisi negli ultimi anni, abbia considerato e consideri sempre con maggiore importanza la «dimensione istituzionale» di tali ambienti e il potere regolatorio dei loro gestori. Ciò detto, allo stato non sembra, tuttavia, che il diritto dell'Unione consideri la regolamentazione privata («*private regulation*») delle piattaforme sullo stesso livello di quella di fonte pubblica e quindi, in buona sostanza, di sé stesso.

L'indagine svolta dimostra, al contrario, come la valorizzazione della «dimensione istituzionale» delle piattaforme e del potere regolatorio dei gestori ad esse preposti non passi mai attraverso una «delega» di funzioni quanto, piuttosto, dal tentativo di orientare tale potere attraverso l'utilizzo di tecniche di coregolamentazione di vario genere, in cui il ruolo dei regolatori pubblici risulta, a seconda dei casi, più o meno incisivo. Tali tecniche, come si è notato, hanno come denominatori comuni i principi della trasparenza e della «*accountability*» (v. Cap. 4, par. 3.2.3), fondamentali nel quadro della strategia delineata dalla Commissione europea.

Un'ulteriore prova dell'assenza di parificazione tra il diritto di fonte pubblica e la *private regulation* nell'ambito delle piattaforme emerge dalle osservate tendenze del diritto internazionale privato dell'Unione (v. Cap. 3).

Si è visto, infatti, come le norme internazionalprivatistiche oggi in vigore – ed in particolare, per quanto qui di interesse, il Regolamento Bruxelles I*bis*, il Regolamento Roma I e il Regolamento Roma II – siano soltanto parzialmente in grado di rispondere a tutti gli interrogativi posti dal fenomeno delle piattaforme. Le difficoltà principali risiedono, come osservato, nelle logiche «statocentriche» e legate al concetto della territorialità su cui si fondano le suddette norme, che mal si attagliano ad ambienti come le piattaforme, caratterizzate da scarsi ancoraggi territoriali e dalla grande importanza della regolamentazione dei gestori privati (v. Cap. 3, par. 1.2).

Tuttavia, la ricerca di nuovi paradigmi non permette ad oggi di individuare uno spazio maggiore per la regolamentazione di fonte diversa da quella pubblica. Al contrario, infatti, dall'indagine svolta emerge una duplice tendenza, in cui la *private regulation* riveste ancora un ruolo marginale a fini internazionalprivatistici.

La prima tendenza, di tipo giurisprudenziale, è rappresentata dal tentativo di adattare le tradizionali norme di diritto internazionale privato dell'Unione

al mondo virtuale, individuando *ex novo* o mutuando criteri di collegamento utilizzati per altre situazioni (Cap. 3, par. 2, 3, 4).

La seconda tendenza è invece di tipo legislativo e si rinviene in diversi strumenti di diritto materiale considerati nel presente lavoro, tra cui il GDPR, il Regolamento P2B o il Digital Services Act. Questi strumenti contengono, infatti, al proprio interno norme di chiara matrice «unilateralista», che ne determinano autonomamente l'ambito di applicazione territoriale, oltre che quello materiale, prescindendo dalle norme di conflitto (v. Cap. 3, par. 5.1). Si tratta di una tendenza non esclusiva dell'Unione europea, che segnala il tentativo dei regolatori pubblici di estendere la propria sovranità sulla rete e in cui non vi è spazio, a fini internazionalprivatisti, per la *private regulation*.

Il rischio principale di questa impostazione è rappresentato dal «*regulatory overreaching*», fenomeno proprio di norme che si propongono di disciplinare situazioni con legami assai minimi con i rispettivi ordinamenti e che hanno in realtà poche possibilità di applicazione reale alle fattispecie che si propongono di disciplinare. Nell'ambito delle piattaforme digitali, il rischio è acuito proprio dalla constatazione per cui i regolatori pubblici abbiano un bisogno strutturale della cooperazione dei gestori per ottenere l'effettiva applicazione delle proprie disposizioni all'interno dei predetti ambienti, come si è potuto notare nel presente lavoro (v. Cap. 3, par. 5.3). Al contrario, i gestori non hanno bisogno della cooperazione dei regolatori pubblici, dal momento che le loro regole non abbisognano di azioni coercitive esterne per poter essere applicate nell'ambito delle piattaforme, risultando quindi auto-esecutive («*self-enforcing*»).

In conclusione, il quadro attuale mostra come il diritto dell'Unione, nel disciplinare le questioni relative alle piattaforme digitali, riconosca e si relazioni con il potere regolatorio dei gestori delle stesse. Non è invece dato scorgere

l'impostazione di un rapporto paritario tra il diritto di fonte pubblica e la *private regulation* che caratterizza le piattaforme, né una delega formale da parte del primo a favore della seconda.

Al contrario, il legislatore dell'Unione sembra perseguire l'obiettivo di orientare l'attività del regolatore privato verso il rispetto dei propri fini, mantenendosi in una posizione, quanto meno formalmente, di preminenza. Ciò sembra corroborato anche dalla previsione, in diversi degli strumenti considerati nel presente lavoro, di sanzioni pecuniarie molto elevate, la cui applicazione necessita l'uso di quei poteri coercitivi su cui ad oggi i regolatori pubblici continuano a mantenere il monopolio. Ponendosi per un momento dal punto di vista delle piattaforme, infine, si è visto come anche la stessa Facebook Oversight Board Charter (v. Cap. 5, par. 2.3) sembri riconoscere – anche in questo caso, quanto meno formalmente – la natura subordinata delle regole del *social network* rispetto al diritto di fonte pubblica, avallando ulteriormente la conclusione cui si è giunti.

Le continue evoluzioni tecnologico-normative che contraddistinguono la materia suggeriscono comunque di prestare cautela e di mantenere costantemente monitorata la situazione. Non può infatti escludersi che, in un futuro non troppo remoto, la preminenza del regolatore pubblico rispetto a quello privato – con le conseguenze che questo comporta anche dal punto di vista internazionalprivatistico – si restringa al punto di risultare poco più che una vuota petizione di principio, imponendo quindi un ancor più radicale cambiamento dei paradigmi vigenti.

Bibliografia

Opere citate

AA.VV., *Massimario della giurisprudenza del lavoro*, numero straordinario, giugno 2020.

F. ABBONDANTE, *Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea*, in Informatica e diritto, Vol. 26, n. 1-2, pp. 41-68, 2017.

L. ALBERTINI, *La responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione sul ruolo di gatekeepers della comunicazione)*, apparso su IlCaso.it, 22 settembre 2020. Disponibile online: https://blog.ilcaso.it/news_996/22-09-20/La_responsabilita_civile_degli_internet_service_provider_per_i_materiali_caricati_dagli_utenti_%28con_qualche_considerazione_sul_ruolo_di_gatekeepers_della_comunicazione%29.

L. AMMANNATI, *Verso un diritto delle piattaforme digitali?*, in federalismi.it, n° 7, 2019. Disponibile al seguente link: https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=38331&content=&content_author=

N. APPELMAN, J.P. QUINTAIS, R. FAHY, *Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?*, apparso su Dsaobservatory.eu, 31 maggio 2021. Disponibile online: https://dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions.

N. APPELMAN, J.P. QUINTAIS, R. FAHY, *Using Terms and Conditions to apply Fundamental Rights to Content Moderation*, in H. RICHTER, M. STRAUB, E. TUCHTFELD

(a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, pp. 29-37, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021.

R. BALDWIN, M. CAVE, M. LODGE, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2010.

M. BARBIERI, *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in Labour & Law Issues, Vol. 7, n. 2, 2021. Disponibile online: https://labourlaw.unibo.it/article/view/14110.

J. BASEDOW, *Foundations of Private International Law in Intellectual Property*, in J. BASEDOW, T. KONO, A. METZGER (a cura di), *Intellectual Property in the Global Arena*, pp. 3-29. Mohr Siebeck, 2010.

M. BASSINI, *La Cassazione e il simulacro del provider attivo: mala tempora currunt*, in Media Laws, n. 2, pp. 248-257, 2019. Accessibile online: https://www.media-laws.eu/la-cassazione-e-il-simulacro-del-provider-attivo-mala-tempora-currunt/.

