Università degli Studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto
Dipartimento di Diritto Pubblico, Internazionale e Comunitario
Corso di Laurea Magistrale in Giurisprudenza

Digital Services Act e Regolamento generale sulla protezione dei dati: un'analisi dei meccanismi di *enforcement* e dei profili di intersezione di due regimi convergenti

Relatore:
Chiar.mo Prof. Bernardo Cortese

Correlatrice:
Prof.ssa Annalisa Volpato

Studente:
Francesco Bissacco
Matricola 1198284

Anno Accademico 2023–2024

INDICE

CAPITOLO INTRODUTTIVO

Presentazione generale

La regolazione dei servizi digitali è oggi data da un corpus normativo molto ampio, composto da molte fonti di diritto internazionale, comunitario e dei singoli Stati membri. Il presente elaborato si concentra sull'analisi di specifici aspetti di due atti legislativi dell'Unione – Digital Services Act[1] e Regolamento generale sulla protezione dei dati.[2] Anziché occuparsi della disciplina sostanziale, si è deciso di dedicare questo lavoro al tema dell'*enforcement* di tali regolamenti. Infatti, uno dei problemi principali del GDPR pare essere, proprio, il fatto che – pur fissando, astrattamente, uno standard elevato di protezione dei dati – quest'ultimo sia poi pregiudicato da un meccanismo di attuazione e vigilanza inidoneo concretamente a garantire i diritti previsti nel regolamento. È, dunque, evidente l'importanza del tema: concedere astrattamente dei diritti senza occuparsi di un adeguato sistema di *enforcement* significa che, nella realtà, tale diritto non sarà adeguatamente protetto. Tale attenzione deve essere riposta anche dall'interprete: in questo senso, si deve notare come i contributi dottrinali e giurisprudenziali sul tema siano minori rispetto a quelli relativi alla disciplina sostanziale del GDPR. Ecco, dunque, un'altra ragione per adottare questa peculiare prospettiva.

GDPR e DSA sembrano rientrare all'interno di due diversi ambiti del diritto dell'Unione: il primo volto a regolare i servizi digitali, inserendosi all'interno delle norme che mirano a tutelare il mercato interno, il secondo invece destinato a proteggere il diritto (fondamentale) alla protezione dei dati personali, sancito a livello primario dall'articolo 8 della Carta. Le ragioni che rendono opportuno un esame congiunto di questi due regolamenti sono tuttavia molteplici. Innanzitutto,

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, GU L 277, 27/10/2022, pp. 1-102.

2 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, GU L 119, 04/05/2016, pp. 1-88.

entrambi gli strumenti sono atti che regolano – direttamente e senza la necessità di ulteriori interventi, vista la natura regolamentare – l'operato dei fornitori di servizi digitali; e, dunque, norme che pongono diritti ed obblighi sia di questi ultimi, sia dei soggetti che di tali servizi si avvalgono.

Inoltre, bisogna rilevare come molto spesso la tutela delle «quattro libertà» (per quanto qui interessa, in particolare la libera prestazione dei servizi) finisca per promuovere indirettamente interessi ulteriori rispetto a quelli meramente "economici". In particolare, non sono rari i casi in cui il legislatore comunitario ha utilizzato la base giuridica di cui all'articolo 114 TFUE al fine di adottare determinati atti legislativi (quali ad esempio la direttiva 95/46/CE[3], il Digital Services Act, il Digital Market Act[4]) volti anche alla tutela dei diritti fondamentali, tra i quali si può annoverare non solo il diritto alla protezione dei dati personali, ma anche la libertà di manifestazione del pensiero e il principio di non discriminazione. Tale utilizzo viene generalmente accettato, sul presupposto che sia necessario assicurare un livello di tutela armonizzato di tali diritti, nonostante vi siano in dottrina delle voci critiche, o che quantomeno segnalano la necessità di rispettare i limiti di tale base giuridica.[5]

Più in generale, non è da trascurare una tendenza a collegare reciprocamente la tutela del mercato interno a quella dei diritti enucleati dalla Carta dei diritti

3 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, GU L 281, 23/11/1995, pp. 31-50.

4 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, GU L 265, 12/10/2022, pp. 1-66.

5 Ad es. v. M. Z. van Drunen et al., «The beginning of EU political advertising law: unifying democratic visions through the internal market», *International Journal of Law and Information Technology*, 30, 2 (2022), p. 193, dove si ricorda che l'art. 114 TFUE conferisce una «*important, albeit limited competence*» in dottrina v. inoltre M. Hiltunen, «Social Media Platforms within Internal Market Construction: Patterns of Reproduction in EU Platform Law», *German Law Journal*, 23, 9 (2022), p. 1229, 1230; L. Lionello, «La creazione del mercato europeo dei dati: sfide e prospettive», *Diritto del Commercio Internazionale*, 3 (2021), p. 678-679; M. Kellerbauer, «Article 114 TFEU», in *The EU Treaties and the Charter of Fundamental Rights*, a cura di M. Kellerbauer et al., Oxford University Press, New York 2019, p. 1236; G. Davies, «The European Union Legislature as an Agent of the European Court of Justice», *Journal of Common Market Studies*, 54, 4 (2016), p. 848. Vi è da segnalare anche la cautela della giurisprudenza, che – in *Tobacco Advertising I*, Corte giust., sentenza del 5 ottobre 2000, causa C-376/98, *Repubblica federale di Germania c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:2000:544, § 83 – ha ribadito che questa norma non può essere interpretata nel senso che attribuisca al «legislatore comunitario una competenza generale a disciplinare il mercato interno», in quanto ciò andrebbe a violare il principio, ora espresso dall'art. 5, par. 2, TUE, per cui le competenze dell'Unione sono competenze di attribuzione.

fondamentali dell'Unione europea.[6] Esempi ne sono proprio i considerando 1 e 9 del DSA, i quali recitano:

> […] Le condizioni per la prestazione dei servizi intermediari in tutto il mercato interno dovrebbero essere armonizzate *in modo da offrire alle imprese accesso a nuovi mercati e opportunità di sfruttare i vantaggi del mercato interno, consentendo nel contempo ai consumatori e agli altri destinatari dei servizi di disporre di una scelta più ampia*.
>
> Il presente regolamento armonizza pienamente le norme applicabili ai servizi intermediari nel mercato interno con l'obiettivo di garantire un ambiente online sicuro, prevedibile e affidabile, *in cui i diritti fondamentali sanciti dalla Carta siano efficacemente tutelati* e l'innovazione sia agevolata, contrastando la diffusione di contenuti illegali online e i rischi per la società che la diffusione della disinformazione o di altri contenuti può generare.[7]

D'altra parte, è altrettanto vero che le esigenze di garantire la libera prestazione dei servizi si traducono molto spesso nella tutela di chi presta tali servizi, ponendosi quindi in contrapposizione con le esigenze di tutela del c.d. "soggetto debole", cioè colui il quale è definito dal GDPR «interessato» e dal DSA «destinatario del servizio». Esempi di questa dinamica saranno analizzati successivamente, in particolare andando a verificare come il principio del paese d'origine (anche nella sua forma di «meccanismo di sportello unico» prevista dal GDPR) – che deriva dalla libertà di cui all'articolo 56 TFUE – possa causare una limitazione dei diritti conferiti all'individuo.

La regolazione dei servizi digitali nell'ambito del mercato interno

Il diritto dell'Unione europea non ha, sin dal suo inizio, contemplato la presenza di specifiche norme inerenti alla regolazione di Internet e dei servizi digitali, e questo per l'evidente fatto che tali fonti si sono sviluppate prima dell'avvento di tali tecnologie o, comunque, in un momento in cui la loro diffusione era talmente ridotta che un intervento regolatorio non appariva necessario.

Una volta che tali tecnologie si sono diffuse, si è invece assistito al proliferare di vari interventi delle istituzioni comunitarie, da una parte attraverso l'opera della Corte di giustizia, e dall'altra mediante l'introduzione di norme di diritto positivo, sia primario che derivato.

Con riferimento all'attività pretoria, inizialmente le sentenze della Corte di giustizia si sono principalmente concentrate sull'applicazione dei già consolidati principi del diritto dell'Unione in materia di mercato interno – che, ai sensi dell'articolo 26, paragrafo 2, TFUE «comporta uno spazio senza frontiere interne,

6 U. Neergaard e S. A. De Vries, «The Interaction between Free Movement Law and Fundamental Rights in the (Digital) Internal Market», *SSRN Electronic Journal* (2023), p. 2-3.

7 Corsivo aggiunto.

nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali» – a fattispecie che contemplavano in vari modi l'utilizzo di Internet. In particolare, l'opera della Corte si è concentrata in riferimento (*i*) alla libera circolazione delle merci e (*ii*) alla libera prestazione dei servizi.

Per quanto riguarda il primo aspetto, nella sentenza *Deutscher Apoterkerverband*[8] la Corte ha analizzato il caso di una legislazione nazionale che, stabilendo il divieto di vendita per farmaci ad uso umano al di fuori delle farmacie autorizzate, vietava di conseguenza anche l'importazione di medicinali spediti da altri Stati membri a seguito di un ordine online.[9] A questo riguardo, la Corte ha riconosciuto l'importanza di Internet quale mezzo che permette di ampliare la portata del mercato interno e aumentare il commercio tra gli Stati membri, affermando che esso «costituirebbe un mezzo più importante per le farmacie che non sono stabilite sul territorio tedesco per raggiungere direttamente tale mercato»[10] e osservando che «un divieto che colpisse in misura maggiore le farmacie stabilite al di fuori del territorio tedesco potrebbe essere *tale da ostacolare maggiormente l'accesso al mercato dei prodotti provenienti da altri Stati membri rispetto a quello dei prodotti nazionali*».[11] La Corte, dunque, riconosce tale divieto come una misura ad effetto equivalente ai sensi dell'articolo 28 CE (ora articolo 34 TFUE).[12]

Con riferimento alla libera prestazione di servizi, invece, l'attività della Corte si è concentrata, almeno in un primo periodo, sui servizi di scommesse online.[13] Nel primo caso degno di nota, *Gambelli*,[14] la Corte equipara i servizi prestati via Internet a quelli offerti da un prestatore che offre tali servizi «telefonicamente a potenziali destinatari stabiliti in altri Stati membri e che questi fornisce senza spostarsi dallo Stato membro nel quale è stabilito».[15] La Corte ha così confermato che qualunque legislazione nazionale[16] che restringa l'attività di un prestatore

8 Corte giust., sentenza del 11 dicembre 2003, causa C-322/01, *Deutscher Apothekerverband eV c. 0800 DocMorris NV e Jacques Waterval*, ECLI:EU:C:2003:664.

9 U. Neergaard, «The Approach of the CJEU in the Era of Digitalization: Free Movement in Relation to the Internet as Its 25th Anniversary», in *General principles of EU law and the EU digital order*, a cura di U. Bernitz et al., Kluwer Law International B.V., Alphen aan den Rijn 2020, p. 91.

10 Corte giust., causa C-322/01, *Deutscher Apothekerverband* cit., § 74

11 Ibidem, corsivo aggiunto.

12 Ivi, punto 76.

13 Neergaard, «The Approach of the CJEU in the Era of Digitalization» cit., p. 104.

14 Corte giust., sentenza del 6 novembre 2003, causa C-243/01, *Procedimento penale a carico di Piergiorgio Gambelli e a.*, ECLI:EU:C:2003:597, § 53.

15 Ed infatti, la Corte richiama il principio stabilito in Corte giust., sentenza del 10 maggio 1995, causa C-384/93, *Alpine Investments BV c. Minister van Financiën*, ECLI:EU:C:1995:126, § 20-22, ove si afferma che l'articolo 59 TCE (ora articolo 56 TFUE) è senz'altro applicabile anche a prestazioni di servizi che vengono offerti telefonicamente.

16 Nel caso di specie, la legislazione italiana che configurava come reato l'attività del privato che,

stabilito in uno Stato membro che, senza spostarsi da quest'ultimo e attraverso Internet, presti il servizio in altri Stati membri, costituisce in linea di principio una restrizione della libertà di cui all'articolo 56 TFUE.[17]

Rispetto alla possibilità che tali restrizioni siano tuttavia giustificate, la giurisprudenza della Corte assume nel corso del tempo un andamento altalenante, talora più a favore della libertà di movimento, talora più a protezione degli interessi regolatori nazionali.[18] Infatti, in *Gambelli*, la Corte, pur rispettando l'autonomia del giudice del rinvio, sembra suggerire che la previsione di una sanzione penale al fine di contrastare le frodi non sia proporzionata[19] e, quindi, favorire il mercato interno rispetto all'autonomia degli Stati membri;[20] d'altra parte, invece, in altri casi, come *Bwin*, la Corte ritiene gli interessi nazionali di lotta contro le frodi e le criminalità sufficienti a giustificare la restrizione alla libertà di prestazione dei servizi.[21]

La direttiva E-Commerce e il principio del paese d'origine

Dal punto di vista del diritto positivo, riveste un'importanza cardine la cd. «direttiva E-Commerce» o «direttiva sul commercio elettronico».[22]

Nell'economia del presente elaborato non è possibile procedere ad una disamina puntuale della direttiva; piuttosto, ci si concentrerà qui sull'esame di un particolare principio in essa contenuto, cioè il principio del paese d'origine. Questa analisi appare opportuna in quanto esso, pur essendo derivato dalle libertà connesse al mercato interno, ha successivamente imperniato – nella sua derivazione di «meccanismo di sportello unico» – anche il meccanismo di *enforcement* transfrontaliero del Regolamento generale sulla protezione dei dati (v. cap. 2). Più in generale, l'esame della direttiva 2000/31/CE risulta ancora più necessario se si considera che l'articolo 89 DSA non ha abrogato tale direttiva nella sua totalità, ma ha disposto la soppressione dei soli articoli da 12 a 15.

trovandosi in Italia, si connette via Internet con un prestatore di servizi di scommesse online di un altro Stato membro.

17 Corte giust., causa C-243/01, *Gambelli e a.* cit., § 54-57.

18 Neergaard, «The Approach of the CJEU in the Era of Digitalization» cit., p. 97.

19 Corte giust., causa C-243/01, *Gambelli e a.* cit., § 73.

20 Neergaard, «The Approach of the CJEU in the Era of Digitalization» cit., p. 91.

21 Corte giust., sentenza del 8 settembre 2009, causa C-42/07, *Liga Portuguesa de Futebol Profissional e Bwin International Ltd c. Departamento de Jogos da Santa Casa da Misericórdia de Lisboa*, ECLI:EU:C:2009:519, § 55-73.

22 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, GU L 178, 17/07/2000, pp. 1-16

L'origine di questo principio viene fatta risalire alla nota dottrina *Cassis de Dijon*[23] o, meglio, ad un'applicazione di tale dottrina (non alla libera circolazione delle merci, ma) alla libera prestazione dei servizi.[24] Si tratta di un principio molto importante nell'ambito del diritto dell'Unione: secondo parte della dottrina si tratterebbe di un «fondamento del diritto comunitario, di un pilastro dell'edificazione dell'Unione europea»[25] e «di un principio generale del diritto comunitario»;[26] altra parte della dottrina sottolinea, però, che tale principio non rientra nell'alveo del diritto *primario* dell'Unione,[27] con la conseguenza che il legislatore comunitario potrebbe comunque adottare delle norme che si discostano da esso,[28] senza che ciò costituisca una violazione dei Trattati.

Nella direttiva E-Commerce, il principio del paese d'origine, espresso dall'articolo 3, si presenta con una duplice formulazione:[29] il paragrafo 1 lo afferma dal punto di vista del paese d'origine, richiedendo che ogni Stato membro si assicuri che ogni servizio della società dell'informazione, fornito da un prestatore stabilito nel suo territorio, rispetti «le disposizioni nazionali vigenti in detto Stato membro nell'ambito regolamentato»; il paragrafo 2 assume il punto di vista degli altri Stati membri, ai quali è vietato «limitare la libera circolazione dei servizi della società dell'informazione provenienti da un altro Stato membro» *per motivi che rientrano nell'ambito regolamentato*.

Si nota, dunque, che tale principio viene applicato (*i*) con riferimento ai servizi della società dell'informazione, e (*ii*) nell'ambito regolamentato.

La definizione di servizio della società dell'informazione è data dall'articolo 2, paragrafo 1, lettera a), il quale rimanda all'articolo 1, paragrafo 2, della direttiva

23 Corte giust., sentenza del 20 febbraio 1979, causa 120/78, *Rewe-Zentral AG c. Bundesmonopolverwaltung für Branntwein*, ECLI:EU:C:1979:42; v. M.-D. Garabiol-Furet, «Plaidoyer pour le principe du pays d'origine», *Revue du Marché commun et de l'Union européenne*, 495 (2006), p. 83 secondo cui «*le juge communautaire a* révelé *l'existence de ce principe dans l'arrêt* Cassis de Dijon» (enfasi aggiunta).

24 O. Brati, «Dassonville and Cassis de Dijon – as the basic jurisprudence of the free movement of goods», *Academic Journal of Business, Administration, Law and Social Sciences*, 6, 1 (2020), p. 196; P. Defraigne e A. De Streel, *What is the digital internal market and where the European Union should intervene?*, rapp. tecn. 2011/33, Florence School of Regulation, 2011, p. 11

25 Garabiol-Furet, «Plaidoyer pour le principe du pays d'origine» cit., p. 82.

26 Ibidem.

27 T. Lutzi, «Internet Cases in EU Private International Law — Developing a Coherent Approach», *The International and Comparative Law Quarterly*, 66, 3 (2017), p. 706.

28 Corte giust., sentenza del 13 maggio 1997, causa C-233/94, *Repubblica federale di Germania c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:1997:231, § 64

29 G. De Baere, «'Is This a Conflict Rule Which I See before Me?' Looking for a Hidden Conflict Rule in the Principle of Origin as Implemented in Primary European Community Law and in the 'Directive on Electronic Commerce'», *Maastricht Journal of European and Comparative Law*, 11, 3 (2004), p. 308.

98/34/CE,[30] come modificata dalla direttiva 98/48/CE.[31] In realtà, tale direttiva risulta abrogata e sostituita dalla direttiva (UE) 2015/1535,[32] nel cui articolo 1, paragrafo 1, lettera b) ritroviamo la definizione di servizio della società dell'informazione:[33] si tratta di un qualsiasi servizio prestato normalmente (*i*) dietro retribuzione, (*ii*) a distanza, (*iii*) per via elettronica e (*iv*) a richiesta individuale di un destinatario di servizi.

Per quanto riguarda, invece, la definizione di «ambito regolamentato», ci si deve riferire all'articolo 2, paragrafo 1, lettera h), secondo cui esso è costituito dalle «prescrizioni degli ordinamenti degli Stati membri e applicabili ai prestatori di servizi della società dell'informazione o ai servizi della società dell'informazione, indipendentemente dal fatto che siano di carattere generale o loro specificamente destinati».

Il paese d'origine viene individuato come quello Stato membro in cui si trova il *prestatore stabilito*, definito dall'articolo 2, paragrafo 1, lettera c), come quel «prestatore che esercita effettivamente e a tempo indeterminato un'attività economica mediante un'installazione stabile». Trattandosi di servizi che, per loro natura, presentano una componente immateriale, a volte è difficile comprendere in quale Stato un prestatore sia stabilito: in generale, è possibile affermare che si tratta, di fatto, del luogo in cui l'attività viene esercitata in maniera stabile e duratura.[34]

Inoltre, per espressa previsione della direttiva, non rileva (o, *rectius*, non costituisce di per sé un indicatore dello stabilimento) il fatto che in tale luogo vi sia la presenza e l'uso dei mezzi tecnologici necessari per prestare il servizio (ad es., il luogo ove i server sono collocati). In dottrina si è sottolineato come questo principio sia diverso da quello espresso dalla direttiva 95/46/CE, poiché quest'ultima darebbe invece rilevanza alla collocazione delle infrastrutture informatiche, evidenziando come invece nel GDPR si possa ritrovare il medesimo criterio previsto

30 Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, GU L 204, 21/07/1998, pp. 37-48

31 Direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998 relativa ad una modifica della direttiva 98/34/CE che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, GU L 217, 5/08/1998, pp. 18-26

32 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 (codificazione), GU L 241, 17/09/2015, pp. 1-15

33 Sul significato di questi aspetti non è essenziale ora soffermarsi; alcuni di essi saranno discussi successivamente con riferimento al regime di applicabilità del DSA (v. par. 1.2).

34 Corte giust., sentenza del 30 novembre 1995, causa C-55/94, *Reinhard Gebhard c. Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, ECLI:EU:C:1995:411, § 27-28.

dalla direttiva E-Commerce.[35] In realtà, come peraltro parzialmente rilevato dalla medesima dottrina, sarebbe più corretto distinguere due diversi piani all'interno del diritto della protezione dei dati: il luogo di collocazione dell'infrastruttura rileva con riferimento al trasferimento di dati personali verso paesi terzi;[36] il luogo di stabilimento è utile per la determinazione dell'Autorità competente (o, vigente la precedente direttiva, della legge applicabile).

Come si è anticipato, se, da una parte, il principio del paese d'origine contribuisce a rafforzare la libertà di prestazione dei servizi, dall'altra esso è stato variamente criticato, in quanto può portare i prestatori a stabilirsi negli Stati membri dotati della disciplina a loro più favorevole, generando così una c.d. «*race to the bottom*»[37] (e così, allo stesso tempo, scoraggiare gli altri Stati membri ad adottare legislazioni più restrittive). La critica è sicuramente fondata, e prova ne sarà data nei successivi capitoli, ove si verificherà come anche il meccanismo di sportello unico previsto in relazione al GDPR abbia indotto molti titolari del trattamento a stabilirsi in luoghi ove le autorità di controllo appaiono meno severe. Bisogna tuttavia ricordare che – almeno teoricamente – tale atteggiamento degli Stati membri si pone in contrasto con lo spirito della direttiva, che, ad esempio, nel considerando 22[38] ricorda come l'obbligazione per lo Stato membro di stabilimento di "controllo all'origine" si traduce nella necessità per tale Stato di assicurare la tutela di interessi pubblici non solo ai suoi cittadini, ma a tutti i cittadini dell'Unione.[39]

Con riferimento al Digital Services Act, in sede di redazione del testo si è discusso circa il principio del paese d'origine, con alcuni Stati membri (prima fra tutti l'Irlanda) che premevano per mantenerlo inalterato, e altri Stati (tra cui la Francia) che spingevano per modificarlo, dando più poteri al paese di appartenenza

35 P. P. Polański, «Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union», *Computer Law & Security Review*, 34, 3 (2018), p. 565- 566.

36 Ragionevolmente, visto che la ratio della norma è evitare che i dati personali *in quanto tali* siano custoditi in Stati che non garantiscono un livello di tutela equivalente; v. cons. 101 GDPR: «[…] È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso […]».

37 D. Holznagel, «Platform Liability for Hate Speech & the Country of Origin Principle: Too Much Internal Market?: How hate speech liability rules for social media platforms are testing the boundaries of the E-Commerce-Directive's country of origin principle», *Computer Law Review International*, 21, 4 (2020), p. 104.

38 «È pertanto necessario garantire che l'autorità competente assicuri questa tutela non soltanto per i cittadini del suo paese ma anche per tutti cittadini della Comunità».

39 Polański, «Revisiting country of origin principle» cit., p. 564.

del destinatario del servizio.[40] Ad un primo esame, pare che il principio sia stato comunque mantenuto, visto che la vigilanza viene affidata al Coordinatore dei servizi digitali del luogo di stabilimento del prestatore del servizio intermediario (v. *infra* cap. 3). Tuttavia, alcuni elementi sembrano andare in senso contrario (e quindi temperare il principio), in particolare: *(i)* l'attribuzione alla Commissione di competenze esclusive di vigilanza sulle piattaforme online di dimensioni molto grandi (VLOP) e motori di ricerca online di dimensioni molto grandi (VLOSE) con riferimento agli obblighi supplementari previsti dalla sezione V del capo III;[41] *(ii)* l'individuazione della nozione di «contenuto illegale» come una qualsiasi informazione che non sia conforme al diritto dell'Unione *o al diritto di uno Stato membro conforme al diritto dell'Unione*: si nota qui come il legislatore europeo, pur avendo uniformato le condizioni e le procedure alle quali sia possibile procedere alla rimozione di tali contenuti,[42] adotta una definizione molto ampia, rimandando a ciascuno Stato membro (e non al solo Stato membro di "origine") l'individuazione di cosa sia contenuto illegale. Ciò comporta che i prestatori del servizio debbano far riferimento alle legislazioni di *tutti* gli Stati membri, rendendo probabilmente più difficoltoso coordinare la prestazione del servizio nell'ambito del mercato interno. Questo differisce dall'impostazione adottata in altre fonti comunitarie, ove invece l'individuazione del contenuto da rimuovere viene effettuata facendo esclusivo riferimento al diritto comunitario: si veda, ad esempio, il regolamento (UE) 2021/784,[43] il quale all'articolo 2, paragrafo 1, numero 7 definisce il «contenuto terroristico» facendo riferimento alla direttiva (UE) 2017/541.[44]

La regolazione dell'ambito digitale e la protezione dei dati personali

L'attività normativa dell'Unione europea non si è concentrata solamente sulla regolazione del mercato interno: infatti – man mano che le tecnologie digitali si diffondevano sempre di più, modificando il modo con cui le persone comunicano

40 L. Bertuzzi, «Digital Services Act: il duello Francia-Irlanda sul principio del 'paese d'origine'», *Euractiv* (27 settembre 2021), (visitato il 03/02/2024).

41 I. Buri e J. van Hoboken, «The General Approach of the Council on the Digital Services Act», *DSA Observatory* (7 dicembre 2021), (visitato il 04/02/2024).

42 A differenza della direttiva E-Commerce, dove anche tali aspetti sostanziali e procedurali erano lasciati agli Stati membri; v. G. Morgese, «Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE», *Federalismi.it*, 1 (2022), p. 86.

43 Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online, GU L 172, 17/05/2021, pp. 79–109

44 Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAIdel Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, GU L 88, 31/03/2017, pp. 6–21.

tra di loro e andando a costituire uno dei più importanti elementi dell'economia dell'Unione – il legislatore comunitario ha avvertito la necessità di regolare in maniera più stringente anche un ulteriore aspetto, ossia la protezione dei dati personali. Ciò è avvenuto (*i*) attraverso l'introduzione di fonti di diritto derivato, ma anche (*ii*) mediante l'inserimento all'interno dei Trattati – e anche della Carta dei diritti fondamentali dell'UE che, ai sensi dell'articolo 6 TUE, ha lo stesso valore dei Trattati – di disposizioni volte alla tutela dei dati personali.

Alla trattazione delle singole fonti normative va premessa un'avvertenza: il piano della prestazione di servizi digitali e quello della tutela dei dati personali non coincidono perfettamente, nel senso che può benissimo darsi un'attività di trattamento dei dati senza che quest'ultimo sia automatizzato[45]; ciò è confermato dall'articolo 2, paragrafo 1 GDPR, il quale afferma la sua applicabilità anche «*al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*», cosicché esso sarà applicabile anche con riferimento a dati personali contenuti in archivi cartacei.[46] Tuttavia, il trattamento di dati avviene pressoché sempre attraverso l'utilizzo di sistemi informatici, cosicché i due piani tendono, all'atto pratico, a sovrapporsi quasi completamente.

i) La protezione dei dati personali nel diritto primario

Nell'ambito del diritto primario, centrale è la norma di cui all'articolo 8 della Carta dei dritti fondamentali dell'Unione europea. Il paragrafo 1 sancisce, in maniera generale, il diritto di ogni individuo alla protezione dei «dati di carattere personale che lo riguardano». Il paragrafo seguente risulta più interessante da un punto di vista pratico, in quanto pone dei precisi requisiti affinché un trattamento possa considerarsi legittimo:[47] (*i*) deve essere presente una base giuridica adeguata (consenso o «altro fondamento legittimo»); (*ii*) è necessario rispettare il principio di lealtà; (*iii*) e il trattamento deve avvenire per finalità determinate dalla legge (ciò che in dottrina viene definito *principle of purpose limitation*). Inoltre, ai sensi del paragrafo 3, il rispetto di questi principi deve essere soggetto al controllo di autorità indipendenti.

45 Agenzia dell'Unione europea per i diritti fondamentali et al., *Manuale sul diritto europeo in materia di protezione dei dati: edizione 2018*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo 2018, p. 113.

46 M. Krzysztofek, *GDPR: General Data Protection Regulation (EU) 2016/679: post-reform personal data protection in the European Union*, Wolters Kluwer, Alphen aan den Rijn 2019, p. 32.

47 J. Reinhardt, «Realizing the Fundamental Right to Data Protection in a Digitized Society», in *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*, a cura di M. Albers e I. W. Sarlet, Springer, Cham 2022, p. 57.

La dottrina rileva come questi concetti siano stati per la prima volta elaborati non nella Carta, ma nel primo strumento dell'Unione dedicato alla protezione dei dati personali, cioè la direttiva 95/46/CE, cosicché si è generato l'insolito fenomeno per cui una norma di rango secondario è servita da base per la redazione di una norma di rango primario.[48] La giurisprudenza sviluppatasi con riferimento alla direttiva è utile per interpretare l'articolo 8.[49]

La disposizione ha generato in dottrina ampie riflessioni che, per ragioni di spazio, non possono essere compiutamente qui analizzate. Tuttavia, appare innanzitutto opportuno precisare che la norma sicuramente si rivolge, ex articolo 51 della Carta, alle istituzioni e agli organi dell'Unione e agli Stati membri quando applicano il diritto comunitario.[50] Discusso è invece il suo effetto orizzontale: il tema è importante in quanto, attualmente, una grande quantità di dati personali è detenuta da attori privati, in particolare dalle cd. *big tech*. Reinhardt sottolinea come il semplice fatto di avere un forte potere economico e sociale non comporti di per sé maggiori responsabilità circa il rispetto dei diritti fondamentali; allo stesso tempo, però, le *big tech* stanno sempre più incorporando – almeno formalmente – i diritti fondamentali nelle proprie linee guida.[51] Questa tendenza ha peraltro ricevuto crisma normativo proprio nel DSA, il quale all'articolo 14, paragrafo 4, ha previsto che i prestatori di servizi intermediari debbano applicare le condizioni generali rispettando i diritti delle parti «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».[52]

L'articolo 8 è stato utilizzato diverse volte dalla Corte di giustizia nelle proprie motivazioni. Ad esempio, nel caso *Digital Rights Ireland*, il giudice di Lussemburgo ha affermato che la direttiva sulla conservazione dei dati (detta anche direttiva *data retention*)[53] era in contrasto con l'articolo 8 della Carta e conseguentemente

48 T. Lock, «Article 8 CFR», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer et al., Oxford University Press, New York 2019, p. 2122.

49 P. Vogiatzoglou e P. Valcke, «Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law», in *Research Handbook on EU Data Protection Law*, Edward Elgar Publishing, Cheltenham 2022, p. 20; Lock, «Article 8 CFR» cit., p. 2122.

50 Reinhardt, «Realizing the Fundamental Right to Data Protection in a Digitized Society» cit., p. 56.

51 Ivi, p. 59-60.

52 Si v. J. P. Quintais et al., «Using Terms and Conditions to apply Fundamental Rights to Content Moderation», *German Law Journal*, 24, 5 (2023), p. 897, secondo cui tra i vari diritti che i prestatori dovrebbero applicare vi è anche il diritto alla protezione dei dati personali di cui all'articolo 8 della Carta.

53 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva

ne ha pronunciato l'invalidità.[54] Inoltre, nel parere emesso ai sensi dell'articolo 218, paragrafo 11, TFUE circa il progetto di accordo tra il Canada e l'Unione europea per il trasferimento dei dati del codice di prenotazione dei passeggeri aerei, la Grande Sezione della Corte ha dato parere negativo a tale proposta in quanto essa contrastava, tra gli altri, con l'articolo 8 della Carta, essendo violati i requisiti stabiliti nel paragrafo 2.[55] Infine, nella nota causa *Schrems*,[56] la Corte si è servita della medesima norma per annullare la decisione della Commissione «*Approdo Sicuro*»[57] che autorizzava il trasferimento dei dati personali verso gli Stati Uniti.

L'altra norma di diritto primario che risulta necessario analizzare è l'articolo 16 TFUE. Il paragrafo 1 stabilisce un principio del tutto analogo rispetto a quello previsto dall'articolo 8, paragrafo 1 della Carta, affermando il diritto di ogni individuo alla protezione dei dati personali che lo riguardano. Tuttavia, la ripetizione non è probabilmente superflua, in quanto l'inserimento di tale diritto nel Trattato sul funzionamento permette di ovviare ai problemi posti dall'articolo 51 della Carta e sancirne l'applicabilità *erga omnes*, e quindi anche a soggetti privati le cui attività possono interferire con lo stesso.[58] Circa il rapporto tra le due disposizioni appena citate, si deve sottolineare che è stato chiarito dalla Corte di giustizia – nel parere *Accordo PNR UE-Canada* già citato – che, se è vero che entrambe sanciscono il diritto alla protezione dei dati, nel valutare la compatibilità di un atto di diritto derivato dell'Unione con il diritto primario vi è da riferirsi alla norma di cui all'articolo 8, paragrafo 2, della Carta, in quanto essa stabilisce condizioni più stringenti in presenza delle quali può essere svolto il trattamento.[59] In altre parole, quest'ultima norma riveste natura di *lex specialis* rispetto al generale diritto stabilito dall'articolo 16 TFUE.[60]

2002/58/CE, GU L 105, 13/04/2006, pp. 54–63.

54 Corte giust., sentenza del 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, ECLI:EU:C:2014:238, § 36-37.

55 Parere della Corte (Grande Sezione) del 26 luglio 2017, 1/15, ECLI:EU:C:2017:592, § 126, 163, 167, 232.

56 Corte giust., sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, ECLI:EU:C:2015:650.

57 Decisione della Commissione 2000/520/CE del 26 luglio 2000 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, GU L 215, 25/08/2000, pp. 7-47.

58 B. Cortese, «La protezione dei dati a carattere personale nel diritto dell'Unione Europea dopo il Trattato di Lisbona», *Il Diritto dell'Unione Europea*, 2 (2013), p. 314, 317.

59 Parere della Corte (Grande Sezione) del 26 luglio 2017, 1/15, cit., § 119-120.

60 C. Graziani, «PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali», *DPCE Online*, 33, 4 (2017), p. 962.

Il paragrafo 2 conferisce invece al Parlamento europeo ed al Consiglio il potere di stabilire, deliberando con la procedura legislativa ordinaria, «le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati». Si tratta di una norma fortemente innovativa,[61] in quanto va ad costituire una base giuridica dapprima inesistente e che conferisce all'Unione il potere di legiferare *in generale* circa la tutela dei dati personali.[62] Ciò segna una differenza rispetto al passato, e in particolare rispetto al vecchio articolo 286 CE,[63] il quale prevedeva sì una base giuridica relativa alla tutela dei dati personali, ma ciò solamente in riferimento ai dati trattati da istituzioni, organi e organismi della Comunità e, quindi, non dagli Stati membri né da soggetti privati.

ii) La protezione dei dati personali nel diritto derivato

L'analisi della base giuridica di cui all'articolo 16 TFUE dà l'occasione per esaminare gli atti di diritto derivato posti a tutela del diritto alla protezione dei dati personali.

In realtà, il primo strumento dedicato a questo tema, ossia la direttiva 95/46/CE, è stato adottato prima dell'entrata in vigore del Trattato di Lisbona e, dunque, in un momento in cui l'articolo 16 non era ancora esistente. Difatti, la base giuridica adottata dal legislatore dell'epoca è l'allora articolo 100A del Trattato CEE (attuale art. 114 TFUE), il quale aveva ad oggetto l'adozione di misure volte all'instaurazione e al funzionamento del mercato interno. Si tratta di un'impostazione giustificata, visto che all'epoca erano già state approvate alcune legislazioni nazionali in materia e si presentava la necessità di armonizzarle,[64] al fine di evitare la frammentazione del mercato interno.[65] La direttiva presentava dunque un duplice approccio: da una parte quello appena citato, relativo al mercato interno, espresso anche dal

61 Si v. AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI et al., *Manuale sul diritto europeo* cit., p. 32, secondo cui l'articolo 16 fornisce «una base giuridica indipendente, per un approccio moderno e globale alla protezione dei dati».

62 CORTESE, «La protezione dei dati a carattere personale nel diritto dell'Unione Europea dopo il Trattato di Lisbona» cit., p. 314.

63 F. POCAR et al., *Commentario breve ai trattati dell'Unione europea*, 2ª ed., CEDAM, Padova 2014, p. 189.

64 AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI et al., *Manuale sul diritto europeo* cit., p. 32.

65 V. cons. 8: «considerando che, per eliminare gli ostacoli alla circolazione dei dati personali, il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento di tali dati deve essere *equivalente in tutti gli Stati membri*; che tale obiettivo, fondamentale per il mercato interno, *non può essere conseguito esclusivamente attraverso l'azione degli Stati membri*, tenuto conto

divieto per gli Stati membri di «restringere o vietare la libera circolazione dei dati personali» tra essi (art. 1 direttiva);[66] dall'altra, il perseguimento di un alto livello di tutela dei diritti fondamentali, e in particolare del diritto alla privacy.[67]

Come è noto, il successore della direttiva 95/46/CE è il Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore il 25 maggio 2018. Sul piano delle fonti, la differenza che si nota è la natura regolamentare del GDPR, da cui discende la sua diretta efficacia ed applicabilità nei confronti degli individui, senza che sia necessario un intervento degli Stati membri: ciò è particolarmente importante se si considera che uno dei problemi principali insorti con riferimento alla direttiva era proprio che la sua implementazione da parte dei legislatori nazionali aveva portato alla creazione di discipline piuttosto disomogenee tra di loro.[68]

L'approvazione del GDPR è stata inoltre favorita anche dall'introduzione di una base giuridica generale riferita alla protezione dei dati (art. 16 TFUE, v. *supra*): il legislatore europeo può dunque assumere come obiettivo principale proprio la tutela di tale diritto, senza che per il suo raggiungimento sia necessario evocare il miglioramento del mercato interno. Ciò non significa che quest'ultima dimensione venga comunque completamente trascurata: infatti, già l'articolo 1 afferma al paragrafo 1 che il GDPR «stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, *nonché norme relative alla libera circolazione di tali dati*» e al paragrafo 3 un principio analogo a quello previsto nell'articolo 1 della direttiva, ossia che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

Sulla portata di quest'ultima norma si è discusso: secondo parte della dottrina essa apparirebbe in contrapposizione con il paragrafo 1, nel senso che andrebbe ad ergere a valore primario non il diritto fondamentale dell'individuo, *ma la libera circolazione dei dati*.[69] Queste osservazioni sono in linea di principio condivisibili, tuttavia è necessario aggiungere alcune considerazioni: nonostante la natura rego-

in particolare dell'ampia divergenza esistente attualmente tra le normative nazionali in materia […]; che risulta pertanto necessario un intervento della Comunità ai fini di un ravvicinamento delle legislazioni;», corsivo aggiunto.

66 V. anche cons. 9: «considerando che, data la protezione equivalente derivante dal ravvicinamento delle legislazioni nazionali, gli Stati membri non potranno più ostacolare la libera circolazione tra loro di dati personali per ragioni inerenti alla tutela dei diritti e delle libertà delle persone fisiche, segnatamente del diritto alla vita privata […]».

67 P. Hustinx, «EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation», in *New Technologies and EU Law*, a cura di M. Cremona, Oxford University Press, Oxford 2017, p. 131.

68 Ivi, p. 149.

69 C. Sarra, *Il mondo-dato: saggi su datificazione e diritto*, 2. ed, CLEUP, Padova 2022, p. 66.

lamentare del GDPR,[70] adottando un'interpretazione sistematica[71] è ragionevole affermare che la disposizione – come accadeva nella precedente direttiva – sia comunque rivolta *solo* agli Stati membri.[72] Difatti, sono proprio questi ultimi che avrebbero, in astratto, il potere di effettuare tali restrizioni, adottando una legislazione nazionale che blocchi il "flusso di dati". Quello che il paragrafo 3 sembra dire è, dunque, che gli Stati membri non possono addurre come motivo per la restrizione della circolazione dei dati personali all'interno dell'Unione europea la presenza, in un altro Stato membro, di uno standard inferiore di tutela del diritto alla protezione dei dati: ammettere un simile scenario significherebbe, di fatto, tradire gli obiettivi sanciti dal legislatore, cioè la creazione di uno spazio giuridico europeo ove la tutela del diritto è uniforme.[73] Peraltro, vista la natura programmatica della norma, risulta difficile ipotizzarne un'applicazione pratica diversa da quella prospettata,[74] cosicché, anche se essa avesse un effetto astratto nei confronti degli individui, concretamente non riuscirebbe a produrre alcuna conseguenza.

Inoltre, vi è da considerare che la base giuridica di cui all'articolo 16 TFUE è indirizzata sia all'obiettivo della tutela dei dati sia a quello della "condivisione" degli stessi all'interno dell'Unione. Quindi, è vero che il GDPR non vede più il suo fondamento nell'articolo 114 TFUE, com'era invece il caso della direttiva 95/46/CE; tuttavia, ciò non significa che il legislatore fosse autorizzato dai Trattati a ignorare completamente uno dei due obiettivi posti dalla norma.

70 Ivi, p. 66-67.

71 Si deve ricordare che, per giurisprudenza costante della Corte, «per quanto riguarda l'interpretazione di una disposizione del diritto dell'Unione, si deve tener conto non soltanto del tenore letterale della stessa, ma anche del suo contesto e degli scopi perseguiti dalla normativa di cui essa fa parte», Corte giust., sentenza del 21 dicembre 2021 (Grande Sezione), causa C-124/20, *Bank Melli Iran c. Telekom Deutschland GmbH*, ECLI:EU:C:2021:1035, § 43; *ex multis* si v. anche Corte giust., sentenza del 18 maggio 2000, causa C-301/98, *KVS International BV c. Minister van Landbouw, Natuurbeheer en Visserij*, ECLI:EU:C:2000:269, § 21; Corte giust., sentenza del 17 novembre 1983, causa 292/82, *Firma E. Merck c. Hauptzollamt Hamburg-Jonas*, ECLI:EU:C:1983:335, § 12.

72 V. H. Hijmans, «Article 1 Subject-matter and objectives», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 57, il quale sottolinea: «*Article 1(3) does not mention the addressees of this negative obligation. Arguably,* this provision is addressed to the Member States *and is meant to prevent them from adopting national laws restricting the free movement of data.*», enfasi aggiunta.

73 Si v. il cons. 10: «[…] il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione […]».

74 Sarra, *Il mondo-dato* cit., p. 70.

Il Regolamento generale sulla protezione dei dati ha apportato numerose innovazioni e pone significative questioni interpretative: chiaramente, non è qui possibile presentare tali tematiche, poiché esulerebbero da quanto necessario per lo sviluppo del tema oggetto dell'elaborato. Si rinvia però al capitolo 2, ove si esamineranno i meccanismi di *enforcement* predisposti dal GDPR.