F. BASSAN, *Digital Platforms and Global Law*, Edward Elgar, 2021.

S. BASTIANON, *La lex sportiva*, in Osservatorio sulle fonti, fasc. 1, pp. 349-366. Disponibile online su: www.osservatoriosullefonti.it.

A. BECKERS, *Towards a Regulatory Private Law Approach for CSR Self- Regulation? The Effect of Private Law on Corporate CSR Strategies*, in European Review of Private Law, Vol. 27, n. 2, pp. 220-244, 2019.

P.S. BERMAN, *The Globalization of Jurisdiction*, in University of Pennsylvania Law Review, Vol. 151, n. 2, pp. 311-529, 2002.

M.E. BARTOLINI, *La regolamentazione privata nel sistema costituzionale dell'Unione europea. Riflessioni sulla disciplina relativa al settore dell'innovazione tecnologica*, in Osservatorio sulle fonti, fasc. 3, pp. 1331-1355, Disponibile in: http://www.osservatoriosullefonti.it

F. BIGNAMI-G. RESTA, *Human Rights Extraterritoriality: the Right to Privacy and National Security Surveillance*, in E. BENVENISTI, G. NOLTE (a cura di) *Community Interests Across International Law*, pp. 357-380, Oxford University Press, 2019.

R. BOCCHINI, *La responsabilità di facebook per la mancata rimozione di contenuti illeciti*, in Giur.it., fasc. 3, pp. 632-656, 2017.

J. BOMHOFF, A. MEUWESE, *The Meta-regulation of Transnational Private Regulation*, in Journal of Law and Society, Vol. 38, n. 1, pp. 138-162, 2011.

A. BONOMI, *The Rome I Regulation on the Law Applicable to Contractual Obligations: Some General Remarks*, in Yearbook of Private International Law, Vol. X, pp. 165-176, 2008.

A. BRADFORD, *The Brussels Effect,* in Northwestern University Law Review, Vol. 107, n. 1, pp. 1-67, 2012. Link SSRN: https://ssrn.com/abstract=2770634

A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

L. BRILMAYER, *Conflict of Laws: Foundations and Future Directions*, Little Brown & Co, 1991.

M. BRKAN, *Data Protection and European Private International Law*, Robert Schuman Centre for Advanced Studies Research Paper n. RSCAS 2015/40, 2015. Disponibile su SSRN: https://ssrn.com/abstract=2631116.

I. BURI, J. VAN HOBOKEN, *The Digital Services Act (DSA) Proposal: A Critical Overview*, DSA Observatory – Discussion paper, 2021.

I. BURI, J. VAN HOBOKEN, *The DSA Proposal's Impact on Digital Dominance*, in H. RICHTER, M. STRAUB, E. TUCHTFELD (a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, pp. 10-16, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021.

C. BUSCH, *Self-Regulation and Regulatory Intermediation in the Platform Economy*, in M. CANTERO GAMITO, H.W. MICKLITZ (a cura di), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, pp. 115-134, Edward Elgar, 2019.

C. BUSCH, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in A. DE FRANCESCHI, R. SCHULZE (a cura di) *Digital revolution - new challenges for law: data protection, artificial intelligence, smart products, blockchain technology and virtual currencies*, pp. 57-75, C.H. Beck-Nomos, 2019.

C. BUSCH, *The P2B Regulation (EU) 2019/1150: Towards a "procedural turn" in EU platform regulation?*, in Journal of European Consumer and Market Law, Vol. 9, n. 4, pp. 133-134, 2020.

P. BONINI, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in Federalismi.it, n. 11, pp. 265-281, 2020.

C. BUSCH, *Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation*, in UCLA Journal of Law & Technology, Vol. 27, n. 2, pp. 32-79, 2022.

L. A BYGRAVE, *Determining Applicable Law pursuant to European Data Protection Legislation*, in Computer Law and Security Report, Vol. 16, n. 4 pp. 252-257, 2000.

L. BYGRAVE, *Internet Governance by Contract*, Oxford Scholarship Online, 2015.

F. CAFAGGI, *The Architecture of Transnational Private Regulation*, EUI Working Paper LAW 2011/12, 2011.

F. CAFAGGI, *New Foundations of Transnational Private Regulation,* in Journal of Law and Society, Vol. 38, n. 1, pp. 20-49, 2011.

F. CAFAGGI, *A Comparative Analysis of Transnational Private Regulation: Legitimacy, Quality, Effectiveness and Enforcement*, EUI Working Paper LAW 2014/15, 2014.

F. CAFAGGI, *Regulating Private Regulators*, in S. CASSESE (a cura di), *Research Handbook on Global Administrative Law*, pp. 212-241, Edward Elgar 2016.

F. CAFAGGI, A. RENDA, *Measuring the Effectiveness of Transnational Private Regulation*, 2014. Disponibile su SSRN: https://ssrn.com/abstract=2508684.

F. CAFAGGI, A. RENDA, R. SCHMIDT, *Transnational Private Regulation*, in OECD, *International Regulatory Co-operation: Case Studies, Vol. 3: Transnational Private Regulation and Water Management*, pp. 9-58, OECD Publishing, 2013.

I. CALZADA, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in Smart Cities, Vol. 5, n. 3, pp. 1129-1150, 2022.

C. CAMPIGLIO, *La legge applicabile alle obbligazioni extracontrattuali (con particolare riguardo alla violazione della privacy)* in Rivista di diritto internazionale privato e processuale, Vol. 51, fasc. 4, pp. 857-866, 2015.

M. CANTERO GAMITO, *Regulation.com. Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda*, in European Journal of Legal Studies, Vol. 9, n. 2, pp. 53-68, 2017.

J. CARRASCOSA GONZALEZ, *The Internet – Privacy and Rights Relating to Personality*, in Collected Courses of The Hague Academy of International Law – Recueil des cours de l'Academie de droit international, Vol. 378, pp. 261-486, Brill Nijhoff, 2016.

C. CARUSO, *La libertà di espressione presa sul serio — CasaPound c. Facebook, Atto I*, apparso su SidiBlog.it, 20 gennaio 2020. Disponibile online: http://www.sidiblog.org/2020/01/20/la-liberta-di-espressione-presa-sul-serio-casa-pound-c-facebook-atto-i/.

M. CASTELLANETA, P. DE SENA, *La libertà di espressione e le norme internazionali, ed europee, prese sul serio: sempre su CasaPound c. Facebook*, apparso su SidiBlog.it, 20 gennaio 2020. Disponibile online: http://www.sidiblog.org/2020/01/20/la-liberta-di-espressione-e-le-norme-internazionali-ed-europee-prese-sul-serio-sempre-su-casapound-c-facebook/.

C. CAUFFMAN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in European Journal of Risk Regulation, Vol. 12, n. 4, pp. 758-774, 2021.

P. CAVALERI, *The Truth in Fake News: How Disinformation Laws Are Reframing the Concepts*, University of Edinburgh School of Law Working Paper n. 12, 2022. Disponibile su SSRN: https://ssrn.com/abstract=4151908.

A. CHANDER, *Facebookistan*, in Southern California Law Review, Vol. 86, n. 1, pp. 1808-1842 – UC Davis Legal Studies Research Paper Series, Research Paper No. 295, 2012. Disponibile su SSRN: http://ssrn.com/abstract=2061300.

Z. CHEN, *Internet, Consumer Contracts and Private International Law: What Constitutes Targeting Activity Test?* in Information & Communications Technology Law, pubblicato il 21 dicembre 2021 e liberamente accessibile al seguente link doi: https://doi.org/10.1080/13600834.2021.2018760

M.A. CHERRY, *Regulatory Options for Conflicts of Law and Jurisdictional Issues in the On-Demand Economy*, Organizzazione Internazionale del lavoro, Condizioni di lavoro e occupazione, n. 106, 2019.

M.A. CHERRY, V. DE STEFANO, *Reflecting on the Roundtable: Online Worker's Rights and Conflicts of Law*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 213-224, Schulthess, 2018.

T. CHRISTAKIS, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)* in AA.VV, *The White Book: Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection,* pp. 16-44, *CEIS & The Chertoff Group White Paper*, 2017. Disponibile su SSRN: https://ssrn.com/abstract=3086820.