Infine, si ritiene opportuno precisare che il Regolamento generale sulla protezione dei dati non esaurisce il novero degli atti volti alla tutela del diritto alla protezione dei dati personali. Infatti, sono in vigore anche altre fonti comunitarie: *(i)* la Direttiva 2002/58/CE[75], chiamata anche direttiva «E-privacy»; *(ii)* la Direttiva (UE) 2016/680[76] – cd. detta «Direttiva Polizia» o «*LED*» (*Law Enforcement Directive*) – la quale si occupa dei casi in cui il trattamento dei dati viene effettuato ai fini di prevenzione, indagine ed accertamento di reati; *(iii)* il Regolamento (UE) 2018/1725[77] il quale sancisce principi del tutto simili a quelli previsti dal GDPR, ma si applica alle istituzioni, agli organi e agli organismi dell'Unione.

Struttura dell'elaborato

Per quanto riguarda la struttura dell'elaborato, nel capitolo 1 si presenteranno, dapprima, le principali novità e caratteristiche del DSA. Successivamente, saranno presentati i punti di intersezione tra le due discipline, in quanto tale disamina è utile a capire come una medesima fattispecie concreta possa essere presa in considerazione dai due regolamenti in esame.

I capitoli 2 e 3 si concentrano sull'analisi dei meccanismi di *enforcement* previsti, rispettivamente, da GDPR e DSA: essi – pur presentando una disciplina in parte comune e in parte diversa – sono accomunati dalla necessità di far sì che la loro attuazione sia effettiva, onde evitare che le norme in essi contenute rimangano di applicazione solo teorica o, comunque, non ottimale. Il meccanismo previsto dal GDPR rappresenta il modello più significativo di attuazione di un regolamento

75 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, GU L 201, 31/01/2002, pp. 37-47.

76 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 116, 04/05/2016, pp. 89-131.

77 Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, GU L 295, 21/11/2018, pp. 39-98.

europeo in ambito digitale: la sua analisi è dunque utile in modo comprendere come l'*enforcement* del DSA potrà poi concretarsi. Chiara è l'esigenza di evitare che gli errori – sia di formulazione del testo normativo, sia applicativi – commessi con riferimento al Regolamento generale sulla protezione dei dati siano ripetuti per il DSA.

1

LA REGOLAZIONE DEI SERVIZI DIGITALI TRA DSA E GDPR

1.1 *La genesi del Digital Services Act*

Nella sua comunicazione del 19 febbraio 2020 *Plasmare il futuro digitale dell'Europa*,[1] la Commissione europea ha annunciato l'intenzione di adottare nuove regole con riferimento al mercato unico digitale, volte ad armonizzare e rinforzare il regime di responsabilità delle piattaforme online. A ciò è conseguita l'emanazione da parte della Commissione, il 15 dicembre 2020, della «Proposta di regolamento relativo a un mercato unico dei servizi digitali».[2] È possibile analizzare brevemente il contenuto di quest'ultima, così da comprendere quali siano le ragioni che hanno portato la Commissione ad esercitare il suo potere di cui all'articolo 17, paragrafo 2, TUE.

(*i*) Innanzitutto, la Commissione osserva che il quadro giuridico dell'UE che disciplina i servizi digitali si fonda in primo luogo sulla direttiva e-commerce.[3] Non vi è l'intenzione di abrogare completamente tale strumento, in quanto si ritiene che i principi generali in esso espressi siano ancora validi. Tuttavia, la Commissione fa notare che a partire dall'adozione della direttiva 2000/31/CE si sono sviluppati nuovi ed innovativi servizi digitali, i quali hanno modificato gli strumenti con i quali i cittadini dell'Unione entrano in contatto tra di loro e hanno trasformato l'economia comunitaria. Tali servizi, quindi, hanno posto – e pongono tuttora – nuove sfide regolatorie, generando così la necessità di un intervento dell'Unione, al fine di sviluppare le potenzialità e contrastare i rischi che essi creano.[4]

(*ii*) Con riferimento al regime di responsabilità dei prestatori di servizi intermediari, la proposta: (*a*) ritiene di conservare i principi della direttiva sul commercio

1 Commissione Europea, *Shaping Europe's digital future.* Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo 2020.

2 Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM(2020) 825 final), d'ora in poi «Proposta DSA».

3 «Proposta DSA», p. 3.

4 Ivi, p. 1.

elettronico, nella convinzione che essi siano «ormai un fondamento dell'economia digitale»[5]; (*b*) esprime la necessità che, tuttavia, tali principi siano ora contenuti in un regolamento, così da armonizzare efficacemente le legislazioni in tutta l'Unione[6] (ed infatti, si propone di abrogare i corrispondenti articoli della direttiva, da 12 a 15, per trasfonderli nel nuovo regolamento). In particolare, si prevede di (*c*) mantenere il divieto di obblighi generali di sorveglianza,[7] consentendo invece misure di monitoraggio specifico.[8] Inoltre, (*d*) viene recepita la giurisprudenza della Corte[9] circa la distinzione tra condotta neutrale del fornitore – caso in cui si applica l'esenzione – e, invece, ruolo attivo dello stesso,[10] ruolo che fa insorgere la responsabilità.

(*iii*) Per quanto riguarda le innovazioni, esse si sono concentrate essenzialmente nei seguenti ambiti: (*a*) previsione di una serie di nuovi obblighi per i fornitori di servizi intermediari;[11] (*b*) armonizzazione delle condizioni procedurali in presenza delle quali può essere ordinata da un'autorità nazionale la rimozione o la limitazione di un certo contenuto (articolo 9 DSA); (*c*) introduzione di obblighi aggiuntivi a carico delle piattaforme di grandi dimensioni, tra cui si annoverano obblighi di trasparenza; (*d*) previsione di forme di controllo del rispetto di tali obblighi da parte non solo di enti pubblici, ma anche di ricercatori, cui viene attribuito un diritto di accesso ai dati (articolo 40 DSA); (*e*) attribuzione alla Commissione di poteri di vigilanza (quasi) esclusivi con riferimento alle grandi piattaforme.

5 Ivi, p. 3.

6 Ibidem.

7 In giurisprudenza v. Corte giust., sentenza del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, ECLI:EU:C:2019:821.

8 G. Caggiano, «La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea», *Annali AISDUE*, 3 (2021), p. 18; per un'analisi sull'impatto che tali misure di monitoraggio possono avere sui diritti fondamentali v. G. Frosio e C. Geiger, «Taking fundamental rights seriously in the Digital Services Act's platform liability regime», *European Law Journal*, 29, 1-2 (2023); A. Turillazzi et al., «The digital services act: an analysis of its ethical, legal, and social implications», *Law, Innovation and Technology*, 15, 1 (2023).

9 La quale non è molto chiara circa la distinzione tra ruolo attivo e neutrale, come ricorda F. Wilman, «The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act», *JIPITEC*, 12, 3 (2021); si v., ad es., i casi Corte giust., sentenza del 12 luglio 2011 (Grande Sezione), causa C-324/09, *L'Oréal SA e altri c. eBay International AG e altri*, ECLI:EU:C:2011:474, § 113-116; Corte giust., sentenza del 23 marzo 2010 (Grande Sezione), cause riunite da C-236/08 a C-238/08, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA (C-236/08), Google France SARL c. Viaticum SA e Luteciel SARL (C-237/08) e Google France SARL c. Centre national de recherche en relations humaines (CNRRH) SARL e altri (C-238/08)*, ECLI:EU:C:2010:159, § 114.

10 Caggiano, «La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea» cit., p. 17.

11 Ivi, p. 4.

(*iv*) Ulteriormente, la proposta si sofferma sulla necessità che, nell'ambito del mercato unico dei servizi digitali, il quale è per sua natura senza frontiere, vi sia «una *cooperazione rafforzata* tra gli Stati membri per garantire l'efficacia della vigilanza e dell'applicazione delle nuove norme».[12] L'analisi di tali meccanismi di coordinamento sarà effettuata nel capitolo 3.
(*v*) Infine, per quanto riguarda la base giuridica, essa viene individuata nell'articolo 114 TFUE. Spiega infatti la Commissione che l'obiettivo principale del regolamento proposto sarebbe garantire il miglior funzionamento del mercato interno con riguardo alla prestazione dei servizi digitali transfrontalieri, «tenendo conto che numerosi Stati membri hanno legiferato o intendono legiferare su questioni quali la rimozione di contenuti illegali online».[13] In effetti, si deve osservare come quest'ultimo punto sia vero:[14] tendenze simili si erano in particolare riscontrate in Germania – con l'approvazione del *Netzwerkdurchsetzungsgesetz* – e in Francia,[15] con l'approvazione della c.d. «*Loi Avia*».[16]

Nell'economia del presente elaborato non è chiaramente possibile procedere ad una disamina di tutte le innovazioni che il regolamento (UE) 2022/2065 ha apportato e dei problemi che esso pone. Nei paragrafi che seguono ci si concentrerà quindi su taluni aspetti che si ritengono più utili ai fini della comprensione dei temi che saranno trattati nei successivi capitoli.

1.2 *L'ambito di applicazione materiale del DSA*

La trattazione di specifici aspetti del regolamento deve essere preceduta dalla comprensione di quale sia il suo ambito di applicazione e dall'illustrazione delle principali definizioni impiegate dal legislatore.

L'articolo 2, paragrafo 1, DSA prevede la sua applicabilità ai «servizi intermediari», i quali sono definiti dall'articolo 3, paragrafo 1, lettera g), come uno dei seguenti *servizi della società dell'informazione*: (*i*) il servizio di semplice trasporto (*mere conduit*); (*ii*) il servizio di memorizzazione temporanea (*caching*); (*iii*) il servizio di memorizzazione di informazione (*hosting*).

12 «Proposta DSA», p. 3.
13 «Proposta DSA», p. 6.
14 R. Sabia, «L'enforcement pubblico del Digital Services Act tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni», *MediaLaws*, 2 (2023), p. 90.
15 G. Buttarelli, «La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche», *Giornale di diritto amministrativo*, 1 (2023), p. 120.
16 La quale, peraltro, è stata parzialmente dichiarata incostituzionale dal *Conseil constitutionnel* con sentenza del 18 giugno 2020, `https://www.legifrance.gouv.fr/cons/id/CONSTEXT000042053930/`.

Prima di addentrarsi nella spiegazione di questi tre concetti, appare necessario concentrarsi sulla definizione di «servizi della società dell'informazione»: infatti, la lettera g) appena citata postula tale qualifica, cosicché non si potrà dire di essere in presenza di un servizio intermediario se esso non presenta i requisiti del «servizio della società dell'informazione». Nel capitolo precedente si è già accennato al fatto che tale definizione (così come confermato anche dall'art. 3, par. 1, lett. a), DSA) è da rinvenire all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535, il quale pone i seguenti requisiti: deve trattarsi di un qualsiasi servizio prestato (*i*) dietro retribuzione, (*ii*) a distanza, (*iii*) per via elettronica e (*iv*) a richiesta individuale di un destinatario di servizi. Con riferimento a quest'ultimo elemento, esso comporta che nella definizione rientrino solo i cd. servizi «on demand», mentre vengono esclusi i servizi «punto-a-multipunto», come ad esempio la diffusione televisiva o radiofonica,[17] i quali sono disciplinati dalla diversa direttiva (UE) 2018/1808 (direttiva sui servizi di media audiovisivi).[18]

Il primo elemento, quello della retribuzione, è particolarmente interessante, in quanto pone un problema circa il suo rapporto con la maggior parte delle piattaforme utilizzate attualmente. Infatti, l'utilizzo di queste ultime non prevede quasi mai un corrispettivo pagato dall'utente, mentre il prestatore è remunerato grazie ai proventi della pubblicità mostrata mentre si fa uso del servizio. Il tema è stato analizzato dalla Corte di giustizia in *Papasavvas*,[19] ove si è osservato che il considerando 18 della direttiva 2000/31/CE esplicitamente precisa che i servizi della società dell'informazione ricomprendono anche «servizi non remunerati dal loro destinatario, nella misura in cui costituiscono un'attività economica».[20] Tale considerazione può essere mantenuta anche per il DSA, visto che l'articolo 2 della direttiva non è stato abrogato. Inoltre, il giudice osserva che tale impostazione è coerente con l'articolo 57 TFUE,[21] il quale – secondo la Corte[22] – non

17 A. Michinelli, «I servizi intermediari della società dell'informazione», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 46.

18 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, GU L 303, 14/11/2018, pp. 69-92.

19 Corte giust., sentenza del 11 settembre 2014, causa C-291/13, *Sotiris Papasavvas c. O Fileleftheros Dimosia Etaireia Ltd e a.*, ECLI:EU:C:2014:2209.

20 Ivi, § 28.

21 Ivi, § 29.

22 V. Corte giust., sentenza del 26 aprile 1988, causa 352/85, *Bond van Adverteerders e altri c. Stato dei Paesi Bassi*, ECLI:EU:C:1988:196, § 16: «[…] l'art. 60 del trattato non prescrive che il servizio sia pagato da coloro che ne fruiscono. Dal canto loro, le emittenti ricevono dai pubblicitari un

prescrive che il servizio sia pagato da colui che ne usufruisce. In *Mc Fadden* la Corte ulteriormente ribadisce:

> […] la remunerazione di un servizio fornito da un prestatore nell'ambito della sua attività economica non è necessariamente versata dai soggetti che ne fruiscono.[23]
>
> […] Ciò si verifica, in particolare, nel caso in cui una prestazione effettuata a titolo gratuito sia fornita da un prestatore a fini pubblicitari per beni venduti o servizi forniti dal medesimo prestatore, dato che il costo di tale attività è così integrato nel prezzo di vendita di tali beni o di tali servizi.[24]

Inoltre, è possibile richiamare l'idea per cui la cessione dei propri dati personali costituirebbe il corrispettivo per l'erogazione del servizio. Si tratta di una tesi assolutamente non pacifica in dottrina. Da una parte vi è chi sostiene che il diritto alla protezione dei dati personali sia un diritto fondamentale, indisponibile ed inalienabile, sancito da numerose disposizioni di diritto primario e che, dunque, non sia possibile in alcun modo commercializzare i dati personali.[25] Custers e Malgieri hanno ulteriormente rilevato che l'idea del dato come corrispettivo entra in contraddizione con le norme del GDPR, ad esempio quella per cui il consenso può essere revocato in ogni momento e senza alcuna motivazione, cosicché il titolare del trattamento potrebbe poi trovarsi senza la "controprestazione" prima pattuita.[26]

Dall'altra parte vi è invece chi fa leva sulla circostanza ormai pacifica per cui, nella pratica, il dato personale è correntemente scambiato per ricevere in cambio beni o servizi.[27] Vi è qui da dar conto di una pronuncia del TAR Lazio che, in riferimento alla tesi per cui la tutela dei dati personali debba essere vista solo come dato personale, così si esprime:

> tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un asset disponibile in senso negoziale,

corrispettivo per il servizio che forniscono a questi mandando in onda i loro messaggi»; v. anche Corte giust., sentenza del 11 aprile 2000, cause riunite C-51/96 e C-191/97, *Christelle Deliège c. Ligue francophone de judo et disciplines associées ASBL, Ligue belge de judo ASBL, Union européenne de judo e François Pacquée*, ECLI:EU:C:2000:199, § 56-57.

23 Corte giust., sentenza del 15 settembre 2016, causa C-484/14, *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, ECLI:EU:C:2016:689, § 41.

24 Ivi, § 42.

25 A. Landi, «L'*exchange commerce*. La Direttiva (UE) 2019/770», in *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, a cura di L. Bolognini, Giuffrè Francis Lefebvre, Milano 2021, p. 146-147.

26 B. Custers e G. Malgieri, «Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data», *Computer Law & Security Review*, 45 (2022).

27 G. D'Ippolito, «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», *Il Diritto dell'Informazione e dell'Informatica*, 634, 3 (2020), p. 647.

> suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto.
>
> A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati.[28]

Non si ha in questa sede il tempo di esaminare quale tesi sia preferibile; tuttavia, bisogna dare atto che in quest'ultima direzione sembra andare anche la direttiva (UE) 2019/770,[29] il cui articolo 3, paragrafo 1, secondo alinea, statuisce la sua applicabilità «altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore *e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico*» (corsivo aggiunto).[30] Inoltre, il considerando 24 ricorda che «[l]a fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico».[31]

Fatta questa precisazione, bisogna ulteriormente chiarire che la nozione di «servizio della società dell'informazione» è risultata, con riferimento alla direttiva e-commerce, talvolta opaca. Visto che la formulazione normativa è rimasta intatta, tali problemi interpretativi rischiano di affliggere anche il DSA e, secondo la dottrina, ciò rischia di avere delle conseguenze perverse circa l'applicabilità del regolamento in esame.[32] Ci si riferisce soprattutto ad alcuni casi portati all'attenzione della Corte di giustizia in cui il giudice del rinvio nutriva dubbi circa l'ascrivibilità di un certo servizio alla categoria in esame, e quindi all'applicabilità a tale servizio di alcune norme, segnatamente dell'articolo 56 TFUE e, appunto, della direttiva 2000/31/CE. Si trattava di casi in cui il servizio prestato potrebbe essere definito come "misto",[33] nel senso che ad una componente di intermediazione on-

28 TAR Lazio, sez. I, 10 gennaio 2020, n. 261.

29 Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, GU L 136, 22/05/2019, pp. 1–27.

30 D'Ippolito, «Commercializzazione dei dati personali» cit., p. 666.

31 Landi, «L'*exchange commerce*.» cit., p. 151.

32 P. Van Cleynenbreugel, «The Commission's digital services and markets act proposals: First step towards tougher and more directly enforced EU rules?», *Maastricht Journal of European and Comparative Law*, 28, 5 (2021), p. 670.

33 Questo il termine utilizzato dall'Avvocato Generale Szpunar nelle sue conclusioni presentate l'11 maggio 2017, causa C-434/15, *Asociación Profesional Elite Taxi c. Uber Systems Spain SL*, § 28; v. anche M. Sieradzka, «Asociación Profesional Elite Taxi vs Uber Systems Spain SL: Differences between the Internet Platform and the Transport Service», *Journal of European Competition Law & Practice*, 11, 5-6 (2020), p. 264-265.

line se ne aggiungeva un'altra, invece, fisica. In particolare, nel caso *Elite Taxi*,[34] lo *Juzgado de lo Mercantil n. 3 de Barcelona* (tribunale di commercio n. 3 di Barcellona) si domandava se il servizio – prestato da una società per mezzo di un'applicazione e in maniera retribuita, consistente nella «messa in contatto di conducenti non professionisti, privi di licenze e autorizzazioni amministrative, che utilizzano il proprio veicolo con persone che intendono effettuare spostamenti urbani»[35] – fosse da considerarsi come rientrante nel concetto di servizio di cui all'articolo 56 TFUE e, all'interno di questa categoria, di servizio della società dell'informazione o se, alternativamente, dovesse essere qualificato come «servizio nel settore dei trasporti», ai sensi dell'articolo 58, paragrafo 1, TFUE, e, di conseguenza, escluso dall'ambito di applicazione dell'articolo 56 TFUE. A questo proposito, la Corte ritiene di tenere distinti da un lato il servizio di intermediazione tramite app, e, dall'altro, il servizio di trasporto vero e proprio,[36] ammettendo che, in linea di principio, il primo di questi soddisfi i criteri per essere qualificato «servizio della società dell'informazione».[37] Tuttavia, nel caso di specie, i giudici osservano che esso è più di un mero servizio di intermediazione: questo perché il software fornito dalla società e l'influenza che la stessa esercita sui fornitori del servizio legano inestricabilmente l'attività online con quella di trasporto fisico dei passeggeri.[38] Infatti, fa notare la Corte che

> il servizio d'intermediazione della Uber si basa sulla selezione di conducenti non professionisti che utilizzano il proprio veicolo ai quali tale società fornisce un'applicazione *senza la quale, da un lato, tali conducenti non sarebbero indotti a fornire servizi di trasporto* e, dall'altro, le persone che intendono effettuare uno spostamento nell'area urbana non ricorrerebbero ai servizi di tali conducenti. Inoltre, la Uber esercita un'*influenza determinante* sulle condizioni della prestazione di siffatti conducenti. In relazione a tale ultimo punto, emerge segnatamente che la Uber fissa, mediante l'omonima applicazione, se non altro il prezzo massimo della corsa, che tale società riceve tale somma dal cliente prima di versarne una parte al conducente non professionista del veicolo e che essa esercita un determinato

34 Corte giust., sentenza del 20 dicembre 2017 (Grande Sezione), causa C-434/15, *Asociación Profesional Elite Taxi c. Uber Systems Spain SL*, ECLI:EU:C:2017:981.

35 Ivi, § 2.

36 Ivi, § 34: «un servizio d'intermediazione consistente nel mettere in contatto un conducente non professionista che utilizza il proprio veicolo e una persona che intende effettuare uno spostamento in area urbana costituisce, in linea di principio, un servizio distinto dal servizio di trasporto che consiste nell'atto fisico di trasferimento di persone o di beni da un luogo a un altro tramite un veicolo».

37 Ivi, § 35.

38 E. Marasà e O. Pollicino, «EU Court of Justice rules that Uber provides a transport service and is not a mere electronic intermediary: regulatory implications and "digital" judicial insulation», *MediaLaws* (8 febbraio 2018), (visitato il 15/02/2024); P. Hacker, «UberPop, UberBlack, and the Regulation of Digital Platforms after the Asociación Profesional Elite Taxi Judgment of the CJEU», *European Review of Contract Law*, 14, 1 (2018), p. 83.