T. CHRISTAKIS, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, in R. MILCH, S. BEN-

THALL (a cura di), *Cybersecurity and Privacy in a Globalized World – Building Common Approaches*, New York University School of Law, e-book, 2019. Disponibile su SSRN: https://ssrn.com/abstract=3397047.

T. CHRISTAKIS, *National Security, Surveillance and Human Rights*, in R. GEISS, N. MELZER (a cura di), *Oxford Handbook on the International Law of Global Security*, Oxford University Press, 2020, disponibile su SSRN: https://ssrn.com/abstract=3599994.

T. CHRISTAKIS, *"European Digital Sovereignty" Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, 2020. Disponibile su SSRN: https://ssrn.com/abstract=3748098.

T. CHRISTAKIS, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in International Data Privacy Law, Vol. 11, n. 2, pp. 81-106, 2021.

G.L. CONTI, *La lex informatica*, in Osservatorio sulle fonti, fasc. 1, pp. 317-347, 2021. Disponibile online su: www.osservatoriosullefonti.it.

J. CONTRERAS, *Private Law, Conflict of Laws, and a Lex Mercatoria of Standards-Development Organizations*, in European Review of Private Law, Vol. 27, n. 2, pp. 245-268, 2019.

N.E. CURTO, *EU Directive on Copyright in the Digital Single Market and ISP Liability: What's Next at International Level?*, in Case Western Reserve Journal of Law, Technology and the Internet, Vol. 11, n. 3, pp.84-110, 2020.

G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell'hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive*

de jure condendo, in federalismi.it, n. 2, pp. 108-147, 2020. Accessibile online: https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=40904.

J. DASKAL, *Google Inc. v. Equustek Solutions Inc.*, in American Journal of International Law, Vol. 112, n. 4, pp. 727-733, 2018.

J. DASKAL, *Borders and Bits*, in Vanderbilt Law Review, Vol. 71, n. 1, pp. 179-240, 2018.

M. DE BELLIS, *Public Law and Private Regulators in the Global Legal Space*, in International Journal of Constitutional Law, Vol. 9, n. 2, pp. 425-448, 2011.

A. DE FRANCESCHI, *Uber Spain and the "Identity Crisis" of Online Platforms*, in Journal of European Consumer and Markets Law, Vol. 7, n. 1, pp. 1-4, 2018.

G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani*, Editoriale Scientifica, 2018.

G. DELLA MORTE, *Limiti e prospettive del diritto internazionale del cyberspazio*, in Rivista di diritto internazionale, fasc. 1, pp. 5-42, 2022.

F. DE LONGIS, *L'agenda digitale europea. Mercato, tecnologia e regolamentazione*, Guerini Next, 2016.

P. A. DE MIGUEL ASENSIO, *Recognition and Enforcement of Judgments in Intellectual Property Litigation: The CLIP Principles*, in J. BASEDOW, T. KONO, A. METZGER (a cura di), *Intellectual Property in the Global Arena*, Mohr Siebeck, pp. 239-292, 2010.

P.A. DE MIGUEL ASENSIO, *Intellectual Property in European Private Law*, in E. PILLOT (a cura di), *Les frontiers du droit privé européen / The Boundaries of European Private Law*, Larcier, pp. 189-213, 2012.

V. DE STEFANO, *The Rise of the "Just-in-time Workforce": On-Demand Work, Crowdwork and Labour Protection in the "Gig-Economy"*, Organizzazione Internazionale del lavoro, Condizioni di lavoro e occupazione, n. 71, 2016.

M. DOUGLAS, *A Global Injunction Against Google,* in The Law Quarterly Review, Vol. 134, n. 2, pp. 181-187, 2018.
Disponibile su SSRN: https://ssrn.com/abstract=3137526

C. ETTELDORF, *Canadian Supreme Court on Google: Effective Legal Protection Tops Jurisdictional Boundaries,* in European Data Protection Law Review (EDPL), Vol. 3, n. 3, pp. 384-386, 2017.

V. FALCE (a cura di), *Competition Law Enforcement in Digital Markets*, Giappichelli, 2021.

P. FALLETTA, *Controlli e responsabilità dei social network sui discorsi d'odio online*, in Media Laws, n. 1, pp. 146-158, 2020. Disponibile online: https://www.medialaws.eu/rivista/controlli-e-responsabilita-dei-social-network-sui-discorsi-dodio-online/.

P. FAVROD-COUNE, *The Legal Position of the Weaker Party in B2B Relationships with Online Platforms in the European Union, an Analysis of Dispute Resolution Mechanisms in Regulation (EU) 2019/1150*, in Yearbook of Private International Law, Vol. XXI, pp. 523- 548, 2021.

O. FERACI, *La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria*, in Rivista di diritto internazionale, Vol. 92, n. 4, pp. 1020-1085, 2009.

O. FERACI, *Digital Rights and Jurisdiction: The European Approach to Online Defamation and IPRs Infringements*, in E. CARPANELLI, N. LAZZERINI (a cura di), *Use and Misuse of New Technologies*, pp. 277-304, Springer, 2019.

G.C. FERONI, *L'Oversight Board di Facebook: il controllo dei contenuti tra procedure private e norme pubbliche*, Key4Biz, 16 febbraio 2021. Disponibile sul sito del Garante per la protezione dei dati personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9542545..

N. FILATOVA-BILOUS, *Once again platform liability: on the edge of the 'Uber' and 'Airbnb' cases*, in Internet Policy Review – Journal of Internet Regulation, Vol. 10, n. 2, pp. 2-27, 2020.

M. FINCK, *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy*, LSE Law, Society and Economy Working Papers, n. 15, 2017.

A. FISCHER-LESCANO, G. TEUBNER, *Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law*, in Michigan Journal of International Law, Vol. 25, n. 4, pp. 999-1046.

S. FRANCQ, *Chapter U.4: Unilateralism*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (a cura di), *Encyclopedia of Private International Law*, pp. 1780–179, Edward Elgar, 2017.

P. FRANZINA, *Norme di conflitto comunitarie in materia di contratti con consumatori e corretto funzionamento del mercato interno*, in Rivista di diritto internazionale, Vol. 92, fasc. 1, pp. 122-129, 2009.

P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. DE FRANCESCHI (a cura di),

European Contract Law and the Digital Single Market, pp. 81-108, Intersentia, 2016.

P. FRANZINA, *Promoting Fairness and Transparency for Business Users of Online Platforms: The Role of Private International Law* in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit comparé*, pp. 147-152, Schulthess, 2018.

P. FRANZINA, *Introduzione al diritto internazionale privato*, Giappichelli, 2021.

F. FRIGERIO, *Responsabilità dell'hosting provider: la Cassazione conferma la distinzione tra attivo e passivo*, in filodiritto.it, 18 aprile 2019, accessibile online: https://www.filodiritto.com/responsabilita-dellhosting-provider-la-cassazione-conferma-la-distinzione-tra-attivo-e-passivo.

E. GABRIELLI, *Il consumatore e il professionista*, in E. GABRIELLI, E. MINERVINI (a cura di), *I contratti del consumatore*, UTET, 2005.

A. GEROSA, *La tutela della libertà di manifestazione del pensiero nella rete tra Independent Oversight Board e ruolo dei pubblici poteri. Commenti a margine della decisione n. 2021-001-FB-FBR*, in Forum di Quaderni Costituzionali, fasc. 2, pp. 427-440, 2021. Disponibile online: https://www.forumcostituzionale.it/wordpress/?p=16395.

C. GOANTA, P. ORTOLANI, *Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts*, 2021. Disponibile su SSRN: https://ssrn.com/abstract=3969360.

J.L. GOLDSMITH, *The Internet and the Abiding Significance of Territorial Sovereignty*, in Indiana Journal of Global Legal Studies, Vol. 5, n. 2, pp. 475-491, 1998.

J.L. GOLDSMITH, *Against Cyberanarchy*, University of Chicago Law Occasional Paper, n. 40, 1999.