> controllo sulla qualità dei veicoli e dei loro conducenti nonché sul comportamento di quest'ultimi, che può portare, se del caso, alla loro esclusione.[39]

Ciò porta la Corte ad affermare che il servizio di intermediazione debba essere considerato parte integrante di un servizio complessivo in cui l'elemento principale è un servizio di trasporto.[40] Inglobato il primo nel secondo, ne discende l'impossibilità di sussumere il servizio di intermediazione nella categoria individuata dall'articolo 2, lettera a), della direttiva 2000/31.

Secondo la dottrina, i giudici di Lussemburgo avrebbero individuato un vero e proprio «*Uber test*»,[41] in base al quale il servizio di intermediazione debba considerarsi parte integrante del servizio intermediato quando: (*i*) la piattaforma rende possibile la prestazione di un servizio che altrimenti non avrebbe potuto essere stato erogato[42], così da creare un mercato dapprima inesistente (cd. piattaforma «*market maker*»);[43] (*ii*) la piattaforma esercita un'influenza dominante sulle caratteristiche del nuovo servizio.[44]

Nel successivo caso *AirBnb Ireland*,[45] la Corte, nel valutare se il servizio offerto da tale società fosse un «servizio della società dell'informazione», pare però aver adottato un'impostazione parzialmente diversa: come in *Elite Taxi*, anche in questo caso la piattaforma offerta da AirBnb incontrerebbe, in linea di principio, i requisiti fissati dalla direttiva 2000/31, in quanto si tratta di un servizio normalmente prestato dietro retribuzione, a distanza, con mezzi elettronici e fornito su richiesta.[46] Tuttavia, viene osservato che, diversamente dal caso precedente, qui il servizio di mediazione immobiliare ha «un carattere distinto dall'operazione immobiliare propriamente detta», [47] precisando inoltre che «un servizio come quello fornito dalla Airbnb Ireland non risulta per nulla indispensabile alla rea-

39 Corte giust., causa C-434/15, *Asociación Profesional Elite Taxi* cit., § 39, corsivo aggiunto.
40 Ivi, § 40.
41 C. Busch, «The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'? Some observations on the pending case C-390/18 – Airbnb Ireland», *Journal of European Consumer and Market Law*, 4 (2018).
42 V. Hatzopoulos, «General Principles for the Collaborative Economy», in *General principles of EU law and the EU digital order*, a cura di U. Bernitz et al., Kluwer Law International B.V., Alphen aan den Rijn 2020, p. 135.
43 M. Inglese, «Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland», *Eurojus*, 1 (2020), p. 44.
44 Hatzopoulos, «General Principles for the Collaborative Economy» cit., p. 135.
45 Corte giust., sentenza del 19 dicembre 2019 (Grande Sezione), causa C-390/18, *Airbnb Ireland*, ECLI:EU:C:2019:1112.
46 Ivi, § 44-49; Busch, «The Sharing Economy at the CJEU» cit., p. 173.
47 Corte giust., causa C-390/18, *Airbnb Ireland* cit., § 53; Inglese, «Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland» cit., p. 46-47.

lizzazione di prestazioni di alloggio».[48] Ciò porta la Corte a concludere per il carattere *scindibile* dei due servizi,[49] cosicché a quello offerto da AirBnb si applichi il regime della direttiva 2000/31.

1.3 *Le principali definizioni del DSA*

Tornando alle tre categorie elencate dalla lettera g), (*i*) l'attività di *mere conduit* consiste nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso ad una rete di comunicazione (art. 3, par. 1, lett. g), punto i) e art. 4, par. 1, DSA);[50] (*ii*) l'attività di *caching* consiste nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio e comporta «la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta» (art. 3, par. 1, lett. g), punto ii) e art. 5, par. 1, DSA);[51] (*iii*) l'attività di *hosting* consiste, infine, nella memorizzazione non temporanea (altrimenti si rientrerebbe nel *caching*), e quindi durevole, di informazioni fornite da un destinatario del servizio (art. 3, par. 1, lett. g), punto iii) e art. 6, par. 1, DSA).[52] Ai fini del presente elaborato, non è necessario soffermarsi ulteriormente su tali categorie – che renderebbero possibili altre riflessioni – per il fatto che l'inquadramento in una fattispecie o nell'altra rileva solo dal punto di vista della esenzione dalla responsabilità dei fornitori,[53] aspetto che però esula dall'oggetto della tesi.

Più utile ai fini della successiva trattazione è invece la definizione di piattaforma, posto che alcune norme – quali, ad esempio, la sezione 3 del capo III, significativamente rubricata «Disposizioni aggiuntive applicabili ai fornitori di piattaforme online», nonché la sezione 4 del medesimo capo – si applicano solo a questa categoria. Tale definizione è rinvenibile all'articolo 3, paragrafo 1, lettera i), DSA, ove si afferma che essa è

> un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e 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.

48 Corte giust., causa C-390/18, *Airbnb Ireland*, cit., § 55.
49 Ivi, § 57.
50 Michinelli, «I servizi intermediari» cit., p. 57.
51 Ivi, p. 58.
52 Ivi, p. 59.
53 Ivi, p. 52.

Dunque, la piattaforma è un particolare tipo di servizio di *hosting* che presenta l'ulteriore caratteristica di *diffondere informazioni al pubblico*,[54] la quale – secondo la lettera k) del medesimo articolo – implica la messa a disposizione di informazioni, fornite dal destinatario del servizio e su richiesta di questo, a favore di un numero potenzialmente illimitato di terzi.[55] Ciò comporta che non siano da considerarsi piattaforme i servizi di comunicazione interpersonale, quali posta elettronica o messaggistica istantanea, perché in questo caso i destinatari sono specificamente individuati dal mittente.[56]

Nell'ambito di questa categoria, il regolamento dedica una grande attenzione ad un particolare tipo di piattaforme, quelle «di dimensioni molto grandi» (cd. «VLOP», *Very Large Online Platform*), le quali sono destinatarie di una serie di obblighi aggiuntivi, stabiliti dalla sezione 5 del capo III. I medesimi obblighi vengono imposti ai «motori di ricerca di dimensioni molto grandi» (cd. «VLOSE», *Very Large Online Search Engine*). La *ratio* di individuazione di obblighi aggiuntivi è da rinvenirsi nel considerando 75, il quale fa leva sul ruolo di facilitazione del dibattito pubblico e della diffusione di informazioni di queste piattaforme. Inoltre, il considerando 76 ricorda che

> [l]e piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi possono comportare *rischi per la società diversi in termini di portata ed effetti rispetto a quelli presentati dalle piattaforme più piccole*. [Essi] dovrebbero pertanto essere soggetti agli obblighi più stringenti in materia di dovere di diligenza, proporzionati al loro impatto per la società. Quando il numero di destinatari attivi di una piattaforma online o di destinatari attivi di un motore di ricerca online, calcolato come media in un periodo di sei mesi, raggiunge una quota significativa della popolazione dell'Unione, i rischi sistemici posti da tale piattaforma online o motore di ricerca *possono avere un effetto sproporzionato sull'Unione*. (corsivi aggiunti)

54 F. De Stefani, «Definizione di: "destinatario", "hosting", "piattaforma e "motori di ricerca"», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 121.

55 V. cons. 14: «Il concetto di "diffusione al pubblico" utilizzato nel presente regolamento dovrebbe implicare la messa a disposizione di informazioni a un numero potenzialmente illimitato di persone, ossia il fatto di rendere le informazioni facilmente accessibili ai destinatari del servizio in generale senza che sia necessario un ulteriore intervento da parte del destinatario del servizio che le ha fornite, indipendentemente dall'accesso effettivo alle informazioni in questione da parte di tali persone[…]».

56 V. cons. 14: «[…] I servizi di comunicazione interpersonale, quali definiti nella direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, come i messaggi di posta elettronica o i servizi di messaggistica privata, non rientrano nell'ambito di applicazione della definizione di piattaforma online poiché sono utilizzati per la comunicazione interpersonale tra un numero limitato di persone stabilito dal mittente della comunicazione. […]»; De Stefani, «Definizione di: "destinatario", "hosting", "piattaforma e "motori di ricerca"» cit., p. 122.

In base all'articolo 33, paragrafo 1, rientrano in questa categoria le piattaforme o motori di ricerca (d'ora in poi si utilizzerà il termine «piattaforme» per includere anche questi ultimi) che abbiano un numero medio mensile di destinatari attivi nell'UE pari o superiore a 45 milioni e che siano designati come tali ai sensi del paragrafo 4. Quindi, non è sufficiente semplicemente raggiungere tale numero di destinatari attivi[57], ma è necessario un intervento "costitutivo" della Commissione, ossia una decisione di quest'ultima che designi la piattaforma come VLOP. A tale proposito, il 25 Aprile 2023 la Commissione ha adottato le prime decisioni nei confronti di diciassette piattaforme, tra cui AliExpress, Amazon, Booking, Facebook, Instagram, LinkedIn, TikTok, Twitter, Zalando.[58] Tale decisione è stata impugnata dinnanzi al Tribunale dell'Unione europea dapprima da Zalando[59] e poi da Amazon.[60] I due ricorsi di annullamento sono attualmente pendenti;[61] vale però la pena analizzare quanto lamentato dalle società ricorrenti. Zalando *(i)* in primo luogo ritiene di non essere un *servizio intermediario*, in quanto metterebbe a disposizione contenuti *propri* e non *di terzi*. *(ii)* Inoltre, la ricorrente rileva che essa non raggiungerebbe il numero di 45 milioni di utenti. Ciò che è interessante è che *(iii)* in terzo luogo, la società si duole del fatto che l'articolo 33, paragrafo 1 e paragrafo 4, in combinato disposto con l'articolo 24, paragrafo 2, del DSA sarebbe viziato da indeterminatezza, in quanto non stabilirebbe i criteri per l'inclusione dell'utente nel calcolo con sufficiente precisione.[62] Come già detto, la causa non è ancora stata decisa e sono state emesse da parte del Tribunale solamente ordinanze.[63]

57 Numero che, peraltro, ai sensi del paragrafo 2 (e alle condizioni previsti dallo stesso) può essere modificato dalla Commissione, con atto delegato ai sensi dell'articolo 87 DSA, qualora la popolazione dell'UE aumenti o diminuisca di almeno il 5%.

58 A. Landi, «I fornitori di servizi di intermediazione molto grandi», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 68-69; L. Bertuzzi, «Commission announces first platforms to fall under EU digital rulebook's stricter regime», *Euractiv* (27 aprile 2023), (visitato il 17/02/2024); v. il comunicato stampa della Commissione del 25 aprile 2023 "Regolamento sui servizi digitali: designato dalla Commissione il primo gruppo di piattaforme e motori di ricerca online di dimensioni molto grandi", `https://ec.europa.eu/commission/presscorner/detail/it/ip_23_2413` (visitato il 17/02/2024).

59 M. Killeen, «Zalando files suit against Commission over very large platform designation», *Euractiv* (27 giugno 2023), (visitato il 17/02/2024).

60 J. Tar, «Amazon joins Zalando in challenging very large online platform designation», *Euractiv* (12 luglio 2023), (visitato il 17/02/2024).

61 Trib. UE, causa T-348/23, *Zalando c. Commissione*, pendente; Trib. UE, causa T-367/23, *Amazon Services Europe c. Commissione*, pendente

62 Causa T-348/23, *Zalando c. Commissione*, ricorso proposto il 27 giugno 2023, GU C 314, 04/09/2023, pp. 9–11

63 Trib. UE, ordinanza del 16 ottobre 2023, causa T-348/23, *Zalando c. Commissione*, annullata da

I motivi di doglianza di Amazon paiono più stringati e si rifanno al fatto che la decisione della Commissione si baserebbe su un «criterio discriminatorio e violerebbe in modo sproporzionato il principio della parità di trattamento e i diritti fondamentali della ricorrente».[64] Anche in questo caso, il procedimento principale è ancora pendente e il Tribunale si è pronunciato solo con riferimento all'istanza cautelare.[65]

1.4 *L'ambito di applicazione territoriale*

Analizzato l'ambito di applicazione materiale, è opportuno soffermarsi anche su quello territoriale. Infatti, Internet – per la sua natura intrinsecamente transfrontaliera (o a-territoriale) – ha posto dei problemi dapprima sconosciuti circa l'applicazione territoriale del diritto dell'Unione. In particolare, è intenzione del legislatore ampliare tale ambito, onde evitare che alcuni fornitori del servizio, non stabiliti nell'Unione ma che erogano servizi a destinatari che si trovano nel territorio dell'UE, si rifugino dietro tale condizione al fine di affermare la non applicabilità nei loro confronti del regolamento. L'articolo 2, paragrafo 1, del DSA, significativamente statuisce:

> [i]l presente 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.

La norma, dunque, pone come criterio di collegamento non già il luogo di stabilimento del fornitore del servizio intermediario, ma quello del destinatario dello stesso («collegamento sostanziale con l'Unione», v. cons. 7). Si tratta di un criterio già utilizzato dal GDPR (art. 3):[66] in sede di redazione di quest'ultimo si era tenuto conto delle problematiche applicative insorte con riferimento alla direttiva 95/46/CE e dei principi stabiliti dalla giurisprudenza nell'interpretare l'articolo 4 di quest'ultima. Ad esempio, in *Google Spain*, la Corte ha attratto all'interno

Corte giust., ordinanza dell'11 gennaio 2024, causa C-647/23 P(I), *European Information Society Institute o.z. (EISi) c. Commissione europea*, ECLI:EU:C:2024:37

64 Causa T-367/23, *Amazon Services Europe c. Commissione*, ricorso proposto il 5 luglio 2023, GU C 296, 21/08/2023, pp. 41-42

65 Trib. UE, ordinanza del 27 settembre 2023, causa T-367/23R, *Amazon Services Europe c. Commissione*, ECLI:EU:T:2023:589, parzialmente annullata da Corte giust., ordinanza del 27 marzo 2024, causa C-639/23 P(R), *Commissione c. Amazon Services Europe*, ECLI:EU:C:2024:277

66 L. Bolognini, «Oggetto, obiettivi e ambito di applicazione del *Digital Services Act*», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 39; L. Lemoine e M. Vermuelen, «The extraterritorial implications of the Digital Services Act», *DSA Observatory* (1 novembre 2023), (visitato il 18/02/2024).

del campo applicativo della legge spagnola sulla protezione dei dati l'attività di gestione del motore di ricerca di *Google Inc.*, società statunitense, in quanto «inscindibilmente connesse» con quelle della vendita degli spazi pubblicitari ad opera di *Google Spain*.[67] Infatti, osserva la Corte che «non si può accettare che il trattamento di dati personali effettuato per le esigenze del funzionamento del suddetto motore di ricerca venga sottratto agli obblighi e alle garanzie previsti dalla direttiva 95/46, ciò che *pregiudicherebbe l'effetto utile di quest'ultima e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche che detta direttiva mira a garantire*».[68] Si deve ritenere che una simile *ratio*, ossia di «garantire un elevato grado di tutela delle libertà e dei diritti fondamentali delle persone fisiche»[69] dei cittadini dell'Unione (o, *rectius*, di soggetti che sono in ogni caso ubicati nell'Unione dalla loro cittadinanza), indipendentemente dal luogo di stabilimento del fornitore, abbia ispirato anche il testo dell'articolo 2 DSA.

1.5 *L'intersezione tra DSA e GDPR: linee generali*

L'analisi dei punti di intersezione tra i due regolamenti oggetto del presente elaborato è utile non solo in quanto tale, ma anche perché è funzionale alla comprensione di come i meccanismi di *enforcement* dei due strumenti normativi possano tra di loro incontrarsi (oppure, scontrarsi). Si vedrà infatti successivamente (v. *infra* cap. 3) che vi sono già stati dei casi in cui una medesima fattispecie concreta (attinente all'ambito digitale) è stata fronteggiata, in quanto patologica, attraverso diverse discipline (segnatamente, il GDPR e il diritto della concorrenza), rendendo necessario un coordinamento sia sostanziale che procedurale tra le stesse. Questo paragrafo si occuperà di analizzare alcuni aspetti sostanziali dell'intersezione tra GDPR e DSA, mentre quelli procedurali/applicativi saranno esaminati nel capitolo 3.

Innanzitutto, bisogna ricordare che la nozione di «trattamento» di dati personali data dall'articolo 4, paragrafo 1, numero 2 del GDPR è molto ampia, includendo «qualsiasi operazione o insieme di operazioni, […] applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, […] la comunicazione mediante trasmissione,

67 Corte giust., sentenza del 13 maggio 2014 (Grande Sezione), causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, ECLI:EU:C:2014:317, § 54-55.

68 Ivi, § 58, corsivo aggiunto.

69 Corte giust., sentenza del 5 giugno 2018 (Grande Sezione), causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, § 26.

diffusione o qualsiasi altra forma di messa a disposizione […]»: è evidente che in essa rientrano la gran parte delle attività svolte dai prestatori di servizi intermediari,[70] i quali molto spesso basano il loro *core business* proprio nella raccolta di dati personali per poi diffonderli presso gli altri utenti della piattaforma oppure per fornire dei contenuti personalizzati. Pertanto, le medesime attività rientreranno sia nel campo applicativo del DSA, sia in quello del GDPR.[71]

Con riferimento al rapporto tra le due fonti, importante è l'articolo 2, paragrafo 4, lettera g), ove si afferma che il DSA non pregiudica il diritto dell'Unione in materia di protezione dei dati personali e in particolare il GDPR e la direttiva e-privacy. Inoltre, il considerando 10 precisa che «la protezione delle persone fisiche con riguardo al trattamento dei dati personali è disciplinata unicamente dalle norme del diritto dell'Unione in materia, in particolare dal regolamento (UE) 2016/679 e dalla direttiva 2002/58/CE». La dottrina ha dunque affermato la natura di *lex specialis* del GDPR e della direttiva e-privacy rispetto al DSA.[72] Chiara è dunque la volontà del legislatore di stabilire la primazia di questi ultimi strumenti sul DSA quando si adotti il punto di vista della protezione dei dati personali.

Si tratta di un'impostazione condivisa anche dalla Corte di giustizia con riferimento al rapporto tra la direttiva e-commerce e la direttiva 95/46/CE: ad esempio, in *Promusicae*, i giudici di Lussemburgo hanno ricordato che la tutela della proprietà intellettuale predisposta dalla direttiva e-commerce non può pregiudicare gli obblighi relativi alla tutela dei dati personali;[73] inoltre, in *La Quadrature du Net*, la Corte ha osservato che, essendo la direttiva 95/46/CE stata sostituita dal GDPR, il ragionamento effettuato nel caso precedente deve essere applicato al Regolamento generale sulla protezione dei dati.[74]

Sul tema dell'esenzione dalla responsabilità, il Garante europeo della protezione dei dati, nella sua Opinione resa ai sensi dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725,[75] avrebbe auspicato una precisazione circa il rap-

70 E. Pelino, «L'interazione tra DSA e GDPR», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 9.

71 Più correttamente, come segnalato da (ivi, p. 9-10), il GDPR si applica solo agli interessati che sono persone fisiche, mentre il DSA include all'interno della definzione di «destinatario» ex articolo 3, paragrafo 1, lettera b) anche le persone giuridiche.

72 Ivi, p. 9.

73 Corte giust., sentenza del 29 gennaio 2008 (Grande Sezione), causa C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, ECLI:EU:C:2008:54, § 57

74 Corte giust., sentenza del 6 ottobre 2020 (Grande Sezione), cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a. c. Premier ministre e a.*, ECLI:EU:C:2020:791, § 199-200

75 Garante europeo della protezione dei dati, *Opinion 1/2021 on the Proposal for a Digital Services Act*, 10 febbraio 2021, punto 20.

porto tra DSA e GDPR, nel senso di affermare esplicitamente che l'esenzione da responsabilità stabilita dal DSA non può in alcun modo intaccare la responsabilità da illecito trattamento di dati stabilita dall'articolo 82 GDPR.

1.6 *Il divieto di pubblicità "mirata" basata sull'utilizzo di dati sensibili*

Posti questi principi generali, la prima disposizione che è interessante analizzare è l'articolo 26, paragrafo 3, DSA: essa stabilisce un divieto di presentare pubblicità ai destinatari basate sulla profilazione (così come definita dall'art. 4, punto 4, GDPR) utilizzando i cd. «dati sensibili» (ossia le «particolari categorie di dati» previste dall'art. 9, par. 1, GDPR). La norma è rilevante in quanto va ad innalzare lo standard di tutela di tali dati.[76]

La portata della norma è particolarmente ampia anche in ragione di un orientamento della Corte di giustizia, che ha adottato un'interpretazione estensiva del concetto di «categorie particolari di dati personali»: in *Vyriausioji tarnybinės etikos komisija* la Corte ha precisato che costituisce trattamento di categorie particolari di dati personali anche il trattamento di dati di per sé non "sensibili", ma idonei – attraverso «un'operazione intellettuale di deduzione o di raffronto»[77] – a svelare indirettamente informazioni di tale natura. Osserva infatti la Corte che adottare l'interpretazione contraria significherebbe, di fatto, contrastare con la finalità della norma di garantire una protezione maggiore contro tali trattamenti e «pregiudicare l'effetto utile di tale regime e la tutela dei diritti e delle libertà fondamentali delle persone fisiche che esso mira ad assicurare».[78] Inoltre, la giurisprudenza ha anche precisato che tale interpretazione si applica anche ai trattamenti effettuati da un social network consistenti «nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati»,[79] escludendo peraltro che si possa rientrare all'interno della deroga del dato reso manifestamente pubblico dall'interessato (prevista dall'articolo 9, paragrafo 2, lettera e, GDPR) per il semplice fatto che l'interessato abbia cliccato il pulsante «Mi piace» o «Condividi».[80]

76 Pelino, «L'interazione tra DSA e GDPR» cit., p. 12.

77 Corte giust., sentenza del 1° agosto 2022 (Grande Sezione), causa C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, § 123.

78 Ivi, § 126-127.

79 Corte giust., sentenza del 4 luglio 2023 (Grande Sezione), C-252/21, *Meta Platforms Inc. e a. c. Bundeskartellamt*, ECLI:EU:C:2023:537, § 73.

80 Ivi, § 74-85.

Combinare l'articolo 9 GDPR così interpretato con l'articolo 26, paragrafo 3, del DSA significa, di fatto, vietare che qualsiasi dato personale che anche indirettamente possa condurre a svelare informazioni "sensibili" possa essere utilizzato per la presentazione di pubblicità basata sulla profilazione. Peraltro, tale divieto varrebbe anche se per tali particolari categorie di dati fosse stato prestato il consenso esplicito ex articolo 9, paragrafo 1, lettera b) del GDPR.[81] Si tratta di una affermazione non priva di conseguenze applicative, in quanto potrebbe non essere facile per i prestatori del servizio/titolari del trattamento individuare quali siano effettivamente questi dati: infatti, un medesimo dato personale (ad es. il visualizzare un determinato contenuto, il condividerlo con altri utenti, il mettere «Mi piace») preso *a sé stante* potrebbe non essere indicatore di alcun dato sensibile, al contrario di quando viene *combinato* con altri. Inoltre, la situazione è resa più complessa dal fatto che l'individuazione inferenziale del dato sensibile è effettuata molto spesso ad opera di algoritmi di intelligenza artificiale, a partire da un ampio *set* di dati.

Sul punto, l'articolo 28, paragrafo 2, DSA afferma un ulteriore divieto di presentazione di pubblicità basata sulla profilazione qualora il fornitore di piattaforma online sia consapevole, con ragionevole certezza, che il destinatario del servizio sia un minore. Pertanto, in relazione a questa categoria, la pubblicità "mirata" (cioè basata sulla profilazione) appare vietata *tout court*, ossia in relazione ad un *qualsiasi* dato personale e *non solo alle particolari categorie di dati* ex articolo 9 GDPR.

Infine, l'articolo 38 DSA stabilisce un'ulteriore restrizione con riferimento alle VLOP: qualora esse utilizzino sistemi di raccomandazione, devono fornire ai destinatari almeno un'opzione, per ciascuno di questi sistemi, che non sia basata sulla profilazione. Si tratta di una norma apprezzabile, in quanto permette al destinatario del servizio – che abbia precedentemente prestato il consenso a che siano trattati i propri dati personali anche per mezzo della profilazione – di evitare le conseguenze di tale scelta, optando per un sistema di raccomandazione che non sia "mirato" al profilo tracciato dalla piattaforma. La valenza della norma è, forse, confermata dal fatto che nel caso *Amazon Services Europe* citato, la ricorrente ha richiesto in via subordinata di annullare la decisione della Commissione che la riguarda, nella misura in cui le impone di rispettare l'articolo 38 DSA, in quanto esso violerebbe il principio della parità di trattamento.[82] Inoltre, nella richiesta di misure cautelari, la ricorrente ha rilevato come questo obbligo altererebbe uno degli elementi fondamentali del *software* alla base del suo modello di impresa,

81 Pelino, «L'interazione tra DSA e GDPR» cit., p. 12.
82 Ricorso proposto il 5 luglio 2023, *Amazon Services Europe c. Commissione* cit., pp. 41-42.

creando anche danni ai consumatori.[83] In attesa della decisione di merito, vale la pena rilevare che il Tribunale ha rigettato quest'ultima argomentazione – quantomeno ai fini della valutazione del *periculum* – osservando che l'articolo 38 non pone un divieto *tout court* di utilizzo di sistemi di raccomandazione basati sulla profilazione, ma semplicemente l'obbligo di fornire tale possibilità, cosicché il destinatario che lo vorrà sarà sempre libero di non optare e continuare a ricevere i suggerimenti "personalizzati".[84]

1.7 *Il sistema di gestione dei reclami e le decisioni automatizzate*

L'articolo 20 DSA impone ai fornitori di piattaforme online di mettere a disposizione dei destinatari del servizio un sistema interno di gestione dei reclami che permetta loro di contestare talune decisioni adottate dal fornitore, e segnatamente: (*i*) le decisioni che indicano se rimuovere le informazioni o disabilitare l'accesso alle stesse o se limitarne la visibilità; (*ii*) le decisioni che indicano se sospendere o cessare in tutto o in parte la prestazione del servizio ai destinatari; (*iii*) le decisioni che indicano se sospendere o cessare l'account dei destinatari; (*iv*) le decisioni che indicano se sospendere, cessare o limitare in altro modo la capacità di monetizzare le informazioni fornite dai destinatari.

Non essendo in questa sede possibile analizzare tutte le implicazioni che la norma pone, appare opportuno concentrarsi sul paragrafo 6, poiché esso si ricollega ad alcune norme previste dal Regolamento generale sulla protezione dei dati. Tale paragrafo prevede che le decisioni sui reclami siano prese «con la supervisione di personale adeguatamente qualificato e non avvalendosi *esclusivamente* di strumenti automatizzati». La norma pone dunque il divieto, per il fornitore, di analizzare e decidere il reclamo facendo uso di sistemi completamente automatizzati. Si tratta di una previsione che riecheggia quella dell'articolo 22 GDPR, il quale vieta[85]

83 Trib. UE, causa T-367/23R, *Amazon Services Europe c. Commissione* cit., § 28-30.

84 Ivi, § 35-37.

85 In dottrina si discute molto sulla portata del paragrafo 1 dell'articolo 22 GDPR: secondo alcuni esso stabilisce un *divieto* in capo al titolare, secondo altri un *diritto* dell'interessato, v. L. A. Bygrave, «Article 22 Automated individual decision-making, including profiling», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 530-532. A favore della prima tesi, in dottrina v. Sarra, *Il mondo-dato* cit., p. 146; M. Brkan, «Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond», *International Journal of Law and Information Technology*, 27, 2 (2019), p. 99; I. Mendoza e L. A. Bygrave, «The Right Not to be Subject to Automated Decisions Based on Profiling», in *EU Internet Law: Regulation and Enforcement*, a cura di T.-E. Synodinou et al., Springer International Publishing, Cham 2017, p. 85-87; in giurisprudenza v. Rechtbank Den Haag, sentenza del 5 febbraio 2020, ECLI:NL:RBDHA:2020:865, par. 6.35, secondo cui «*op grond van*

di sottoporre l'interessato ad una «decisione basata unicamente sul trattamento automatizzato», qualora tale decisione produca nei suoi confronti effetti giuridici o comunque incida in modo significativamente analogo sulla sua persona. Si è pertanto osservato come il DSA non farebbe altro che ripetere una norma già presente nel GDPR, sottolineando che però l'elemento di novità pare essere il fatto che il DSA escluda in ogni caso l'operare delle eccezioni stabilite dall'articolo 22, paragrafo 2 del GDPR.[86]

Bisogna anche evidenziare come il legislatore, redigendo la norma del DSA in esame, sia ricaduto nella medesima vaghezza di formulazione già sperimentata con riferimento all'articolo 22 GDPR. Infatti, l'articolo 26 non afferma un divieto *tout court* di utilizzare strumenti automatizzati, ma, più indulgentemente, di impiegare *esclusivamente* tali strumenti. Non si tratta di un'annotazione da poco, perché l'assenza del requisito dell'esclusività comporta che l'utilizzo degli strumenti automatizzati sia consentito. Questa scelta del legislatore riapre il medesimo dibattito che si è sviluppato circa l'utilizzo del termine «*unicamente*» da parte dell'articolo 22, paragrafo 1, GDPR:[87] in particolare, si discute di quale sia il necessario grado di "incisività" dell'intervento umano affinché il requisito dell'unicità non sia soddisfatto e, quindi, non si rientri nell'ambito applicativo della norma di cui all'articolo 22. Senza soffermarsi distesamente sulle varie tesi proposte, si può ricordare che (*i*) è generalmente condiviso il concetto per cui sia necessaria una reale influenza dell'uomo sul processo decisionale: ad esempio, è necessario che la persona preposta valuti *attivamente* il responso dato dal sistema automatico.[88] Inoltre, secondo le linee guida del Gruppo di lavoro articolo 29,[89]

artikel 22 AVG geldt een algemeen verbod op volledig geautomatiseerde individuele besluitvorming». In senso contrario v. L. Tosoni, «The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation», *International Data Privacy Law*, 11, 2 (2021), p. 161-162.

86 Pelino, «L'interazione tra DSA e GDPR» cit., p. 13.

87 Con riferimento a questa discussione, si v. le varie posizioni dottrinali esposte da S. Wachter et al., «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», *International Data Privacy Law*, 7, 2 (2017), p. 91-92; in dottrina v. anche Sarra, *Il mondo-dato* cit., p. 144; Bygrave, «Article 22» cit., p. 531-534; G. Malgieri e G. Comandé, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *International Data Privacy Law*, 7, 4 (2017), p. 247; M. Hildebrandt, «The Dawn of a Critical Transparency Right for the Profiling Era», in *Digital Enlightenment Yearbook 2012*, a cura di J. Bus et al., IOS Press, Amsterdam 2012, p. 51; L. A. Bygrave, «Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», *Computer Law & Security Review*, 17, 1 (2001), p. 19.

88 Bygrave, «Article 22» cit., p. 532.

89 Gruppo di lavoro articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017,

il titolare del trattamento *(ii)* «non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi»; *(iii)* deve garantire che il controllo sia *significativo* e non costituisca un gesto simbolico e che *(iv)* sia effettuato da un individuo che ha l'autorità (e la competenza) di modificare la decisione. Peraltro, quest'ultimo principio è positivamente espresso dal paragrafo 6 dell'articolo 26 DSA. Più in generale, si ritiene che quanto appena esposto debba valere anche in relazione alla risoluzione dei reclami disciplinata dal DSA, visto che le due norme presentano una formulazione molto simile e ne condividono lo spirito.

1.8 *I dark pattern*

L'ultima norma che appare opportuno prendere in esame è l'articolo 25 DSA, il quale è rubricato «Progettazione e organizzazione delle interfacce online». Il paragrafo 1 pone il divieto per i fornitori di piattaforme online di progettare, organizzare o gestire le loro interfacce online in modo tale da ingannare o manipolare i destinatari del servizio o comunque da materialmente falsare o compromettere in altri modi la loro capacità di prendere decisioni libere ed informate. Il paragrafo 2 stabilisce la non applicabilità della norma del paragrafo precedente alle pratiche contemplate dalla direttiva sulle pratiche commerciali sleali,[90] nonché del Regolamento generale sulla protezione dei dati.

L'articolo è dedicato ai cd. «*dark pattern*» o «*deceptive design pattern*». Essi sono definiti dalle linee guida dell'EPDB[91] come interfacce implementate in piattaforme online che tentano di influenzare gli utenti al fine di far loro prendere decisioni non volute o potenzialmente dannose e che molto spesso vanno contro il miglior interesse dell'utente (favorendo invece la piattaforma), con riferimento al trattamento dei dati. Essi consistono, secondo tali linee guida, tra gli altri, nell'inondare l'utente di informazioni e richieste; nell'influenzare le scelte dell'utente facendo appello alle sue emozioni o usando sollecitazioni visive (ad es., inserendo dei

versione emendata e adottata in data 6 febbraio 2018 (wp251rev.01), disponibili al link `https://ec.europa.eu/newsroom/article29/items/612053/en`, p. 23

90 Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e 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, GU L 149, 11/06/2005, pp. 22–39.

91 Comitato europeo per la protezione dei dati, *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, versione 2.0, adottate in data 14 febbraio 2023, disponibili al seguente link: `https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf`, punto 3.

pulsanti di grandezza diversa); nell'ostacolare l'utente nella gestione dei propri dati. Tali esemplificazioni sono presenti, in maniera pressoché analoga, anche in un elenco di «pratiche specifiche» contenuto nel paragrafo 3 dell'articolo 26 DSA: (*i*) «attribuire maggiore rilevanza visiva ad alcune scelte quando si richiede al destinatario del servizio di prendere una decisione»; (*ii*) «chiedere ripetutamente che un destinatario del servizio effettui una scelta laddove tale scelta sia già stata fatta, specialmente presentando pop-up che interferiscano con l'esperienza dell'utente»; (*iii*) «rendere la procedura di disdetta di un servizio più difficile della sottoscrizione dello stesso».

Dal punto di vista del diritto della protezione dei dati, si ritiene che i *dark pattern* violino alcune norme del GDPR, in particolare: il principio di correttezza del trattamento (art. 5, par. 1, lett. a GDPR),[92] il principio di *privacy by design* di cui all'articolo 25 GDPR.[93] Inoltre, ai sensi dell'articolo 4, paragrafo 1, numero 11, GDPR, qualora la base giuridica per il trattamento sia il consenso, esso deve essere una «manifestazione di volontà libera, specifica, informata e inequivocabile»: è evidente che un consenso "estorto" tramite le pratiche in esame difetti di tali requisiti, e dunque, non costituendo una base giuridica idonea, rende il trattamento illegittimo.

Si comprende, quindi, come molte delle pratiche di *dark pattern* siano sussumibili in una fattispecie vietata dal GDPR: ciò comporta che tale fattispecie si ponga fuori dall'ambito applicativo dell'articolo 25 DSA, ai sensi del paragrafo 2 della medesima norma. Dunque, vi sarebbe forse da ridimensionare parzialmente la portata innovativa della previsione: tornando ad un esempio di pratica specifica prevista dal paragrafo 3, quella di «attribuire maggiore rilevanza visiva ad alcune scelte quando si richiede al destinatario del servizio di prendere una decisione» esulerà dall'ambito applicativo dell'articolo 25 DSA qualora la scelta consista nel dare il consenso al trattamento di alcuni dati (molto frequente, ad es., la prassi di indurre gli interessati ad accettare il trattamento dei cookie evidenziando il pulsante «consenti»).[94] Tuttavia, la norma non è priva di una qualsiasi conseguenza applicativa, in quanto non necessariamente tali pratiche comportano la violazione di norme del GDPR o della disciplina consumeristica,[95] cosicché, almeno astrattamente, appare possibile individuare un autonomo spazio residuo di applicazione della norma. Inoltre, al paragrafo 3 il legislatore indica tre condotte che costituiscono *dark pattern* ai sensi del DSA: la novità è che in

92 Ivi, punto 9.

93 Ivi, punto 18.

94 G. Spindler e L. Förster, «Privacy-compliant design of Cookie Banners according to the GDPR», *JIPITEC*, 14, 1 (2023), p. 26.

95 Comitato europeo per la protezione dei dati, *Guidelines 03/2022*, cit., punto 4.

questo caso l'individuazione è effettuata da una fonte regolamentare, e non, come in precedenza, da semplici linee guida.

D'altra parte, come ricordato anche dal Comitato, è necessario fare attenzione alla possibilità che le varie discipline si sovrappongano:[96] ciò è da tenere a mente in vista di quanto si affermerà nel capitolo 3 circa la cooperazione tra le varie autorità.

96 Ibidem.

2

L'ATTUAZIONE TRANSFRONTALIERA DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

2.1 *Introduzione*

Il presente lavoro, una volta presentate le principali caratteristiche del *Digital Services Act* nel primo capitolo, si propone di esaminare – a cinque anni dalla sua entrata in vigore – lo stato dell'*enforcement* del Regolamento generale sulla protezione dei dati, verificando quali siano i problemi che l'attuazione transnazionale di questo regolamento comporta e quali siano le strategie individuate dai vari attori in gioco – autorità di controllo nazionali, Comitato europeo per la protezione dei dati, giudici nazionali, Corte di Giustizia, Commissione – per assicurarne l'applicazione.

Con riferimento alla dimensione transfrontaliera del trattamento dei dati, l'obiettivo primario che il legislatore dell'Unione si è posto con l'approvazione del GDPR pare essere quello di garantire un livello uniforme di tutela dei diritti in tutta l'Unione. Tale scopo emerge anche dal Considerando 10 del Regolamento, il quale recita:

> [a]l fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. […]

L'importanza di un livello uniforme di tutela del diritto alla protezione dei dati emerge anche dalla giurisprudenza della Corte, la quale ha più volte richiamato proprio il considerando 10. Ad esempio, in *Latvijas Republikas Saeima (Punti di penalità)*, i giudici di Lussemburgo hanno evidenziato che:

> [d]al considerando 10 del RGPD emerge […] che quest'ultimo mira a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia garantendo un livello coerente ed elevato di protezione delle persone fisiche con riguardo al trattamento dei dati personali,

> il che presuppone che tale livello di protezione sia equivalente ed omogeneo in tutti gli Stati membri.[1]

La precedente direttiva 95/46/CE si era presentata come strumento inadeguato a garantire tale uniformità, a causa della sua natura non regolamentare, e quindi della sua non diretta applicabilità nei confronti degli individui. Conseguentemente, gli Stati membri avevano adottato delle legislazioni tra loro divergenti.[2] De Hert e Papakonstantinou sottolineano come la natura regolamentare del GDPR sia, di per sé, una rivoluzione, affermando che «*perhaps the most important contribution to EU personal data processing by the Regulation is the choice of instrument itself*»,[3] cosicché, almeno in linea teorica, l'abbandono della direttiva dovrebbe essere di per sé sufficiente per evitare che si generino i problemi di armonizzazione del passato.[4]

Come si vedrà, quanto appena affermato non rimane scalfito nella teoria, ma nella pratica si è dovuto scontrare con i problemi che verranno di seguito illustrati, i quali *(i)* non hanno permesso di raggiungere un livello effettivamente uniforme di tutela dei diritti sanciti dal regolamento, cosicché esso non è il medesimo in tutta l'Unione. Anzi, *(ii)* l'utilizzo del meccanismo di coerenza – pur effettivamente garantendo una maggiore uniformità tra le decisioni – ha rallentato l'*enforcement* del regolamento in caso di violazioni transnazionali, cosicché ci si chiede se esso, in realtà, non comporti nel concreto una tutela inferiore dei diritti.[5] Inoltre, questo strumento sembra aver inciso (negativamente) su altri diritti sanciti dalla Carta, come ad esempio il diritto ad una buona amministrazione e il diritto ad un rimedio giurisdizionale effettivo.

Il capitolo, come già anticipato, si concentrerà sulla dimensione transnazionale e sui problemi che essa pone. Tuttavia, il paragrafo 2.8 analizzerà alcuni aspetti dell'enforcement non transfrontaliero, cioè riferito a questioni meramente

1 Corte giust., sentenza del 22 giugno 2021 (Grande Sezione), causa C-439/19, *B c. Latvijas Republikas Saeima*, ECLI:EU:C:2021:504, § 83; v. anche Corte giust., sentenza del 28 aprile 2022, causa C-319/20, *Meta Platforms Ireland Limited c. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2022:322, § 52; Corte giust., sentenza del 15 giugno 2021 (Grande Sezione), causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:483, § 64 segnalate da L. Scaffidi Runchella, «Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero», *Cuadernos de derecho transnacional*, 15, 2 (2023), p. 901.

2 Ivi, p. 900-901.

3 P. de Hert e V. Papakonstantinou, «The new General Data Protection Regulation: Still a sound system for the protection of individuals?», *Computer Law & Security Review*, 32, 2 (2016), p. 182.

4 Ibidem.

5 H. C. Hofmann e L. Mustert, «Data protection», in *Research Handbook on the Enforcement of EU Law*, a cura di M. Scholten, Edward Elgar, Cheltenham 2023, p. 465.

"nazionali" che non comportano un «trattamento transfrontaliero» (v. *infra* par. 2.2). Infatti, anche tale analisi mostra come situazioni analoghe vengano trattate diversamente a seconda delle norme e delle prassi applicative dei vari Stati membri.

Infine, si tenterà di comprendere quali soluzioni siano state proposte in relazione ai problemi sinora presentati. In particolare, nel paragrafo 2.9 si comprenderà quale ruolo possa avere la Commissione europea, mentre nel paragrafo 2.10 si darà conto di una recente proposta di regolamento volto ad armonizzare talune norme procedurali relative alla gestione dei procedimenti transfrontalieri.[6]

2.2 *I meccanismi di «sportello unico» e di coerenza*

Al fine di proteggere i diritti dell'interessato e porre rimedio alle violazioni, il Regolamento generale sulla protezione dei dati conferisce all'interessato vari strumenti rimediali. In particolare, taluni rimedi sono concepiti sotto forma di diritti che l'interessato può vantare nei confronti del titolare o del responsabile del trattamento. Tra questi, si segnala il diritto di accesso (art. 15), il diritto di rettifica (art. 16), il diritto alla cancellazione (c.d. «diritto all'oblio») (art. 17), il diritto di opposizione (art. 21). Tuttavia, ci si concentrerà qui, più che altro, sull'altro ordine di rimedi, ossia strumenti con i quali l'interessato può reagire ad una (ritenuta) violazione non rivolgendosi al titolare del trattamento, ma ad un'autorità pubblica. In particolare, fermo restando il diritto di lamentare tale violazione davanti all'autorità giudiziaria (art. 79), l'articolo 77 prevede il *diritto* dell'interessato di presentare un reclamo all'autorità di controllo, qualora «ritenga che il trattamento che lo riguarda violi [il GDPR]».