L. GOLDSMITH, *The Internet, Conflicts of Regulation, and International Harmonization*, in C. ENGEL, K.H. KELLER (a cura di), *Governance of Global Networks in the Light of Differing Local Values*, pp. 197-207, Nomos Verlagsges, 2000.

J.L. GOLDSMITH-T. WU, *Who Controls the Internet? Illusion of a Borderless World*, Oxford University Press, 2006.

O. GRANDINETTI, *Facebook vs. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali*, in MediaLaws, n. 1, pp. 173-203, 2021.

C.G. GRANMAR, *Global Applicability of the GDPR in Context*, in International Data Privacy Law, Vol. 11, n. 3, pp. 225-244, 2021.

F. HEINDLER, *Streaming Platforms and Copyright in Conflict of Laws*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 193-202, Schulthess, 2018.

D. HOLZNAGEL, *The Digital Services Act wants you to "sue" Facebook over content decisions in private de facto courts*, apparso su Verfassungsblog.de, 24 giugno 2021. Disponibile online: https://verfassungsblog.de/dsa-art-18/.

C. HONORATI, *Regolamento n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali*, in F. PREITE (a cura di), *Atti notarili - Diritto dell'Unione e internazionale,* Vol. IV, t. 1, pp. 483-558, Utet Giuridica, 2011.

M. ILLMER, Article 6 – *Unfair Competition and Acts Restricting Free Competition*, in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome II Regulation: Commentary*, pp. 230-286, Verlag Dr. Otto Schmidt, 2019.

M. INGLESE, *Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland*, in Eurojus, fasc. 1, pp. 37-52, 2020.

P.C. JESSUP, *Transnational Law*, Yale University Press, 1956.

C. JOERGES, *Constitutionalism in Postnational Constellations: Contrasting Social Regulation in the EU and in the WTO* in C. JOERGES, E.U. PETERSMANN (a cura di), *Constitutionalism, Multilevel Trade Governance and Social Regulation*, pp. 491-507, Hart Publishing, 2006.

D.R. JOHNSON, D. POST, *Law and Borders-The Rise of Law in Cyberspace,* Vol. 48, n. 5, Stanford Law Review, pp. 1378-1389, 1996.

O. KAHN-FREUND, *General Problems of Private International Law,* Sijthoff, 1976, p. 272.

C. KLONICK, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, in Yale Law Journal, Vol. 129, n. 8, pp. 2418-2499, 2020.

C. KOHLER, *Conflict of Law Issues in the Data Protection Regulation of the European Union*, in Rivista di Diritto Internazionale Privato e Processuale, Vol. 52, n. 3, pp. 653-675, 2016.

T. KONO, *Intellectual Property Rights, Conflict of Laws and International Jurisdiction: Applicability of the ALI Principles in Japan?*, in Brooklyn Journal of International Law, Vol. 30, n. 3, pp. 865-883, 2005.

C. KUNER, *The 'Internal Morality' of European Data Protection Law*, 2008, disponibile su SSRN: https://ssrn.com/abstract=1443797.

C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, in International Journal of Law and Information Technology, Vol. 18, n. 3, pp. 227-247, 2010.

C. KUNER, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, in International Data Privacy Law, Vol. 5, n. 4, pp. 235-245, 2015.

C. KUNER, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, in B. HESS, C.M. MARIOTTINI (a cura di), *Protecting Privacy in Private International and Procedural Law and by Data Protection*, pp. 19-55, Nomos Verlagsgesllschaft, 2015.

C. KUNER, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, in International Data Privacy Law, Vol. 5, n. 4, pp. 235-245, 2015.

C. KUNER, *The Internet and the Global Reach of EU Law*, in M. CREMONA, J. SCOTT (a cura di), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, pp. 112-145, Oxford University Press, 2019. Disponibile su SSRN: https://ssrn.com/abstract=2890930.

C. KUNER, *Article 47 Binding Corporate Rules*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 813-824, Oxford University Press, 2020.

C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020.

C. KUNER, L.A. BYGRAVE, C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary – Update of Selected Articles*, Oxford University Press, 2021. Disponibile su SSRN: https://ssrn.com/abstract=3839645.

C. KUNER, *European Data Protection Law: Corporate Compliance and Regulation*, 2a edizione, Oxford University Press, 2007 (in particolare v. p. 217).

M. LEHMANN, *Who Owns Bitcoin? Private Law Facing the Blockchain*, EBI Working Paper Series, n. 42, 2019.

E. LACHAUD, *What GDPR Tells about Certification*, 2020, disponibile su SSRN: https://ssrn.com/abstract=3557167

L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, 1999.

L. LESSIG, *Code and Other Laws of Cyberspace, Version 2.0*, Basic Books, 2006.

I.M. LO PRESTI, *CasaPound, Forza Nuova e Facebook. Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e social network*, in Forum di Quaderni Costituzionali, fasc. 2, pp. 924-946, 2020, disponibile online: https://www.forumcostituzionale.it/wordpress/?p=14887.

A.R. LODDER, J. MORAIS CARVALHO, *Online Platforms: Towards an Information Tsunami with New Requirements on Moderation, Ranking, and Traceability*, in European Business Law, Vol. 33, n. 4, pp. 537-556, 2022.

A.M. LUCIANI, *La nuova lex mercatoria*, in Osservatorio sulle fonti, fasc. 1, pp. 241-254, 2021. Disponibile online su: www.osservatoriosullefonti.it.

L. LUNDSTEDT, *International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR*, Faculty of Law, Stockholm University Research Paper, n. 57, 2018. Disponibile su SSRN: https://ssrn.com/abstract=3159854.

T. LUTZI, *Private Ordering, the Platform Economy, and the Regulatory Potential of Private International Law*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 129-146, Schulthess, 2018.

T. MADIEGA, *Digital Sovereignty for Europe*, EPRS Ideas Paper, PE 651.992, 2020, disponibile online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992.

T.A. MADIEGA, *Digital Services Act*, EPRS – European Parliamentary Research Service, PE 689.357, 2022. Disponibile online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689357.

U. MAGNUS, *Article 4*, in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome I Regulation: Commentary*, Verlag Dr. Otto Schmidt, 2016.

B. MAIER, *How Has the Law Attempted to Tackle the Borderless Nature of the Internet?* in International Journal of Law and Information Technology, Vol. 18, n. 2, pp. 145-172, 2010.

P. MANKOWSKI, *Article 3: Freedom of Choice* in U. MAGNUS, P. MANKOWSKI (a cura di) *Rome I Regulation: Commentary*, pp. 87-263, Verlag Dr. Otto Schmidt, 2016.

M. MANTOVANI, *Contractual Obligations as a Tool for International Transfers of Personal Data under the GDPR*, apparso su Eapil.blog, 24 gennaio 2020. Disponibile online: https://eapil.org/2020/01/20/contractual-obligations-as-a-tool-for-international-transfers-of-personal-data/.

C.M. MARIOTTINI, *Freedom of Speech and Foreign Defamation Judgments:From New York Times v. Sullivan via Ehrenfeld to the 2010 SPEECH Act*, in B. HESS, C.M. MARIOTTINI (a cura di), *Protecting Privacy in Private International and Procedural Law and by Data Protection,* pp. 115-168, Nomos Verlagsgesllschaft, 2015.

F. MARONGIU BONAIUTI, *Le obbligazioni non contrattuali nel diritto internazionale privato,* Giuffré, 2013.

F. MARONGIU BONAIUTI, *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 Ibis"*, in Cuadernos de Derecho Transnacional, Vol. 9, n. 2, pp. 448-464, 2017.

A. MEIER, *Le futur dialogue social et du tripartisme dans le contexte de la digitalisation de l'économie*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 305-324, Schulthess, 2018.

R. MICHAELS, *The Re-State-ment of Non-State Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism*, in Wayne Law Review, Vol. 51, n. 3, p. 1209-1260, 2005.

R. MICHAELS, *True Lex Mercatoria: Law Beyond the State*, in Indiana Journal of Global Legal Studies, Vol. 14, n. 2, 2007.

R. MICHAELS, *Non-State Law in the Hague Principles on Choice of Law in International Commercial Contracts*, in K. PURNHAGEN, P. ROTT (a cura di), *Varieties of European Economic Law and Regulation: Liber Amicorum for Hans Micklitz*, pp. 43-69, Springer, 2014.