Come già menzionato, il capitolo si occuperà, principalmente, non di tutti questi reclami, ma di quelli aventi una dimensione transfrontaliera. L'articolo 4, numero 23 del GDPR definisce il trattamento transfrontaliero, alla lettera a), come quel trattamento «che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro» oppure, alla lettera b), come quel «trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che

6 Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679 (COM(2023) 348 final), d'ora in poi "Proposta di regolamento di armonizzazione procedurale".

incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro».[7]

Per i casi di trattamento transfrontaliero, il Regolamento individua un meccanismo particolare, definito «di sportello unico» (o con il termine inglese *one-stop-shop*), in base al quale l'autorità di controllo dove il titolare del trattamento o il responsabile del trattamento[8] ha lo stabilimento principale (o l'unico stabilimento) è individuata come autorità di controllo «capofila» ed è, in linea di principio, l'unica autorità competente circa tale trattamento transfrontaliero (articolo 56, paragrafo 1, GDPR). Il paragrafo 6 dell'articolo 56 GDPR precisa, inoltre, che tale autorità deve essere l'*unico* interlocutore del titolare o del responsabile del trattamento. A questo riguardo, la dottrina tiene a sottolineare che, tuttavia, quest'ultima previsione non deve intendersi come completamente preclusiva della possibilità per l'autorità che ha informato la capofila di prendere contatti con il titolare.[9] Infatti, si osserva che, in caso contrario, sarebbe impossibile per la prima redigere il progetto di decisione di cui al paragrafo 4.[10]

Quindi, il meccanismo di sportello unico prevede che, qualora un interessato presenti un reclamo nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione (art. 77, par. 1, GDPR), ma tale Stato membro non sia quello ove il titolare ha il suo stabilimento principale, l'autorità cui è stato presentato il reclamo trasmetterà lo stesso all'autorità capofila. Ciò a meno che non si rientri nell'eccezione prevista dal paragrafo 2 dell'articolo 56, ossia che «l'oggetto riguard[i] unicamente uno stabilimento nel suo Stato membro o incid[a] in modo sostanziale sugli interessati unicamente nel suo Stato membro». In quest'ultimo caso, l'autorità che riceve il reclamo è tenuta, ai sensi del paragrafo 3, ad informare l'autorità capofila, la quale ha tre settimane di tempo per decidere se "trattenere" il caso o meno. Qualora decida in senso positivo, si applica la procedura di cui all'articolo 60 (v. *infra*) e l'altra autorità ha diritto di presentare una bozza di decisione.

La *ratio* di un simile meccanismo è da rinvenirsi nella volontà di far sì che il titolare del trattamento sia sottoposto alla vigilanza di, tendenzialmente, una sola autorità di controllo, senza dover interloquire con gli altri Stati membri.[11]

7 Per una trattazione più estesa sulla portata di questa definizione si rimanda a L. Tosoni, «Article 4(23) Cross-border processing», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020.

8 D'ora in poi, per esigenze di leggibilità, ci si riferirà al solo titolare del trattamento.

9 H. Hijmans, «Article 56 Competence of the lead supervisory authority», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 923.

10 Ivi, p. 924.

11 Ivi, p. 915.

In effetti, il regime predisposto dalla previgente direttiva aveva creato non pochi problemi per i titolari, che dovevano obbedire non solo a diverse *autorità di controllo*, ma anche ad una differente disciplina *sostanzale*.[12] Come anticipato nel capitolo introduttivo, sembra possibile affermare che questo sistema sia derivante da quanto, nell'ambito del mercato interno, si è sviluppato sotto il nome di «principio del paese d'origine» o «principio di mutuo riconoscimento»,[13] visto che l'idea alla base pare essere la stessa: la regolazione di una certa attività – nel caso del GDPR, ovviamente, non dal punto di vista del diritto positivo (essendovi già un regolamento), ma di intervento delle autorità di controllo – deve essere effettuata solo dal paese di stabilimento principale, e gli altri Stati membri non possono opporre proprie iniziative più stringenti.

L'autorità capofila non è, però, libera di determinare in maniera completamente autonoma il contenuto della propria decisione che definisce il reclamo o comunque decide sulla possibile violazione. Infatti, è necessario rispettare le norme previste dal capo VII, rubricato «Cooperazione e coerenza». Quest'ultimo si apre con l'articolo 60, il quale pone, innanzitutto, un dovere di cooperazione tra l'autorità capofila e le altre autorità di controllo interessate al fine di *(i)* raggiungere un consenso tra di loro e *(ii)* scambiarsi tutte le informazioni utili. Tuttavia, la dottrina nota come specifici doveri di cooperazione siano disciplinati agli articoli successivi, in particolare all'articolo 61 (assistenza reciproca)[14] e 62 (operazioni congiunte),[15] mentre l'articolo 60 sia dedicato alla procedura di co-decisione da seguire quando si applica il meccanismo di sportello unico.[16]

Tale procedura di co-decisione coinvolge, chiaramente, l'autorità capofila, nonché le altre «autorità di controllo interessate». Queste ultime vengono definite dall'articolo 4, numero 22, GDPR come quelle autorità che sono interessate da un certo trattamento dei dati in quanto *(i)* il titolare ha uno stabilimento presso tale Stato membro; *(ii)* « gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento»; *(iii)* hanno ricevuto un reclamo.[17] Pertanto, se un'autorità di controllo

12 Tosoni, «Article 4(23)» cit., p. 280.

13 Hijmans, «Article 56» cit., p. 917.

14 Si v. P. Blume, «Article 61 Mutual assistance», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020.

15 Si v. P. Blume, «Article 62 Joint operations of supervisory authorities», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020.

16 L. Tosoni, «Article 60 Cooperation between the lead supervisory authority and the other supervisory authorities concerned», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 960.

17 Per una disamina più completa sul significato di questi tre casi, v. L. Tosoni, «Article 4(22). Supervi-

ricade in uno di questi tre casi, sarà da considerarsi «autorità di controllo interessata» e avrà diritto di partecipare al meccanismo di codecisione. Si è segnalato come, in caso di questioni che riguardino un trattamento di dati massiccio, in quanto a natura e portata dei dati trattati, nonché al numero degli interessati – come, ad esempio, quello effettuato da un *social network* – è probabile che le autorità di tutti gli Stati membri siano da considerarsi come interessate.[18]

All'autorità capofila spetta il ruolo di redigere un «progetto di decisione», il quale deve senza indugio essere trasmesso alle autorità interessate, al fine di ottenere il loro parere. Come è stato sottolineato in dottrina, il ruolo dell'autorità capofila è di essere un *primus inter pares*, avendo essenzialmente incarichi procedurali di *conduzione/guida* della procedura di co-decisione (in questo senso è più eloquente il termine inglese «lead *supervisory authority*»).[19] Al contrario, essa non deve intendersi come dotata di un potere decisionale (ossia di determinazione del contenuto della decisione finale) maggiore delle altre.[20] Al fine di garantire ciò, si prevede che, una volta ricevuto il progetto di decisione ai sensi del paragrafo 3, le autorità interessate – entro 4 settimane – possano esprimere un'«obiezione pertinente e motivata». Con riferimento a quest'ultimo concetto, la dottrina ritiene che la *ratio* della previsione di un'obiezione *qualificata* stia nella volontà del legislatore di evitare che le autorità possano sollevare al progetto di decisione multiple obiezioni sostenute da argomentazioni non particolarmente solide, causando peraltro dispendio di tempo e risorse economiche da parte dell'autorità capofila e del Comitato europeo per la protezione dei dati.[21]

A questo punto, per l'autorità capofila si aprono due strade: (*i*) seguire tale obiezione, redigendo un nuovo progetto di decisione e successivamente sottoponendolo al medesimo meccanismo di "controllo" previsto dal paragrafo 4 (con un termine per la presentazione delle obiezioni da parte delle altre autorità di due settimane, anziché quattro); oppure, (*ii*) non accogliere le obiezioni presentate o ritenerle non pertinenti e motivate. In quest'ultimo caso, essa deve sottoporre la questione al meccanismo di coerenza previsto dall'articolo 63 (v. *infra*).

Qualora, invece, nessuna delle autorità interessate sottoponga un'obiezione entro il termine previsto, il paragrafo 6 prevede che si consideri come se l'autorità

sory authority concerned», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020.

18 Tosoni, «Article 60» cit., p. 963.

19 Hijmans, «Article 56» cit., p. 918.

20 Ibidem.

21 L. Tosoni, «Article 4(24) Relevant and reasoned objection», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 290.

capofila e le autorità interessate acconsentano a tale progetto e siano da esso vincolate.

A seguito dell'operare del meccanismo di cui al paragrafo 6 appena citato, oppure dell'intervento del parere vincolante dell'EPDB, l'autorità capofila è incaricata di adottare la decisione finale, notificarla al titolare del trattamento e informare le altre autorità nonché l'EPDB (paragrafo 7). Tuttavia, il paragrafo 8 prevede una deroga per il caso in cui tale decisione consista nell'archiviazione o nel rigetto di un reclamo: in questo caso, è l'autorità cui è stato presentato il reclamo a dover adottare la decisione finale e notificarla al reclamante.

Come si è anticipato, qualora si rientri nel caso previsto dall'articolo 60, paragrafo 4, cioè vi sia un dissenso tra l'autorità capofila e (anche solo una del)le autorità interessate, la questione viene deferita al Comitato europeo per la protezione dei dati (CEPD o, nella versione inglese, EPDB), il quale opera ai sensi dell'articolo 65. Oltre che nell'eventualità appena citata, il medesimo meccanismo si applica anche nel caso in cui (*i*) vi siano opinioni contrastanti circa l'individuazione di quale sia lo Stato in cui insiste lo stabilimento principale del titolare, e di conseguenza quale sia l'autorità capofila (quindi vi sia una sorta di conflitto di competenza tra le varie autorità);[22] (*ii*) un'autorità di controllo non abbia richiesto il parere del comitato ai sensi dell'articolo 64, paragrafo 1, oppure non si sia conformata al parere emanato in conformità al medesimo articolo. In quest'ultimo caso la procedura può essere attivata anche da parte della Commissione: ciò segnala che la *ratio* della norma è assicurare un'applicazione uniforme del regolamento, manifestando – diversamente dalla normalità del GDPR – preferenza verso un sistema centralizzato di enforcement.[23]

Il paragrafo 2 disciplina le modalità di decisione del comitato: è prevista una maggioranza qualificata dei due terzi dei membri del comitato, il quale deve pronunciarsi entro un mese dal deferimento della questione. Tale termine può essere prorogato di un ulteriore mese qualora la questione sia giudicata come complessa.

Come si è già detto, il comitato emana un parere vincolante («decisione vincolante», ai sensi del paragrafo 1), ma la decisione definitiva è adottata dall'autorità capofila (o dall'autorità cui è stato presentato il reclamo, ex articolo 60, paragrafo 8). L'iter successivo all'adozione della decisione vincolante di cui ai paragrafo 1 è il seguente: (*i*) l'autorità competente è tenuta ad adottare la decisione senza ingiustificato ritardo e comunque entro un mese dalla notifica del parere del comitato

22 H. Hijmans, «Article 65 Dispute resolution by the Board», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 1017.

23 Ibidem.

(paragrafo 6); *(ii)* tale autorità informa il comitato circa la data in cui la propria decisione finale è stata notificata al titolare e all'interessato (paragrafo 6); *(iii)* la decisione finale deve accludere anche il parere vincolante emesso dal comitato e la menzione che esso verrà pubblicato sul sito web dell'EPDB (paragrafo 6); *(iv)* la decisione vincolante del comitato viene pubblicata sul sito web, solo dopo la notifica al titolare (paragrafo 5).

2.3 *Le patologie del meccanismo di coerenza: quale ruolo per l'EPDB?*

2.3.1 Lo scambio di informazioni

Terminata la presentazione, per sommi capi, del meccanismo di cui all'articolo 65, è possibile iniziare ad illustrare i problemi che esso pone. Un primo nucleo di questioni, che saranno illustrate nel presente paragrafo, attiene al modo con cui, talvolta, l'autorità capofila (non) collabora con le autorità interessate.

Secondo l'articolo 60, paragrafo 1, GDPR, le autorità sono tenute a cooperare e a «scambiarsi tutte le informazioni *utili*». Ciò può, già di per sé, generare delle discussioni su quali informazioni siano effettivamente utili, e dunque destinate ad essere scambiate;[24] le difficoltà interpretative sono aggravate dal fatto che la versione italiana utilizza il termine «utile» (al pari di quella francese, «*utile*»), mentre quella inglese il termine «*relevant*». L'assenza di ulteriori specificazioni farà sì che, di fatto, la scelta di quali siano le informazioni utili sarà fatta dall'autorità che le detiene. È evidente la posizione privilegiata in cui essa si trova: custodisce le informazioni, potendo scegliere quelle rilevanti/utili da condividere, e nessun altro – almeno nella fase iniziale del procedimento – non essendo in possesso delle stesse, non sarà in grado di sindacare tale scelta. Inoltre, è sempre tale autorità che sceglie *quando* condividere le informazioni.

2.3.2 La determinazione dell'ambito di indagine

Ulteriore problema è il fatto che, secondo talune autorità capofila, sarebbero esse stesse a dover stabilire quali norme del regolamento si debbano considerare violate e, quindi, l'ambito di indagine in un certo procedimento. In linea teorica, non è che sia precluso all'EPDB, con la sua decisione vincolante, di prescrivere all'autorità capofila l'ampliamento della compagine delle norme ritenute violate. Tuttavia, ciò si presenta come problematico se si considera che il procedimento amministrativo di irrogazione della sanzione deve rispettare il principio per cui

24 Hofmann e Mustert, «Data protection» cit., p. 466.

è necessario dare la possibilità al titolare del trattamento di esprimersi in ogni fase del procedimento sulle contestazioni ad esso mosse e, una volta notificato l'atto con cui si contestano talune violazioni, non è più possibile individuarne delle altre, quantomeno nel medesimo procedimento.[25]

Nell'ordinamento italiano, ciò è previsto dall'articolo 166, comma 5, d.lgs. 196/2003,[26] secondo cui «l'Ufficio del Garante, […] avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 *notificando al titolare o al responsabile del trattamento le presunte violazioni*» e dal regolamento 1/2019 del Garante, il quale all'articolo 12, comma 2, prevede che la comunicazione di avvio del procedimento correttivo e sanzionatorio contenga «una sintetica descrizione dei fatti e delle presunte violazioni della disciplina rilevante in materia di protezione dei dati personali». Successivamente, il destinatario della comunicazione può presentare le proprie difese entro 30 giorni dalla ricezione della stessa (art. 166, c. 6, d.lgs. 196/2003 e art. 13, c. 3, regolamento 1/2019). Sarebbe contrario ai principi del diritto amministrativo prevedere che, dopo la presentazione delle difese, sia possibile per l'autorità ampliare l'ambito di indagine, visto che per tali ulteriori violazioni il titolare non avrebbe la possibilità di esercitare il proprio diritto di difesa.

È questo quanto sostenuto dalla DPC (*Data Protection Commission*, l'autorità di controllo irlandese) nel caso *Twitter* (v. *infra* par. 2.4), sottolineando che essa aveva informato il titolare all'inizio della procedura circa l'ambito di indagine:[27] ampliarlo successivamente avrebbe significato mettere a repentaglio «l'intero processo di indagine a norma dell'articolo 60, esponendolo al rischio di rivendicazioni di iniquità procedurale».[28] Se è vero che tale principio va rispettato, a maggior ragione l'autorità capofila ha una responsabilità aggravata circa l'individuazione delle disposizioni ritenute violate, operazione che deve avvenire in maniera accurata, così da evitare che alcune violazioni rimangano non sanzionate.

25 L'ulteriore soluzione sarebbe quella di avviare un nuovo procedimento, operazione che, tuttavia, allungherebbe di molto i tempi di intervento, v. C. Docksey, «Article 65. Dispute Resolution by the Board», in *The EU General Data Protection Regulation: A Commentary - 2021 Update*, a cura di C. Kuner et al., Oxford University Press, New York 2021, p. 233-234.

26 Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali», recante «disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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)» (GU n. 174 del 29/07/2003).

27 L. Mustert, «The First Article 65 Decision – Correct and Consistent Application of the GDPR Ensured?», *European Data Protection Law Review*, 7, 1 (2021), p. 99.

28 Decisione 01/2020 cit., § 93.

Peraltro, non può essere condivisa la tesi espressa dalla DPC, secondo la quale la determinazione dell'ambito di indagine ricadrebbe all'interno della assoluta discrezionalità dell'autorità capofila.[29] Come già ricordato, è opinione diffusa che – una volta attivato il meccanismo di coerenza, per mezzo della proposizione di un'obiezione rilevante e motivata – l'autorità capofila abbia ruoli più che altro procedurali, spettando la determinazione del contenuto sostanziale della decisione all'EPDB.[30] Lasciare assoluta discrezionalità all'autorità capofila comporta, invece, non permettere al comitato di esercitare tale ruolo in maniera piena. Usando le parole dell'EPDB, ciò significherebbe incidere sul suo mandato «ai fini dell'indagine e sull'ulteriore accertamento dei fatti, nonché sulla capacità delle autorità interessate di presentare elementi sufficienti affinché l'EDPB possa sostenere le obiezioni».[31]

La principale soluzione al problema non è di certo quella di violare il diritto di difesa del titolare del trattamento. Invece, essa deve essere identificata in quella prospettata dall'EPDB stesso sin dalla decisione 1/2020: la cooperazione tra le autorità coinvolte deve avvenire *sin dal primo inizio* dell'attività di indagine, cosicché quest'ultimo sarà determinato concordemente in sede di comitato.[32] Tale necessità di cooperare non è espressione di una semplice cortesia istituzionale, ma un vero obbligo giuridico derivante dall'articolo 60, paragrafi 1 e 3, GDPR. Inoltre, ciò è prescritto anche dalle Linee guida relative alle obiezioni pertinenti e motivate: «Il sistema concepito dal legislatore sembra indicare che le autorità di controllo competenti dovrebbero definire consensualmente l'ambito dell'indagine in una fase precedente della procedura».[33] Quando l'individuazione delle disposizioni violate, avvenuta *concordemente con le altre autorità interessate*, preceda le notifiche al titolare prescritte dagli ordinamenti nazionali, non vi sarà lesione del diritto di difesa, né si sarà costretti ad avviare un altro procedimento *ex novo*.

29 Ivi, § 92.

30 Si v. le eloquenti parole dell'Avvocato Generale Bobek nelle sue conclusioni presentate il 13 gennaio 2021, causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:5, § 111-112: «è abbastanza chiaro che l'ACC non è l'unico organo incaricato dell'applicazione del RGPD in situazioni transfrontaliere. L'ACC è, piuttosto, un primus inter pares. […] Pertanto, la posizione dell'ACC a tal riguardo non è preminente rispetto a quella di qualsiasi altra autorità. […] Come affermato dall'ex Garante europeo della protezione dei dati, P. Hustinx, all'interno dello schema del RGPD, il ruolo di un'ACC "non dovrebbe essere inteso come una competenza esclusiva, ma come un modo strutturato di cooperare con altre autorità di controllo competenti a livello locale"».

31 Decisione 1/2020 cit., § 133.

32 Decisione 1/2020 cit., § 134-136.

33 Linee guida 9/2020 sull'obiezione pertinente e motivata ai sensi del regolamento (UE) 2016/679, versione 2.0, adottate il 9 marzo 2021, `https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202009_rro_final_it.pdf`, punto 28.

2.3.3 L'avvio di indagini d'ufficio

Bisogna ora dare conto un'altra prassi adottata da alcune autorità di controllo: quando vengono loro presentati dei reclami, l'autorità – anziché verificare la sussistenza delle violazioni lamentate nel reclamo *nell'ambito del procedimento generato dalla presentazione dello stesso* – iniziano una parallela indagine d'ufficio sulle medesime violazioni.

Tale prassi è censurabile. Innanzitutto, essa priva i reclamanti di qualsiasi diritto procedurale:[34] poiché essi non sono parte di tale procedimento, non vengono loro concessi i diritti previsti dalla legge, come ad esempio (*i*) il diritto di essere informati circa lo stato del reclamo ex articolo 77, paragrafo 2, GDPR; (*ii*) il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda (art. 78, par. 1, GDPR); (*iii*) il diritto di essere ascoltati nell'ambito del procedimento.[35] È quanto accaduto nel caso *WhatsApp*,[36] ove l'autorità di controllo irlandese ha iniziato un procedimento d'ufficio anziché dar seguito ai reclami presentati.[37] Peraltro, ciò ha l'ulteriore vantaggio di evitare che siano i reclamanti a definire le norme violate, lasciando che esse siano individuate dall'autorità stessa[38] (v. *supra* par. 2.3.2).

Anche la giurisprudenza pare criticare tali tendenze: nel caso *Schrems* ha stabilito che le autorità di controllo non hanno discrezionalità circa la trattazione dei reclami, dovendo essi essere esaminati con tutta la dovuta diligenza[39] (v. *infra* 2.9). Nel successivo caso *Facebook Ireland e Schrems* (cd. *Schrems II*), la Corte ha ulteriormente precisato che, oltre all'obbligo appena enunciato, qualora poi l'autorità, al termine dell'indagine, constati una violazione del GDPR, essa è tenuta a reagire in maniera appropriata al fine di porre rimedio all'inadeguatezza constatata.[40]

Inoltre, nella recente sentenza *SCHUFA Holding (Esdebitazione)*, la Corte ha avuto modo di precisare quale sia la natura del reclamo. Secondo lo *Hessischer*

34 Hofmann e Mustert, «Data protection» cit., p. 470.

35 L. Mustert, «EDPB Decision 1/2023: The Schrems Saga Back on the GDPR's Enforcement Rails», *European Data Protection Law Review*, 9, 2 (2023), p. 199.

36 Il caso che è culminato con la Decisione vincolante 1/2021 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente WhatsApp Ireland ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, adottata il 28 luglio 2021, `https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_it.pdf`.

37 Ivi, § 158.

38 L. Mustert, «The EDPB's second Article 65 Decision – Is the Board Stepping up its Game?», *European Data Protection Law Review*, 7, 3 (2021), p. 418.

39 Corte giust., causa C-362/14, *Schrems* cit., § 63.

40 Corte giust., sentenza del 16 luglio 2020 (Grande Sezione), causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, ECLI:EU:C:2020:559, § 111.

Beauftragter für Datenschutz und Informationsfreiheit (Commissario per la protezione dei dati e la libertà di informazione del Land dell'Assia), il diritto di presentare un reclamo sarebbe da concepire come un diritto di petizione, cosicché (*i*) il reclamo avrebbe la natura di una semplice "informativa" all'autorità[41] e (*ii*) il controllo giurisdizionale dovrebbe limitarsi a verificare la correttezza della condotta dell'autorità di controllo dal punto di vista *meramente procedurale*, senza poter esaminare la decisione nel merito.[42] La Corte non ritiene questa tesi corretta. Infatti, essa puntualizza che «la procedura di reclamo, che *non è simile a quella di una petizione*, è concepita come un *meccanismo idoneo a salvaguardare efficacemente i diritti e gli interessi delle persone coinvolte*».[43] Ulteriormente, i giudici osservano che la decisione di un'autorità di controllo che rigetti un reclamo presentato da una persona è una «decisione giuridicamente vincolante dell'autorità di controllo che la riguarda» ai sensi dell'articolo 78, paragrafo 1, GDPR.[44] Ammettere un controllo giurisdizionale ristretto su tale decisione significherebbe, quindi, privare l'interessato reclamante del diritto ad un ricorso giurisdizionale effettivo, concesso dalla norma appena citata e dall'articolo 47 della Carta.[45]

Infine, la medesima conclusione è stata tratta con riferimento alla direttiva 2016/680. Infatti, nel caso *Ligue des droits humains (Verifica del trattamento dei dati da parte dell'autorità di controllo)*, la Corte ha precisato che il diritto ad un rimedio giurisdizionale effettivo si sostanzia in un sindacato pieno del giudice, dovendo quest'ultimo avere il potere di esaminare le motivazioni poste alla base della decisione dell'autorità di controllo, nonostante questa si avvalga del potere di comunicare all'interessato solo le informazioni minime previste dall'articolo 17, paragrafo 3 di tale direttiva.[46]

41 M. Magierska, «No, the Data Protection Complaint is Not a Petition», *European Law Blog* (25 gennaio 2024), (visitato il 03/03/2024).

42 Corte giust., sentenza del 7 dicembre 2023, cause riunite C-26/22 e C-64/22, *UF (C-26/22) e AB (C-64/22) c. Land Hessen*, ECLI:EU:C:2023:958, § 32.

43 Ivi, § 58, corsivi aggiunti.

44 Ivi, § 50.

45 Ivi, § 47-51. Dell'opinione per cui sia necessario concedere al giudice un sindacato pieno è anche la giurisprudenza di legittimità italiana, si v. Cass. civ., sez. I, ordinanza 11 ottobre 2023, n. 28417: «*in tema di sanzioni amministrative, l'opposizione all'ordinanza-ingiunzione non configura un'impugnazione dell'atto, ed introduce, piuttosto, un ordinario giudizio sul fondamento della pretesa dell'autorità amministrativa, devolvendo al giudice adito la piena cognizione circa la legittimità e la fondatezza della stessa, con l'ulteriore conseguenza che il giudice ha il potere-dovere di esaminare l'intero rapporto, con cognizione non limitata alla verifica della legittimità formale del provvedimento, ma estesa – nell'ambito delle deduzioni delle parti – all'esame completo nel merito della fondatezza dell'ingiunzione, ivi compresa la determinazione dell'entità della sanzione sulla base di un apprezzamento discrezionale.*».

46 Corte giust., sentenza del 16 novembre 2023, causa C-333/22, *Ligue des droits humains ASBL e BA contro Organe de contrôle de l'information policière*, ECLI:EU:C:2023:874, § 67-72.

2.4 *La determinazione del contenuto delle sanzioni*

Un ulteriore problema che è stato segnalato dalla dottrina attiene alla modalità con la quale, una volta accertata la sussistenza di una certa violazione del GDPR, viene determinata la sanzione a carico del titolare del trattamento. Sul punto, il GDPR ha sicuramente rappresentato un passo in avanti verso l'uniformazione della disciplina sanzionatoria: confrontandolo con la direttiva 95/46/CE, si nota che quest'ultima non armonizzava in alcun modo le modalità di definizione del contenuto della sanzione, generando così significative differenze tra gli Stati membri.[47]

Al contrario, l'articolo 83 GDPR definisce delle «condizioni generali per infliggere sanzioni amministrative pecuniarie», valevoli per tutte le autorità di controllo: innanzitutto, le sanzioni devono essere, in ogni caso, *effettive, proporzionate e dissuasive*. Inoltre, per la loro determinazione è necessario tenere conto degli elementi indicati al paragrafo 2 (ad es., la natura, la gravità e la durata della violazione, il carattere doloso o colposo della violazione, il grado di cooperazione con l'autorità di controllo, …).

Da un punto di vista pratico, rivestono però particolare rilevanza i paragrafi 4, 5 e 6, i quali stabiliscono – in relazione alla violazione di diversi insiemi di norme del regolamento – un limite all'importo della sanzione rispettivamente di: (*i*) 10 milioni di euro, o per le imprese,[48] fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (paragrafo 4); (*ii*) 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (paragrafo 5); (*iii*) il medesimo importo, per la violazione di quanto richiamato dal paragrafo 6. Si deve sottolineare che la disposizione è rilevante non tanto in quanto fissi dei tetti massimi, ma più che altro perché – letta *a contrario* – conferisce alle autorità il potere di irrogare sanzioni di valore significativamente alto, soprattutto per la previsione di una soglia non fissa, ma parametrata al fatturato annuo (che, in caso di taluni titolari del trattamento che rientrano nella categoria delle cd. *big tech*, può essere molto elevato).

Quindi, come si nota, in astratto le autorità hanno i medesimi poteri sanzionatori e dovrebbero applicare le sanzioni in maniera uniforme.[49] Ciò è ricordato

47 Si v. A. Schreiber, «Feeling fine! Harmonisation and inconsistency in EU supervisory authority administrative fines», *Journal of Data Protection & Privacy*, 2, 4 (2019), p. 376, il quale ricorda che, ad es., in Romania la sanzione massima era di 50000 Lei (circa € 10500), mentre in Belgio di € 600000.

48 Con riguardo al significato di "impresa", il considerando 150 ritiene che la nozione debba essere mutuata da quella di cui agli articoli 101 e 102 TFUE.

49 Mustert, «EDPB Decision 1/2023» cit., p. 195.

anche dal considerando 129 del GDPR:

> [a]l fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento. Tali poteri dovrebbero includere anche il potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. […]

Tuttavia, se quanto appena affermato è valido nella teoria, l'analisi dei casi sinora oggetto di decisione vincolante dell'EPDB ha fatto emergere come, almeno inizialmente, nella pratica le sanzioni effettivamente erogate siano state molto spesso di importo non sufficientemente alto e, dunque carenti del requisito della dissuasività. Una delle principali cause di questo problema è stata identificata in dottrina con il fatto che la determinazione dell'effettiva entità della sanzione finale (e delle eventuali misure correttive) è effettuata non tanto *dall'EPDB* nella sua decisione vincolante, ma *dall'autorità capofila* quando adotta la decisione finale.[50] Tale discrezionalità dell'autorità capofila ha, infatti, generato numerose dispute tra questa e le altre autorità interessate durante l'adozione delle decisioni vincolanti del comitato.[51]

Ad esempio, nel caso che ha dato origine alla prima decisione presa ex articolo 65,[52] avente ad oggetto la violazione di alcune norme del GDPR da parte di Twitter, l'autorità capofila irlandese (*Data Protection Commission*) aveva proposto di irrogare una sanzione compresa tra 135000 e 275000 euro, pari ad un importo tra «lo 0,005% e lo 0,01% del fatturato annuo dell'impresa o tra lo 0,25% e lo 0,5% dell'importo massimo della sanzione pecuniaria che può essere applicata in relazione a tali violazioni».[53] Tale sanzione è stata oggetto di critiche da parte delle altre autorità interessate, le quali hanno proposto importi più elevati: ad esempio, lo *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (autorità di controllo del *Land* di Amburgo), anche in rappresentanza delle altre autorità tedesche, ha sottolineato come l'importo proposto sarebbe troppo basso, non dissuasivo, e

50 G. Gentile e O. Lynskey, «Deficient by Design? The Transnational Enforcement of the GDPR», *International & Comparative Law Quarterly*, 71, 4 (2022), p. 810.

51 Mustert, «EDPB Decision 1/2023» cit., p. 196.

52 Decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, adottata il 9 novembre 2020, `https://edpb.europa.eu/system/files/2021-04/edpb_bindingdecision01_2020_it.pdf`.

53 Decisione 01/2020 cit., § 165.

quindi in violazione dei criteri di cui all'articolo 83, proponendo una sanzione da € 7348035 a € 22044105.[54] Il comitato ha, in effetti, ritenuto la sanzione proposta dall'autorità capofila troppo bassa, in quanto non soddisfacente «la sua finalità di misura correttiva» nonché «i requisiti di cui all'articolo 83, paragrafo 1».[55] Tuttavia, ciò che il comitato non fa è stabilire quale debba essere l'entità della sanzione pecuniaria,[56] limitandosi a chiedere all'autorità di «riesaminare gli elementi su cui si basa per quantificare l'importo della sanzione pecuniaria fissata da infliggere a TIC in modo da garantire che sia adeguata ai fatti del caso».[57] L'autorità irlandese ha quindi inflitto una sanzione finale di € 450000, la quale, sebbene più alta di quella originariamente proposta, solleva comunque significativi dubbi circa la sua dissuasività.[58] D'altra parte, vi è da chiedersi se l'atteggiamento dell'EPDB non avrebbe potuto essere più incisivo: se l'autorità capofila aveva già manifestato l'intenzione di irrogare una sanzione non molto elevata, probabilmente la semplice indicazione di riconsiderare alcuni elementi non è stata sufficiente per modificare un atteggiamento di tendenziale favore verso i titolari del trattamento da parte della *Data Protection Commission*.

Anche nella seconda decisione[59] si è ritenuto l'importo (50 milioni di euro), proposto nel progetto di decisione, sempre ad opera della DPC, troppo basso, ordinando all'autorità irlandese di individuare un «importo della sanzione pecuniaria più elevato per le violazioni individuate rispetto alla sanzione amministrativa prevista nel progetto di decisione, pur rimanendo in linea con i criteri di efficacia, proporzionalità e dissuasività sanciti dall'articolo 83, paragrafo 1, RGPD».[60] Tuttavia, anche in questo caso si omette di identificare uno specifico importo (o, quantomeno, un intervallo), cosicché la DPC lo ha rideterminato in 225 milioni di euro:[61] se si tratta, comunque, di un ammontare piuttosto considerevole, rappresentativo di una delle sanzioni più elevate irrogate per la violazione del GDPR, bisogna comunque notare come esso sia pari solo allo 0,08% del fatturato annuo di Facebook.[62]

Un cambio di rotta si è verificato, invece, con la Decisione 01/2023.[63] Nel caso

54 Ivi, § 169.
55 Ivi, § 199.
56 Docksey, «Article 65. Dispute Resolution by the Board» cit., p. 233.
57 Decisione 1/2020 cit., § 200, 207.
58 Mustert, «The First Article 65 Decision» cit., p. 99.
59 Decisione vincolante 1/2021 cit.
60 Ivi, § 424.
61 Mustert, «The EDPB's second Article 65 Decision» cit., p. 422.
62 Ibidem.
63 Decisione vincolante 1/2023 in merito alla controversia presentata dall'autorità di controllo irlandese sui trasferimenti di dati da parte di Meta Platforms Ireland Limited per il servizio offerto da

di specie, l'autorità capofila (ancora una volta, la DPC) aveva ritenuto, nel proprio progetto di decisione, sufficiente l'adozione di misure correttive ex articolo 58, paragrafo 2, GDPR, reputando invece l'irrogazione di una sanzione amministrativa pecuniaria sproporzionata, non effettiva e non dissuasiva.[64] A tale impostazione sono state opposte obiezioni, ritenute pertinenti e motivate, da parte di molte autorità interessate: secondo queste ultime, invece, sarebbe necessario irrogare anche una sanzione amministrativa pecuniaria, in quanto solo quest'ultima sarebbe idonea a dissuadere efficacemente Meta dal continuare a tenere una condotta[65] già ritenuta più volte in violazione del regolamento. Quest'ultimo orientamento è stato condiviso anche dal CEPD, il quale ritiene che vi sia la necessità di una sanzione amministrativa pecuniaria.[66] Ciò che vi è di nuovo in questa decisione è il fatto che il comitato, ritenendo la violazione commessa da Meta come particolarmente grave,[67] incarica la DPC di irrogare a tale titolare una sanzione che non solo tenga conto dei criteri stabiliti dall'articolo 83 GDPR, *ma anche delle linee guida dell'EDPB sul calcolo delle sanzioni*[68] e *della valutazione del comitato contenuta nella decisione stessa*.[69] In particolare, il CEPD ritiene che «l'autorità di controllo capofila debba determinare l'importo iniziale per il successivo calcolo della sanzione pecuniaria a un livello compreso tra il 20% e il 100% del massimo legale applicabile».[70] Come affermato precedentemente, quest'ultima decisione pare segnare un cambio di passo in seno al comitato, il quale appare meno timido nell'esercitare il proprio ruolo di garante della coerenza nell'applicazione del regolamento generale sulla protezione dei dati, anche se ciò significa restringere la discrezionalità circa la determinazione del contenuto finale da parte della capofila. Tale restrizione è peraltro parziale, visto che è stata lasciata alla DPC un'ampia "forbice" (dal 20 al 100%), come testimonia il fatto che l'autorità ha determinato l'importo della sanzione in 1,2 miliardi di euro, quando il 4% del fatturato di Meta sarebbe stato 4,2 miliardi di euro.[71]

Facebook (articolo 65 GDPR), adottata il 13 aprile 2023, https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_it.pdf.

64 Ivi, § 37-38.

65 Segnatamente, il trasferimento di dati personali dall'Unione europea agli Stati Uniti d'America, in violazione dei principi stabiliti da Corte giust., causa C-311/18, *Facebook Ireland e Schrems* cit.

66 Decisione 1/2023 cit., § 141-142.

67 Ivi, § 173.

68 Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR, versione 2.1, adottate il 24 maggio 2023, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_it_0.pdf.

69 Ivi, § 178.

70 Ivi, § 174.

71 Mustert, «EDPB Decision 1/2023» cit., p. 198.

2.5 *La possibile lesione del diritto di essere ascoltati durante il procedimento*

Da un lato, l'impiego del meccanismo di coerenza, almeno nella teoria, permette di assicurare che l'applicazione delle norme del regolamento generale sulla protezione dei dati sia uniforme. Dall'altro, l'uso di questo strumento deve essere valutato dal punto di vista del diritto delle parti ad essere sentite nell'ambito del procedimento che le riguarda.

L'articolo 41, paragrafo 2, della Carta prevede «il diritto di ogni individuo di essere ascoltato prima che nei suoi confronti venga adottato un provvedimento individuale che gli rechi pregiudizio». Secondo la Corte, esso

> garantisce a chiunque la possibilità di manifestare, utilmente ed efficacemente, il proprio punto di vista durante il procedimento amministrativo e prima dell'adozione di qualsiasi decisione che possa incidere in modo negativo sui suoi interessi.[72]

Si deve ritenere che, in caso di presentazione di un reclamo, tale diritto debba essere attribuito sia all'interessato reclamante che al titolare del trattamento, posto che la decisione che accerta la violazione ed accoglie il reclamo è sfavorevole al secondo, mentre quella che lo respinge è pregiudizievole nei confronti del primo, in quanto non vengono adottate misure contro le lesioni del diritto alla protezione dei dati da lui lamentate.

È necessario precisare che costituisce giurisprudenza costante della Corte il principio secondo cui la norma sarebbe indirizzata *solamente alle istituzioni e agli organi dell'Unione* (e *non agli Stati membri*), ancorché, come in questo caso, lo Stato membro stia attuando il diritto dell'Unione e, quindi, si rientri nell'ambito applicativo della Carta ex articolo 51, paragrafo 1. Infatti, viene osservato come il paragrafo 1 dell'articolo 41 sia indirizzato espressamente alle «*istituzioni e dagli organi dell'Unione*».[73] Tuttavia, la stessa Corte ha precisato che esso riflette un principio generale di diritto dell'Unione[74] espresso anche dagli articoli 47 e 48 della

72 Corte giust., sentenza del 11 dicembre 2014, causa C-249/13, *Khaled Boudjlida c. Préfet des Pyrénées-Atlantiques*, ECLI:EU:C:2014:2431, § 36.

73 *Ex multis* v. Corte giust., sentenza del 8 maggio 2019, causa C-230/18, *PI contro Landespolizeidirektion Tirol*, ECLI:EU:C:2019:383, § 56; Corte giust., causa C-249/13, *Boudjlida*, cit., § 32; Corte giust., sentenza del 17 luglio 2014, cause riunite C-141/12 e C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel e Minister voor Immigratie, Integratie en Asiel c. M e S*, ECLI:EU:C:2014:2081, § 67; Corte giust., sentenza del 21 dicembre 2011, causa C-482/10, *Teresa Cicala c. Regione Siciliana*, ECLI:EU:C:2011:868, § 28.

74 Corte giust., sentenza del 5 novembre 2014, causa C-166/13, *Sophie Mukarubega c. Préfet de police e Préfet de la Seine-Saint-Denis*, ECLI:EU:C:2014:2336, § 45; Corte giust., cause riunite C-141/12 e C-372/12, *YS e a.* cit., § 68; Corte giust., sentenza del 8 maggio 2014, causa C-604/12, *H.N. c. Minister for Justice, Equality and Law Reform e a.*, ECLI:EU:C:2014:302, § 49.

Carta,[75] cosicché sembra possibile affermare che anche gli Stati membri, quando attuano il diritto dell'Unione (e l'applicazione del GDPR rientra sicuramente in questo caso) siano comunque tenuti a garantirlo.

I procedimenti relativi al trattamento transfrontaliero si presentano come particolarmente problematici per la tutela di questo diritto e, come si vedrà nel paragrafo successivo, anche per il diritto ad un rimedio giurisdizionale effettivo. Per comprendere come mai ciò sia vero, si deve considerare la natura di tali procedimenti e delle decisioni cui essi conducono. Normalmente, il principio generale che regge l'attuazione del diritto comunitario, fissato dall'articolo 291, paragrafo 1, TFUE è il seguente: poiché i Trattati non conferiscono una competenza generale all'Unione per l'esecuzione delle norme comunitarie, tale potere spetta agli Stati membri.[76] Tuttavia, in specifici ambiti accade che norme di diritto primario o derivato prevedano l'attribuzione del potere di determinare il contenuto sostanziale del provvedimento finale sia alle autorità nazionali, *ma anche ad istituzioni, organi od organismi dell'Unione europea*, dando origine ad un cd. «procedimento amministrativo misto».[77] Quest'ultimo è caratterizzato dalla sussistenza di una serie di sub-procedimenti (taluni a livello nazionale, altri a livello europeo), i quali poi si combinano assieme, formando la decisione finale.[78]

Secondo la dottrina, uno degli ambiti in cui si ha questa «amministrazione condivisa» (concetto più noto con il termine inglese di «*shared administration*»)[79] sarebbe proprio l'attuazione del GDPR nel caso di trattamenti transfrontalieri.[80] Per comprendere meglio questo aspetto, si prenda in considerazione il caso in cui viene effettuato un reclamo: *(i)* l'interessato lo presenta dinnanzi all'autorità dello Stato membro in cui ha la residenza, lavora abitualmente o in cui si è verificata la presunta violazione (art. 77, par. 1, GDPR); *(ii)* se il titolare non ha lo stabilimento principale in tale Stato membro, l'autorità trasmette il fascicolo alla capofila; *(iii)* quest'ultima cura l'istruttoria, svolgendo le indagini necessarie, e poi redige il progetto di decisione; *(iv)* se vi sono obiezioni pertinenti e motivate e l'autorità capofila non intende conformarsi, la questione viene deferita all'EPDB;

75 Corte giust., sentenza del 22 novembre 2012, causa C-277/11, *M.M. c. Minister for Justice, Equality and Law Reform e a.*, ECLI:EU:C:2012:744, § 82.

76 G. della Cananea, «The European Union's Mixed Administrative Proceedings», *Law and Contemporary Problems*, 68 (2004), p. 197.

77 Ivi, p. 198-199.

78 C. Eckes e J. Mendes, «The Right to Be Heard in Composite Administrative Procedures: Lost in between Protection?», *European Law Review*, 36 (2011), p. 651.

79 Per una definizione di «*shared administration*» si v. P. P. Craig, *EU administrative law*, 3ª ed., Oxford University Press, Oxford 2018, p. 30-34.

80 M. Eliantonio e N. Vogiatzis, «Judicial and Extra-Judicial Challenges in the EU Multi- and Cross-Level Administrative Framework», *German Law Journal*, 22, 3 (2021), p. 316.

(v) quest'ultimo adotta la sua decisione vincolante; *(vi)* la capofila adotta la decisione finale (oppure l'autorità cui è stato presentato il reclamo, se si tratta di rigettarlo). Si nota, quindi, come l'effettivo contenuto della decisione finale sia (almeno potenzialmente) determinato dall'intervento di soggetti diversi: autorità capofila, autorità interessate ed EPDB. Si deve porre l'accento sul fatto che l'eventuale decisione dell'EPDB è vincolante: l'autorità capofila, nell'adottare la decisione finale, non potrà discostarsene, cosicché la determinazione sostanziale del contenuto di tale decisione sarà, in concreto, ad opera del comitato.