A. MILLS, *The Law Applicable to Cross-Border Defamation on Social Media: Whose law governs free speech in 'Facebookistan'?*, in Journal of Media Law, Vol. 7, n. 1, pp. 1-35, 2015.

L. MOEREL, *Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection*, 2011. Disponibile online: https://research.tilburguniversity.edu/en/publications/binding-corporate-rules-fixing-the-regulatory-patchwork-of-data-p

L. MOEREL, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, in International Data Privacy Law, Vol. 1, n. 1, pp.28-46, 2011.

G. MONGA, *Italian Supreme Court Rules on Jurisdiction under the Montreal Convention*, apparso su Eapil.blog, 9 aprile 2020, disponibile online: https://eapil.org/2020/04/09/italian-supreme-court-rules-on-jurisdiction-over-passengers-claims-to-damages-under-the-montreal-convention/

E. MOSTACCI, *Faut-il prévoir des règles impératives pour la protection des parties faibles dans les relations de travail? Quelques suggestions méthodologiques pour une réponse éclairée*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 243-254, Schulthess, 2018.

A. NICITA, A. MANGANELLI, *Regulating Digital Markets – The European Approach*, 2022.

R. NIRO, *Piattaforme digitali e libertà di espressione fra autoregolamentazione e coregolazione: note ricostruttive,* in Osservatorio sulle fonti, fasc. 3, pp. 1369-1391, 2021. Disponibile online su: www.osservatoriosullefonti.it.

A. PALMIERI, *Profili giuridici delle piattaforme digitali – La tutela degli utenti commerciali e dei titolari di siti web aziendali*, Giappichelli, 2019.

F. PAOLUCCI, *L'Oversight Board di Facebook conferma la sospensione degli account di Trump*, apparso su Iusinitinere.it, 5 maggio 2021. Disponibile online: https://www.iusinitinere.it/loversight-board-di-facebook-conferma-la-sospensione-degli-account-di-trump-38521.

J.R. PAUL, *Comity in International Law*, in Harvard International Law Journal, Vol. 32, n. 1, pp. 2-44, 1991.

S. PELLERITI, *La governance privata di Facebook e la presa di coscienza del regolatore europeo: qualcosa sta cambiando?*, in Rivista della Regolazione dei mercati, fasc. 2, pp. 429-444, 2021.

J. PERRY BARLOW, *Cyberspace Independence Declaration*, 8 febbraio 1996. Reperibile online: https://www.eff.org/it/cyberspace-independence.

M. PERTEGAS SENDER, *Cross-Border Enforcemenr of Patent Rights – An Analysis of the Interface Between Intellectual Property and Private International Law*, Oxford University Press, 2002.

F. PEZZA, *Art. 42 Certificazione*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione, pp. 380-386, Ipsoa, 2022.

F. PEZZA, *Art. 43 Organismi di certificazione*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione pp. 387-393, Ipsoa, 2022.

P. PIRODDI, *Profili internazionalprivatistici della responsabilità del gestore di un motore di ricerca per il trattamento dei dati personali*, in G. RESTA, V. ZENO-ZENCOVICH

(a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, pp. 63-98, Roma TrE-Press, 2015.

A. PIZZORUSSO, *Corso di diritto comparato*, Giuffré, 1983.

O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in Percorsi Costituzionali, fasc. 1, pp. 45-74, 2014.

O. POLLICINO, *The Road Towards a Strengthened Code Against Disinformation: About Metaphors in Free Speech and the Need to Handle Them Carefully*, in European Law Institute Newsletter, n. 3, pp. 2-3, 2022.

O. POLLICINO, M. BASSINI, G.M. RICCIO (a cura di), *Copyright versus (other) Fundamental Rights in the Digital Age. A Comparative Analysis in Search of a Common Constitutional Ground*, Edward Elgar, 2020.

O. POLLICINO, M. BASSINI, G. DE GREGORIO, *Trump's Indefinite Ban – Shifting the Facebook Oversight Board away from the First Amendment Doctrine*, apparso su Verfassungsblog.de, 11 maggio 2021. Disponibile online: https://verfassungsblog.de/fob-trump-2/.

O. POLLICINO, R. FRANZOSI, G. CAMPUS (a cura di), *Internet and Copyright protection in the European perspective, The Digital Single Market Copyrig*ht, Aracne, 2016.

O. POLLICINO, G. PITRUZZELLA, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, 2017.

O. POLLICINO, G. PITRUZZELLA, *Disinformation and Hate Speech: A European Constitutional Perspective,* Egea, 2021.

G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service providers*, in S. SICA, P. STANZIONE (a cura di), *Commercio elettronico e categorie civilistiche*, Giuffrè, 2002.

T. PRASTITOU-MERDI, *The Notion of "Online Intermediation Services" Found in the New EU Platform Regulation: Who Is Caught After All?*, in T. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU-MERDI (a cura di), *EU Internet Law in the Digital Single Market*, pp. 543-560, Springer, 2021.

I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 55-80, Schulthess, 2018.

I. PRETELLI, *The Economic Rise of Digital Platforms' Business Models and its Impact in the Conflict of Laws*, in in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 17-53, Schulthess, 2018.

I. PRETELLI, *Protecting Digital Platform Users by Means of Private International Law*, in *Cuadernos de Derecho Transnacional*, Vol. 13, n. 1, pp. 574-585, 2021, disponibile su SSRN: https://ssrn.com/abstract=3784912.

K. PURNHAGEN, *Mapping Private Regulation – Classification, Market Access and Market Closure Policy and Law's Response*, in Journal of World Trade, Vol. 49, n. 2, pp. 309–324, 2015.

F. RAGNO, *Article 2 Universal Application*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 55-57, Cambridge University Press, 2020.

F. RAGNO, *The Law Applicable to Consumer Contracts under the Rome I Regulation*, in F. FERRARI, S. LEIBLE (a cura di), *Rome I – The Law Applicable to Contractual Obligations in Europe,* pp.129-170, Sellier European Law Publishers, 2009.

F. RAGNO, *Article 3 Freedom of Choice*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 59-87, Cambridge University Press, 2020.

F. RAGNO, *Article 6 Consumer Contracts*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, pp. 161-162, Cambridge University Press, 2020.

J.R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in Texas. Law Review, Vol. 76, n. 3, 1998.

G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE,* in Diritto dell'informazione e dell'informatica, fasc. 4-5, p. 697-718, 2015.

G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in Rivista trimestrale di diritto e procedura civile, Vol. 72, n. 2, pp. 411-440, 2018.

G.M. RICCIO, *La responsabilità civile degli internet service providers*, Giappichelli, 2002.

G.M. RICCIO, *Art. 46 Trasferimento soggetto a garanzie adeguate*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione, pp. 404-408, Ipsoa, 2022.

G.M. RICCIO, *Art. 47 Norme vincolanti d'impresa*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione, pp. 408-413, Ipsoa, 2022.

G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy – Commentario*, seconda edizione, Ipsoa, 2022.

G.M. RICCIO, V. VITI, in MediaLaws.eu, 19 luglio 2017, disponibile al seguente link: https://www.medialaws.eu/le-certificazioni-privacy-ed-il-regolamento-ue/.

G.M. RICCIO, *Tre buoni motivi per salutare con favore il Code of Practice on Disinformation*, apparso su MediaLaws.eu, 17 novembre 2022. Disponibile online: https://www.medialaws.eu/tre-buoni-motivi-per-salutare-con-favore-il-code-of-practice-on-disinformation/.

H. RICHTER, M. STRAUB, E. TUCHTFELD (a cura di), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package*, Max Planck Institute for Innovation & Competition Research Paper No. 21-25, 2021. Disponibile su SSRN: https://ssrn.com/abstract=3932809.

T. RODRÍGUEZ DE LAS HERAS BALLELL, *Rules for a Platform Economy: A Case for Harmonisation to Counter "Platform Shopping" in the Digital Economy*, in I. PRETELLI (a cura di), *Conflict of Laws in the Maze of Digital Platforms - Le droit international privé dans le labyrinthe des plateformes digitales – Publications de l'Institut Suisse de droit compare*, pp. 55-80, Schulthess, 2018.

T. RODRÍGUEZ DE LAS HERAS BALLELL, *The background of the Digital Services Act: Looking Towards a Platform Economy*, in ERA Forum, Vol. 22, n. 1, pp. 75-86, 2021.

G. ROMANO, *L'unilateralismo nel diritto internazionale privato moderno*, Schulthess, 2014.

G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Collana di studi sull'integrazione europea, Cacucci, 2021.

S. RUSSO, R. SCAVIZZI, *Manuale di diritto dell'Unione dell'informatica*, Giuffrè, 2010.

G. SARTOR, M.V. DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/UE*, in *Diritto dell'informazione e dell'informatica,* fasc. 4-5, pp. 657-680, 2014.

H. SCHEPEL, *Private Regulators in Law*, in J. PAUWELYN, R. WESSEL, J. WOUTERS, (a cura di), *Informal International Lawmaking*, pp. 356-367, Oxford University Press, 2012.

C. SCHMON, *The Interconnection of the EU Regulations Brussels I Recast and Rome I*, Springer, 2020.

S.F. SCHWEMER, *Liability Exemptions of Non-hosting Intermediaries: Sideshow in the Digital Services Act?*, in Oslo Law Review, Vol. 8, n. 1, pp. 4-29, 2021.

L. SENDEN, E. KICA, M. HIEMSTRA, K. KLINGER, *Mapping Self- and Co-regulation Approaches in the EU Context. Explorative Study for the European Commission, DG Connect*, Commissione Europea, 2015.

K. SIEHR, *Violation of Privacy and Rights Relating to Personality*, in A. MALATESTA (a cura di), *The Unification of Choice of Law Rules on Torts and Other Non-Contractual Obligations in Europe*, pp. 159-172, Cedam, 2006.

C. SCOTT, F. CAFAGGI, L. SENDEN, *The Conceptual and Constitutional Challenge of Transnational Private Regulation*, in Journal of Law and Society, Vol. 38, n. 1, pp. 1-19, 2011.

S. SICA, *Giurisprudenza nazionale ed europea e frammentazione legislativa della responsabilità civile del provider*, in A.M. MANCALEONI, E. POILLOT (a cura di), *National Judges and the Case Law of the Court of Justice of the European Union*, pp. 205-222, Roma Tre-Press, 2021.

S.R. SWANSON, *Comity, International Dispute Resolution and the Supreme Court*, in Georgetown Journal of International Law, Vol. 21, pp. 333-365, 1990, disponibile su SSRN: https://ssrn.com/abstract=1955652.

R.C.R, SIEKMANN, J. SOEK, *Lex Sportiva. What is Sport Law?*, Springer, 2012.

M. SONNENTAG, *Chapter S.4: Savigny, Friedrich Carl von*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (a cura di), *Encyclopedia of Private International Law*, pp. 1610–1615, Edward Elgar, 2017.

N. SRNICEK, *Platform Capitalism*, Polity Press, 2016.

A. STEMLER, *Regulation 2.0: The Marriage of New Governance and Lex Informatica*, in Vanderbilt Journal of Entertainment & Technology Law, Vol. 19, n. 1, pp. 87-132, 2016.

D.J. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and its Practical Effect on U.S. Businesses*, in Stanford Journal of International Law, Vol. 50, n. 1, pp. 53-117, 2014.

D.J. SVANTESSON, *A "Layered Approach" to Extraterritoriality of Data Privacy Laws*, in International Data Privacy Law, Vol. 3, n. 4, pp. 278-286, 2013.

D.J. SVANTESSON, *Sovereignty in International Law – How the Internet Changed Everything, but not for Long*, in Masaryk University Journal of Law and Technology, Vol. 8, n. 1, pp. 137-155, 2014.

D.J. SVANTESSON, *A Jurisprudential Justification for Extraterritoriality in (Private) International Law*, in Santa Clara Journal of International Law, Vol. 13, n. 2, pp. 517-571, 2015.

D.J. SVANTESSON, *The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach*, EUI Working Papers, RCAS 2015/45, Robert Schuman Centre for Advanced Studies - Florence School of Regulation, 2015.

D.J. SVANTESSON, *Extraterritoriality and Targeting in the EU Data Privacy Law: the Weak Spot Undermining the Regulation*, in International Data Privacy Law, Vol. 5, n. 4, pp. 226-234, 2015.

D.J. SVANTESSON, *Private International Law and the Internet* (3rd edition), Kluwer Law International, 2016.

C. TAN, *Regulating Disinformation on Twitter and Facebook*, in Griffith Law Review, Vol. 31, n. 4, pp. 513-536, 2022. Liberamente accessibile online: https://doi.org/10.1080/10383441.2022.2138140.

Z.S. TANG, *Electronic Consumer Contracts in the Conflict of Laws*, Hart Publishing, 2018.

R. TARCHI, *Diritto transnazionale o diritti transnazionali? Il carattere enigmatico di una categoria giuridica debole ancora alla ricerca di un proprio statuto*, in Osservatorio sulle fonti, fasc. 1, pp. 1-16, 2021. Disponibile online: www.osservatoriosullefonti.it.

E. TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in Rivista di Diritto Industriale, fasc. 1, pp. 3-122, 2017.

E. TOSI, *Responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilità ex post*, in Il diritto degli affari, fasc. 1, pp. 1-24, 2020.

C. TWIGG-FLESNER, *The EU's Proposals for Regulating B2B Relationships on online platforms – Transparency, Fairness and Beyond*, in Journal of European Consumer and Markets Law, Vol. 7, n. 6, pp. 222-233, 2018. Disponibile su SSRN: https://ssrn.com/abstract=3253115.

B. UBERTAZZI, *Recognition and Enforcement of Foreign Judgments in Intellectual Property: a Comparison for the Intellectual Property Association*, in Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 3, n. 3, pp. 306-349, 2012.

B. VAN ALSENOY-M. KOEKKOEK, *Internet and Jurisdiction after Google Spain: the Extra-Territorial Reach of the EU's "Right to be Forgotten"*, KU Leuven Working Paper n. 153, 2015.

J. VAN HOBOKEN, I. BURI, J.P. QUINTAIS, R. FAHY, N. APPELMAN, *The DSA Has Been Published – Now the Difficult Bit Begins*, apparso su Verfassungsblog.de, 31 ottobre 2022. Disponibile online: https://verfassungsblog.de/dsa-published/.

R. VAN LOO, *Federal Rules of Platform Procedure*, in The University of Chicago Law Review, Vol. 88, n. 4, pp. 829-896, 2020.

P. VERBRUGGEN, *Regulating Private Regulators: Understanding the Role of Private Law*, in European Review of Private Law, Vol. 27, n. 2, pp. 175-186, 2019.

R. WAI, *Transnational Liftoff and Juridical Touchdown: Regulatory Function of Private International Law in an Era of Globalization*, in Columbia Journal of Transnational Law, Vol 40, n. 2, pp. 209-274, 2002.

W. WENGLER, *The General Principles of Private International Law* (Volume 104), in *Collected Courses of the Hague Academy of International Law*, Sijthoff, 1961.

B.J. WETZEL, *Theodore Roosevelt: Preaching from the Bully Pulpit*, Oxford University Press, 2021.

D. WIELSCH, *Private Law Regulation of Digital Intermediaries*, in European Review of Private Law, Vol. 27, n. 2, pp. 197-220, 2019.

K. YEUNG, *Algorithmic regulation and intelligent enforcement*, in M. LODGE (a cura di), *Regulation Scholarship in Crisis?*, Centre for Analysis of Risk and Regulation at the London School of Economics and Political Science – Discussion Paper n. 84, pp. 50-61, 2016.

H.E. YNTEMA, *The Comity Doctrine*, in Michigan Law Review, Vol 65, n. 1, pp. 9-32, 1966.

V. ZENO-ZENCOVICH, *Profili attivi e passivi della responsabilità dell'utente in Internet*, in A. PALAZZO, U. RUFFOLO (a cura di), *La tutela del navigatore in Internet*, pp. 137-144, Giuffrè, 2002.

V. ZENO-ZENCOVICH, *Intorno alla decisione del caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, in Diritto dell'informazione e dell'informatica, Vol. 31, fasc. 4-5, pp. 683-696, 2015.

G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina Editore, 2016.

Giurisprudenza citata

159 U.S. 113, *Henry Hilton* v. *Gustave Bertin Guyot, et al.*, 3 giugno 1895

Boschetto v. Hansing, 539 F.3d 1011 (9th Cir. 2008)

Cass. Sez. I Civ., sentenza 19 marzo 2019, n. 7708.

Cass. Sez. I Civ., sentenza 19 marzo 2019, n. 7709.

Cass., Sez. Un. Civ., ordinanza 8 luglio 2019, n. 18257.

Cass. Sez. Lav., sentenza 24 gennaio 2020, n. 1660.

CGUE, causa 10-56, *Meroni & Co., Industrie Metallurgiche, società in accomandita semplice* c. *Alta Autorità della Comunità europea del Carbone e dell'Acciaio*, 13 giugno 1958 – ECLI:EU:C:1958:8.

CGUE, causa C-21/76, *Handelskwekerij G.J. Bier B. V.* c. *Mines de potasse d'Alsace S.A.*, 20 novembre 1976 – ECLI:EU:C:1976:166.

CGUE, causa C-150/77, *Bertrand* c. *Paul Ott KG.*, 21 giugno 1978 – ECLI:EU:C:1978:137.

CGUE, causa C-53/81, *D.M. Levin* c. *Segretario di Stato per la giustizia*, 23 marzo 1982 – ECLI:EU:C:1982:105.

CGUE, causa C-66/85, *Deborah Lawrie-Blum* c. *Land Baden-Württemberg*, 3 luglio 1986 – ECLI:EU:C:1986:284.

CGUE, causa C-266/85, *Hassan Shenavai* c. *Klaus Kreischer*, 15 gennaio 1987 – ECLI:EU:C:1987:11.

CGUE, causa C-32/88, *Six Constructions Ltd* c. *Paul Humbert*, 15 febbraio 1989 – ECLI:EU:C:1989:68.

CGUE, causa C-68/93, *Fiona Shevill e a.* c. *Presse Alliance SA*, 7 marzo 1995 – ECLI:EU:C:1995:61.

CGUE, causa C-269/95, *Francesco Benincasa* c. *Dentalkit Srl*, 3 luglio 1997 – ECLI:EU:C:1997:337.

CGUE, causa C-85/96, *María Martínez Sala* c. *Freistaat Bayern*, 12 maggio 1998 – ECLI:EU:C:1998:217.

CGUE, causa C-337/97, *C.P.M. Meeusen* c. *Hoofddirectie van de Informatie Beheer Groep*, 8 giugno 1999 – ECLI:EU:C:1999:284.

CGUE, causa C-138/02, *Brian Francis Collins* c. *Secretary of State for Work and Pensions*, 23 marzo 2004 – ECLI:EU:C:2004:172.

CGUE, causa C-464/01, *Johann Gruber* c. *Bay Wa AG*, 20 gennaio 2005 – ECLI:EU:C:2005:32.

CGUE, cause riunite da C-236/08 a C-238/08, *Google France SARL e Google Inc.* c. *Louis Vouitton Malletier SA*, *Google France SARL* c. *Viaticum SA e Luteciel SARL*, *Google France SARL* c. *Centre National de recherche en relations humaine*s *(CNRRH) SAR, Pierre Alexis Thonet, Bruno Raboin e Tiger SARL*, 23 marzo 2010 – ECLI:EU:C:2010:159.

CGUE, cause riunite C-585/08 e C-144/09, *Peter Pammer* c. *Reederei Karl Schlüter GmbH & Co. KG* e *Hotel Alpenhof GesmbH* c. *Oliver Heller*, 7 dicembre 2010 – ECLI:EU:C:2010:740.

CGUE, causa C- 324/09, *L'Oréal SA e altri* c. *eBay International AG e altri*, 12 luglio 2011 – ECLI:EU:C:2011:474.

CGUE, cause riunite C-509/09 e C-161/10, *eDate Advertising GmbH e a.* c. *X e Société MGN LIMITED*, 25 ottobre 2011 – ECLI:EU:C:2011:685.

CGUE, causa C-523/10, *Wintersteiger AG* c. *Products 4U Sondermaschinenbau GmbH*, 19 aprile 2012 – ECLI:EU:C:2012:220.

CGUE, causa C-133/11, *Folien Fischer AG e Fofitec AG* c. *Ritrama SpA*, 25 ottobre 2012 – ECLI:EU:C:2012:664.

CGUE, causa C-548/12, *Marc Brogsitter* c. *Fabrication de Montres Normandes EURL e Karsten Fräßdorf*, 13 marzo 2014 - ECLI:EU:C:2014:148.

CGUE, causa C-131/2012, *Google Spain SL e Google Inc*. c. *Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, 13 maggio 2014 – ECLI:EU:C:2014:317.

CGUE, C-291/13 *Sotiris Papasavvas* c. *O Fileleftheros Dimosia Etaireia Ltd, Takis Kounnafi, Giorgos Sertis*, 11 settembre 2014 – ECLI:EU:C:2014:2209.

CGUE, causa C-352/13, *Cartel Damage Claims (CDC) Hydrogen Peroxide SA* c. *Akzo Nobel NV e a.*, 21 maggio 2015 – ECLI:EU:C:2015:335.

CGUE, causa C-230/14, *Weltimmo s.r.o.* c. *Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 ottobre 2015 – ECLI:EU:C:2015:639.

CGUE, causa C-362/2014, *Maximillian Schrems* c. *Data Protection Commissioner*, 6 ottobre 2015 –ECLI:EU:C:2015:650.

CGUE, causa C-191/15, *Verein für Konsumenteninformation* c. *Amazon EU Sàrl*, 28 luglio 2016 – ECLI:EU:C:2016:612.

CGUE, causa C-613/14, *James Elliott Construction Limited* c. *Irish Asphalt Limited*, 27 ottobre 2016 – ECLI:EU:C:2016:821.

CGUE, causa C-106/16, *Polbud* c. *Wykonawstwo*, 25 ottobre 2017 – ECLI:EU:C:2017:804.

CGUE, causa C-434/15, *Asociación Profesional Élite Taxi* c. *Uber Systems Spain SL*, 20 dicembre 2017 – ECLI:EU:C:2017:981.

CGUE, causa C-498/2016, *Maximilian Schrems* c. *Facebook Ireland Limited*, 25 gennaio 2018.

CGUE, causa C-320/16, procedimento penale a carico di *Uber France SAS* con l'intervento di: *Nabil Bensalem*, 10 aprile 2018 – ECLI:EU:C:2018:22.

CGUE, causa C-610/15, *Stichting Brein* c. *Ziggo BV*, *XS4ALL Internet BV*, 14 giugno 2018 – ECLI:EU:C:2017:456.

CGUE, causa C-521/17, *Coöperatieve Vereniging SNB-React U.A.* c. *D.M.*, 7 agosto 2018 – ECLI:EU:C:2018:639.

CGUE, causa C-451/18, *Tibor-Trans Fuvarozó és Kereskedelmi Kft.* c. *DAF Trucks NV*, 29 luglio 2019 – ECLI:EU:C:2019:635.

CGUE, causa C-507/17, *Google LLC* c. *Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019 – ECLI:EU:C:2019:772.

CGUE, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook Ireland Limited*, 3 ottobre 2019 – ECLI:EU:C:2019:821.

CGUE, causa C-390/18, procedimento penale a carico di *X*, con l'intervento di: *YA*, *Airbnb Ireland UC*, *Hôtelière Turenne SAS*, *Association pour un hébergement et un tourisme professionnels (AHTOP)*, *Valhotel*, 19 dicembre 2019 – ECLI:EU:C:2019:1112.

CGUE, causa C-343/19, *Verein für Konsumenteninformation* c. *Volkswagen AG*, 9 luglio 2020 – ECLI:EU:C:2020:534.

CGUE, causa C-311/18, *Data Protection Commissioner* c. *Facebook Ireland Limited e Maximillian Schrems*, 16 luglio 2020 – ECLI:EU:C:2020:559.

CGUE, causa C-59/19, *Wikingerhof GmbH & Co. KG* c. *Booking.com BV*, 24 novembre 2020 – ECLI:EU:C:2020:950.

CGUE, causa C-774/19, *A. B. e B. B.* c. *Personal Exchange International Limited*, 20 dicembre 2020 – ECLI:EU:C:2020:1015.

CGUE, causa C-30/20, *RH* c. *AB Volvo, Volvo Group Trucks Central Europe GmbH, Volvo Lastvagnar AB, Volvo Group España SA*, 15 luglio 2021 – ECLI:EU:C:2021:604.

Commission Administrative de règlement de la relation de travail (CRT), n. 116-FR- 20180209, 23 febbraio 2018.

Cour d'appel de Paris, Pôle 6, Chambre 2, n. 16/12875, 9 novembre 2017.

Cour d'appel de Paris, Pôle 6, Chambre 4, n. 18/028467, aprile 2021.

FOB, Decisione 2021-001-FB-FBR, *Sospensione dell'ex Presidente degli Stati Uniti Trump*. Disponibile online: https://www.oversightboard.com/decision/FB-691QAMHJ.

Supreme Court of Canada, *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34, [2017] 1 S.C.R. 824, 28 giugno 2017.

Tribunale di Chieti, R.G. 1489/2019, ordinanza del 29 gennaio 2020

Tribunale di Milano, Sez. spec. prop. Industriale, R.G. 79619/2009, e intellettuale, sentenza del 9 settembre 2011, n. 10893.

Tribunale di Roma, Sez. Impresa, R.G. 59264/2019, ordinanza del 12 dicembre 2019.

Tribunale di Roma, Sez. Diritti della persona e immigrazione civile, R.G. 64894/2019, ordinanza del 23 febbraio 2020.

Tribunale di Roma, Sez. XVII Civile, R.G. 80961/19, ordinanza del 29 aprile 2020.

Tribunale di Siena, R.G. 2968/2019, ordinanza del 19 gennaio 2020.

Report, articoli di stampa, documenti istituzionali citati

Ansa, *Amazon, prima causa penale contro le recensioni false*, apparso su www.ansa.it il 21 ottobre 2022. Consultabile online: https://www.ansa.it/sito/notizie/postit/Amazon/2022/10/20/amazon-prima-causa-penale-contro-le-recensioni-false_e7bbc95f-4663-4318-8b35-11ba6c7b4a58.html

Censis, *Sedicesimo Rapporto sulla comunciazione – I media e la costruzione dell'identità*, 20 febbraio 2020. Disponibile al seguente link: https://www.censis.it/comunicazione/16%C2%B0-rapporto-censis-sulla-comunicazione-0

Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio sulla legge applicabile alle obbligazioni contrattuali (Roma I*), COM(2005) 650 def. –2005/0261 (COD), 15 dicembre 2005.

Commissione europea, *Libro verde – Revisione dell'acquis relativo ai consumatori*, COM (2006) 744 definitivo, 8 febbraio 2007.

Commissione europea, *Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations*

of privacy and rights relating to personality, JLS/2007/C4/028, Final Report, 1 febbraio 2009.

Commissione europea, *Codice di condotta per lottare contro le forme illegali di incitamento all'odio online*, maggio 2016. Disponibile online: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_it

Commissione europea, *Codice di buone pratiche dell'UE sulla disinformazione*, 16 ottobre 2018. Disponibile online al seguente link: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online*, COM(2018) 238 final, 26 aprile 2018.

Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali*, COM(2021) 762 final, 9 dicembre 2021.

Commissione europea, *Codice di buone pratiche sulla disinformazione rafforzato*, 16 giugno 2022. Disponibile online al seguente link: https://digital-strategy.ec.europa.eu/it/library/2022-strengthened-code-practice-disinformation.

Commissione europea, *Programma di monitoraggio della disinformazione sulla Covid-19*. Dettagli e i report presentati dalle piattaforme aderenti accessibili online: https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Legiferare con intelligenza nell'Unione europea*, COM(2010) 543 definitivo, 8 ottobre 2010.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 6 maggio 2015.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Legiferare meglio per ottenere risultati migliori — Agenda dell'UE*, COM(2015) 215 final, 19 maggio 2015.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Le piattaforme online e il mercato unico digitale – Opportunità e sfide per l'Europa*, COM(2016) 288 final, 25 maggio 2016.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un'agenda europea per l'economia collaborativa*, COM(2016) 356 final, 2 giugno 2016.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Lotta ai contenuti illeciti online – Verso una maggiore responsabilizzazione delle piattaforme online*, COM(2017) 555 final, 28 settembre 2017.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni, *Contrastare la disinformazione online: un approccio europeo*, COM(2018) 236 final, 26 aprile 2018.

Comunicazione della Commissione 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, 19 febbraio 2020.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Orientamenti della Commissione europea sul rafforzamento del codice di buone pratiche sulla disinformazione*, COM(2021) 262 final, 26 maggio 2021.

EDPB, *Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3) – versione 2.0 adottata dopo la pubblica consultazione*, 12 novembre 2019.

EDPB, *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali*, 18 giugno 2021.

EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, 19 novembre 2021.

EU Commission Staff Working Document, *A Digital Single Market Strategy for Europe - Analysis and Evidence – Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe*, SWD(2015) 100 final, 6 maggio 2015.

EU Commission Staff Working Document, *Online Platforms – Accompanying the document Communication on Online Platforms and the Digital Single Market*, SWD(2016) 172 final, 25 maggio 2016.

EU Commission Staff Working Document, *Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*, SWD(2020) 180 final, 10 settembre 2020.

B. HARRIS, *Establishing Structure and Governance for an Independent Oversight Board*, apparso su Facebook newsroom, 17 settembre 2019. Disponibile online: https://about.fb.com/news/2019/09/oversight-board-structure/.

House of Lords, *Select Committee on European Union*, 10th Report of Session 2015–16, *Online Platforms and the Digital Single Market*, HL Paper 129, 20 aprile 2016.

Human Rights Watch, *Canada: Court Decision a Global Threat to Information Access*, 29 giugno 2017. Reperibile online: https://www.hrw.org/news/2017/06/29/canada-court-decision-global-threat-information-access

Il Post, *II social network, Trump e l'attacco al Congresso*, apparso su ilPost.it, 7 gennaio 2021. Reperibile online: https://www.ilpost.it/2021/01/07/attacco-congresso-trump-social-network/.

E. KLEIN, *Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next*, apparso su Vox.com, 2 aprile 2018. Disponibile online: https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge.

Monopolkommissione, *Written evidence from Monopolkommission*, (OPL0046). Reperibile online: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online-platforms-and-the-eu-digital-single-market/written/23265.html.

Raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. (97)/20, 30 ottobre 1997.

Risoluzione del Parlamento europeo del 10 maggio 2012 recante raccomandazioni alla Commissione concernenti la modifica del regolamento (CE) n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali (Roma II) (2009/2170(INI)).

The Santa Clara Principles – On Transparency and Accountability in Content Moderation. Disponibili online: https://santaclaraprinciples.org/.

We Are Social, Hootsuite Inc., *Digital 2021 Global Overview Report*, 27 gennaio 2021. Disponibile online: https://datareportal.com/reports/digital-2021-global-overview-report.

WP29, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites* – 5035/01/EN/Final WP 56, 30 maggio 2002.

WP29, *Opinion 8/2010 on applicable law* – 0836-02/10/EN WP179, 16 dicembre 2010.

WP29, *Orientamenti per l'esecuzione della sentenza della Corte di giustizia dell'Unione europea nella causa C-131/12 "Google Spain e Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González"* – 14/IT WP 225, 26 novembre 2014.

WP29, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* – 176/16/EN WP 179 update, 16 dicembre 2015.

M. ZUCKERBERG, *A Blueprint for Content Governance and Enforcement*, apparso su Facebook il 15 novembre 2018. Disponibile online: https://www.facebook.com/notes/751449002072082/ – ultima modifica del 5 maggio 2021.