Dal punto di vista dell'interessato, egli ha sì diritto di essere ascoltato nell'ambito del procedimento che lo riguarda, ma quest'ultimo è sussistente con riferimento al procedimento incardinato in seno all'autorità di presentazione del reclamo, la quale *non è però quella che determinerà il contenuto sostanziale della decisione finale*. Infatti, esso sarà definito dalla capofila oppure dall'EPDB. Dinnanzi alla prima, non sembra potersi ipotizzare un diritto del reclamante ad intervenire;[81] in ogni caso, anche se tale diritto sussistesse, il suo esercizio si rivelerebbe molto complesso, vista la necessità di rivolgersi ad un altro Stato membro, probabilmente in un'altra lingua e secondo regole procedurali proprie di tale Stato.[82] Invece, con riferimento alla posizione del titolare del trattamento, quest'ultimo è, quantomeno, agevolato dal fatto che l'autorità capofila, in quanto tale, si trova nello Stato membro ove vi è il suo stabilimento principale. Vi è da chiedersi se questa disparità tra le situazioni di interessato e titolare sia giustificata, se si considera che il secondo – specie se si tratta di una *big tech* – è molto spesso dotato di risorse economiche ed organizzative idonee ad affrontare procedimenti (ed eventualmente processi) in altri Stati membri, mentre il primo no.

La situazione davanti all'EPDB non pare essere migliore. Infatti, il processo decisionale di cui all'articolo 65 si svolge alla presenza dei soli membri del comitato, senza che, tendenzialmente, sia previsto l'intervento delle parti interessate. Infatti, in linea teorica, l'articolo 11 del regolamento interno dell'EPDB[83] prevede, al

81 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 814-815.

82 Si v. H. C. Hofmann, «Multi-Jurisdictional Composite Procedures - The Backbone to the EU's Single Regulatory Space», *University of Luxembourg Law Working Paper*, 3 (2019), nota 91, il quale osserva: «*when the lead authority will open an investigation against a data controller, the complainant has no enforceable rights to participate since procedures before a lead authority are, in this system, conducted like investigations upon another authority's initiative. Essentially, procedural rights of those individuals, who are not capable of mounting a complaint outside of their home jurisdiction will be disadvantaged, possibly thereby in violation of the prohibition of discrimination on the basis of nationality or origin protected under Article 21 CFR.*».

83 Regolamento interno del Comitato europeo per la protezione dei dati, versione 8, adottato il 25 maggio 2018, modificato da ultimo e adottato il 6 aprile 2022, https://www.edpb.europa.eu/system/files/2022-08/edpb_rules_of_procedure_version_8_adopted_20220406_i

paragrafo 1:

> Il Comitato rispetta il diritto a una buona amministrazione sancito dall'articolo 41 della Carta. Prima di prendere una decisione, il Comitato si assicura che siano state ascoltate tutte le persone alle quali tale decisione potrebbe recare pregiudizio.

Ciò sembra però, normalmente, estrinsecarsi tramite la trasmissione, da parte dell'autorità capofila, a norma del paragrafo 2, lettera f), di:

> […] osservazioni scritte raccolte dall'autorità di controllo capofila con riguardo alle persone alle quali la decisione del Comitato potrebbe recare pregiudizio, unitamente alla conferma, suffragata da elementi probatori, dei documenti che, fra quelli presentati al Comitato stesso, sono stati trasmessi a dette persone quando sono state invitate a esercitare il diritto al contraddittorio, oppure a una chiara indicazione degli elementi rispetto ai quali quanto sopra non si è verificato.

Il terzo alinea del paragrafo 2 pare però adottare un approccio diverso. Infatti, da un lato esso ribadisce che «il Comitato tiene conto esclusivamente dei documenti forniti dall'autorità di controllo capofila e dall'altra o dalle altre autorità di controllo interessate prima del deferimento della questione suddetta»; dall'altro, però, afferma che «il Comitato tiene conto delle *informazioni eventualmente acquisite* nel contesto delle *attività finalizzate ad assicurare il diritto al contraddittorio delle parti interessate*». Quindi, quest'ultimo periodo sembra ammettere la possibilità che in seno all'EPDB stesso vi sia l'audizione delle parti interessate. Tuttavia, si tratta solamente di una deduzione teorica, in quanto nel regolamento non sono presenti ulteriori disposizioni volte ad attuare questo principio e non risulta, al momento, che tali audizioni siano mai avvenute.

Parte della dottrina osserva che questo problema potrebbe essere attenuato qualora la decisione vincolante si basi esclusivamente su temi che sono stati affrontati dall'autorità capofila nel suo progetto di decisione.[84] Tuttavia, questa soluzione non convince, in quanto: (*i*) come si è visto nei paragrafi precedenti, molto spesso ciò non succede e l'EPDB sente la necessità di espandere l'ambito di intervento (v. par. 2.3.2); (*ii*) anche qualora quanto affermato fosse vero, ciò riporta al problema precedente, cioè l'impossibilità per l'interessato di intervenire davanti alla capofila.

Piuttosto, sembra necessario concentrarsi su alcuni aspetti sottolineati da dottrina e giurisprudenza. Innanzitutto, il diritto ad essere sentiti dovrebbe essere assicurato nella fase in cui viene presa la decisione sostanziale[85] e, quindi, nel caso

t.pdf.

84 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 816.

85 T. Lock, «Article 41 CFR Right to good administration», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer et al., Oxford University Press, New York 2019, p. 2205; Eckes e Mendes, «The Right to Be Heard» cit., p. 669.

di specie dinnanzi all'EPDB. Adottare questa prospettiva avrebbe l'ulteriore conseguenza di far ricadere di nuovo la fattispecie all'interno dell'ambito applicativo espressamente individuato dall'articolo 41, paragrafo 1, della Carta.

Chiaramente, se sulla questione di cui si discute le parti si siano già espresse durante le loro interlocuzioni con l'autorità, non paiono necessari ulteriori adempimenti. Tuttavia, se questo non è il caso, non sembra ostare ad un'eventuale audizione davanti al comitato la mancanza di specifiche norme volte a prevedere una simile prassi. Infatti, la Corte di Giustizia ha ricordato che

> il rispetto dei diritti della difesa in qualsiasi procedimento promosso nei confronti di una persona e che possa sfociare in un atto per essa lesivo costituisce un principio fondamentale del diritto comunitario e dev'essere garantito *anche in mancanza di qualsiasi norma riguardante il procedimento di cui trattasi*.[86]

Resta da vedere se il comitato, in futuro, si adeguerà a questa interpretazione, eventualmente novellando il regolamento di procedura. Peraltro, ciò gli permetterebbe di acquisire, probabilmente, un ruolo più di primo piano rispetto all'autorità capofila, in quanto sarebbe l'EPDB – collegialmente – a gestire l'audizione. Inoltre, sarebbero al contempo risolti anche i timori rappresentati dalla DPC nei casi enunciati nel paragrafo 2.3.2.

2.6 *La tutela giurisdizionale effettiva contro le decisioni dell'autorità di controllo*

Nel paragrafo precedente si è presa in considerazione la possibilità, per le parti, di manifestare la propria opinione *prima* dell'adozione della decisione nei loro confronti. Ora, invece, si analizzeranno quali sono i modi date alle parti per impugnare la decisione dell'autorità di controllo che sia nei loro confronti sfavorevole. Inoltre, nel paragrafo successivo, si tenterà di capire se, e in che modo, sia possibile impugnare la decisione vincolante di cui all'articolo 65 GDPR dinnanzi alla Corte di Giustizia dell'Unione europea.

L'articolo 78, paragrafo 1, GDPR prevede che «[f]atto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica [abbia] il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda». Il paragrafo 2 prevede il

86 Corte giust., sentenza del 24 ottobre 1996, causa C-32/95 P, *Commissione delle Comunità europee contro Lisrestal - Organização Gestão de Restaurantes Colectivos Ld[a], Gabinete Técnico de Informática Ld[a] (GTI), Lisnico - Serviço Marítimo Internacional Ld[a], Rebocalis - Rebocagem e Assistência Marítima Ld[a] e Gaslimpo - Sociedade de Desgasificação de Navios SA*, ECLI:EU:C:1996:402, § 21, corsivo aggiunto; v. anche Corte giust., causa C-277/11, *M.* cit., § 86; Corte giust., sentenza del 18 dicembre 2008, causa C-349/07, *Sopropé - Organizações de Calçado Lda c. Fazenda Pública*, ECLI:EU:C:2008:746, § 38.

medesimo diritto in caso di inerzia dell'autorità cui si è presentato un reclamo, ossia qualora essa non lo tratti oppure ometta di informare il reclamante circa lo stato o l'esito di esso entro tre mesi. Come si comprende, la norma è rilevante in quanto espressiva del principio di cui all'articolo 47 della Carta: non essendo le autorità di controllo "tribunali", deve essere garantito nei loro confronti un ricorso effettivo dinanzi a un giudice imparziale,[87] al quale deve essere attribuito un sindacato giurisdizionale pieno.[88]

Nell'economia del presente elaborato non è possibile concentrarsi su tutte le questioni derivanti da questa norma. La trattazione si focalizzerà, dunque, sulle implicazioni che essa ha nei procedimenti transfrontalieri. Innanzitutto, bisogna considerare che l'articolo 78, paragrafi 1 e 2, non dicono quale sia lo Stato membro in cui sia necessario radicare la controversia. Tale informazione è fornita dal paragrafo 3, secondo cui «[l]e azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita». Pertanto, nel caso di trattamento transfrontaliero, possono darsi due casi: *(i)* qualora la decisione rigetti il reclamo, essa sarà presa dall'autorità cui esso era stato presentato (art. 60, par. 8, GDPR), e di conseguenza l'azione va intentata dinnanzi al giudice dello Stato membro ove ha sede quella autorità; *(ii)* negli altri casi, la decisione sarà ad opera della capofila e il ricorso verso la stessa andrà presentato nello Stato membro di appartenenza della stessa.

Per comprendere quale sia il problema principale che la disciplina comporta, si devono considerare le posizioni delle due parti. Il titolare del trattamento: *(i)* se il reclamo viene rigettato, non avrà interesse ad impugnare; *(ii)* se il reclamo viene accolto (e, quindi, una violazione viene accertata), egli potrà ricorrere ad un giudice dello Stato membro ove egli ha lo stabilimento principale. Invece, l'interessato: *(i)* se il reclamo viene rigettato, dovrà rivolgersi al giudice dello Stato membro ove ha presentato il reclamo, giurisdizione che dovrebbe essere a lui conveniente, in quanto da lui scelta ex articolo 77, paragrafo 1, GDPR; *(ii)* se il reclamo viene accolto, il ricorso contro tale decisione dovrà essere presentato nello Stato dell'autorità capofila. In relazione a quest'ultimo punto, bisogna precisare che il reclamante – ancorché il reclamo sia accolto – potrebbe aver interesse, comunque, ad impugnare la decisione: si pensi a tutti quei casi in cui egli non condivida la portata delle misure correttive e sanzionatorie individuate dall'autorità capofila.

Dal rilievo appena effettuato emerge, quindi, la disfunzionalità della disciplina: nel caso *sub* (*ii*), l'interessato è costretto a promuovere un giudizio davanti ad un

87 W. Kotschy, «Article 78 Right to an effective judicial remedy against a supervisory authority», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 1127.

88 Corte giust., cause riunite C-26/22 e C-64/22, *SCHUFA Holding (Esdebitazione)* cit., § 47-51.

giudice di uno Stato membro (probabilmente) diverso da quello ove risiede, in una lingua molto spesso diversa dalla propria e secondo delle norme procedurali a lui non familiari. Invece, il titolare del trattamento avrà, più o meno sempre, la sicurezza di poter contare su una giurisdizione familiare, ossia quella dello Stato membro ove ha lo stabilimento principale. La stortura è più evidente se si considera che l'interessato reclamante è per definizione una persona fisica, e quindi soggetto che non necessariamente dispone di una disponibilità economica tale da farsi carico delle spese legali di promozione di un giudizio in altro Stato membro. Addirittura, secondo Hofmann, ciò configurerebbe una violazione del divieto di discriminazione sulla base della nazionalità previsto dall'articolo 21 della Carta.[89]

Ad oggi, non consta che la Corte si sia pronunciata espressamente sul tema. Tuttavia, essa – in relazione al principio del paese d'origine che, come si è detto pare essere un precursore del meccanismo *one-stop-shop* – ha più volte negato deroghe alla giurisdizione stabilita, quando si adduceva come motivazione la debolezza di una delle parti.[90] Inoltre, in *Facebook Ireland e a.*, essa ha escluso che altre autorità, che non siano l'autorità capofila, possano promuovere un'azione giurisdizionale contro il titolare davanti ad un giudice del loro Stato membro, per lamentarsi di una presunta violazione del GDPR.[91]

Non pare d'aiuto neanche quanto affermato dall'Avvocato Generale Bobek nelle proprie conclusioni sul caso *Facebook Ireland e a.* appena citato, ossia che

> sebbene tale norma possa sembrare meno favorevole per i singoli, occorre tener presente che, ai sensi dell'articolo 60, paragrafi 8 e 9, del RGPD, ove un reclamo presentato da un interessato sia integralmente o parzialmente rigettato o archiviato, la relativa decisione è adottata e notificata all'interessato *ad opera dell'autorità di controllo cui è stato proposto il reclamo*. Ciò vale indipendentemente dalla circostanza che tale autorità sia o meno l'ACC, consentendo così (se del caso) all'interessato di agire giudizialmente nel proprio Stato membro.[92]

Infatti, tale prospettiva offre una soluzione incompleta. È vero che il paragrafo 9 prevede che, nel caso di accoglimento del reclamo solo parziale, la decisione di rigetto sia adottata dall'autorità (non capofila, ma) di presentazione del reclamo. Tuttavia, come si è già anticipato, il problema di tutela si pone proprio in relazione

89 Hofmann, «Multi-Jurisdictional Composite Procedures» cit., nota 91.

90 Lutzi, «Internet Cases in EU Private International Law» cit., p. 707; Corte giust., sentenza del 16 gennaio 2014, causa C-45/13, *Andreas Kainz c. Pantherwerke AG*, ECLI:EU:C:2014:7, § 31; Corte giust., sentenza del 25 ottobre 2012, causa C-133/11, *Folien Fischer AG e Fofitec AG c. Ritrama SpA*, ECLI:EU:C:2012:664, § 46.

91 Corte giust., causa C-645/19, *Facebook Ireland e a.* cit.

92 Conclusioni dell'AG Bobek, causa C-645/19, *Facebook Ireland Limited e a.* cit., § 104.

all'altra "porzione", ossia quella «riguardante azioni in relazione al titolare del trattamento», che viene adottata dalla capofila. Infatti, lo si ripete, il reclamante può avere interesse a ricorrere anche contro tale parte, in quanto essa, *pur accogliendo una parte di reclamo, può farlo in maniera ritenuta non soddisfacente dall'interessato*. Peraltro, Hofmann e Mustert vedono questa norma non in termini agevolativi, ma come idonea a creare una «*complicating situation*», sottolineando che essa obbliga l'interessato a ricercare la tutela giurisdizionale in *due differenti Stati membri* per *una medesima* fattispecie concreta.[93]

In conclusione, da un lato è vero che il principio del paese d'origine rappresenta un caposaldo del funzionamento del mercato interno e, segnatamente, della libera prestazione dei servizi. La giurisprudenza *Cassis* e tutti i suoi corollari, incluso il meccanismo di sportello unico previsto dal GDPR, permettono alle imprese di erogare i propri servizi all'interno del territorio dell'Unione senza che questo appaia diviso da «frontiere interne». Nel caso di specie, ciò evita ai titolari del trattamento di dover dialogare con più di cinquanta autorità di controllo (si tenga conto che solo la Germania è dotata di diciotto autorità: un'autorità federale, più una per ogni *Land*, esclusa la Baviera che ne ha due). Dall'altro, però, in una prospettiva *de iure condendo* vi è da chiedersi se sia più ragionevole far dialogare con autorità di altri Stati membri il titolare, dotato di un'organizzazione strutturata e, molto spesso, di dotazioni economiche ingenti, oppure costringere un individuo a «"fare il giro" delle aule di giustizia dell'Unione europea»[94] al fine di difendere il proprio diritto alla protezione dei dati personali. Ad avviso dello scrivente, un'interpretazione volta a garantire in maniera effettiva il diritto previsto dall'articolo 16 TFUE e dall'articolo 8 della Carta sembra propendere verso la prima di queste ipotesi.

2.7 *L'impugnazione delle decisioni vincolanti dell'EPDB: ricorso per annullamento o rinvio pregiudiziale di validità?*

Continuando dal paragrafo precedente, vi è ulteriormente da indagare l'effettività della tutela giurisdizionale qualora si utilizzi il meccanismo di coerenza previsto dagli articoli 63 e seguenti del GDPR e, quindi, intervenga una decisione vincolante ex articolo 65. Si deve precisare che è, indubbiamente, consentito il ricorso verso la decisione finale dell'autorità di controllo. In relazione a questo caso, valgono i dubbi e le perplessità emerse nel paragrafo 2.6. Invece, ciò di cui si discute qui è la possibilità di agire – *direttamente* o *indirettamente*, come si vedrà – contro

93 Hofmann e Mustert, «Data protection» cit., p. 469.
94 Conclusioni dell'AG Bobek, causa C-645/19, *Facebook Ireland Limited e a.* cit., § 105.

la decisione vincolante presa dal comitato, al fine di ottenere l'annullamento della stessa. Il tema è rilevante, in quanto tale giudizio permetterebbe di lamentare la violazione delle norme rappresentate nei paragrafi precedenti, ad esempio la lesione dei diritti procedurali.[95]

Per raggiungere questo scopo, sono disponibili due opzioni: il ricorso per annullamento, di cui all'articolo 263 TFUE, oppure il rinvio pregiudiziale di validità ex articolo 267 TFUE. Per quanto riguarda la prima ipotesi, essa deve essere esaminata attentamente, in quanto la possibilità per gli individui – non rientrando questi ultimi nel novero dei cd. «ricorrenti privilegiati» – di proporre un ricorso per annullamento è di molto limitata dagli stringenti requisiti previsti dal paragrafo 4.[96]

Innanzitutto, si deve comprendere se la decisione vincolante del comitato sia un atto impugnabile, e quindi se rientri nella nozione di «atti degli organi o organismi dell'Unione destinati a produrre effetti giuridici nei confronti di terzi», prevista dal paragrafo 1 dell'articolo 263 TFUE. L'opinione del Tribunale, che qui si condivide, è che tale decisione sia, effettivamente, un atto di un organismo dell'Unione, essendo, peraltro, l'EPDB dotato di personalità giuridica.[97] Il primo problema sorge, però, in relazione alla necessità che tale atto produca effetti giuridici nei confronti di terzi. Infatti, osserva il Tribunale, è vero che esso produce effetti nei confronti dell'autorità di controllo, che sarà vincolata dalla decisione. Tuttavia, per giurisprudenza costante della Corte, è necessario – nel caso di legittimati non privilegiati – che l'atto produca tali effetti *proprio in relazione ai ricorrenti*.[98] Tale requisito, secondo la giurisprudenza, finisce per sovrapporsi con le condizioni fissate dal paragrafo 4,[99] le quali devono, quindi, essere ora esaminate.

La norma appena citata prevede tre ipotesi in presenza delle quali sussiste la legittimazione attiva di un individuo: (*i*) l'atto è adottato «nei suoi confronti»; (*ii*) l'atto, pur non essendo a lui indirizzato, lo riguarda «direttamente e individualmente»; (*iii*) si tratta di «atti regolamentari che la riguardano direttamente e che

95 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 816.

96 Il Tribunale dell'Unione europea si è pronunciato in un caso del tutto analogo in Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati*, ECLI:EU:T:2022:783, il cui giudizio di appello è attualmente pendente dinnanzi alla Corte: si v. Corte giust., causa C-97/23 P, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati*, pendente.

97 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 36.

98 Ivi, § 37-38.

99 Ivi, § 39 e Corte giust., sentenza del 13 ottobre 2011, cause riunite C-463/10 P e C-475/10 P, *Deutsche Post AG e Repubblica federale di Germania c. Commissione europea*, ECLI:EU:C:2011:656, § 38.

non comportano alcuna misura d'esecuzione».[100] La prima ipotesi è da scartare, in quanto la decisione vincolante è indirizzata alle autorità di controllo e non agli individui.

È necessario, quindi, concentrarsi sull'ipotesi *sub* (*ii*), la quale richiede la sussistenza di un interesse individuale e diretto. Secondo i giudici di Lussemburgo, nel caso di specie, l'atto impugnato deve considerarsi un atto individuale, in quanto esso «attiene a taluni aspetti di un progetto di decisione finale dell'autorità di controllo irlandese che [lo] riguarda specificamente».[101] Tuttavia, non si sa fino a che punto questa statuizione del Tribunale possa essere estesa ad altri casi simili. Infatti, qualora sia un interessato (reclamante) a voler presentare il ricorso, vi è il rischio che la sua posizione sia colpita dalla formula *Plaumann*, secondo la quale

> [c]hi non sia destinatario di una decisione può sostenere che questa lo riguarda individualmente soltanto qualora il provvedimento lo tocchi a causa di determinate qualità personali, ovvero di particolari circostanze atte a distinguerlo dalla generalità, e quindi lo identifichi alla stessa stregua dei destinatari.[102]

Ciò potrebbe accadere, in particolare, quando il ricorrente appartenga ad una categoria, anche molto ampia, di interessati, i quali siano tutti toccati in maniera pressoché identica dalla medesima violazione.[103] D'altra parte, però, bisogna anche considerare che chi presenta un reclamo si troverà in una posizione differente dalla generalità, *quantomeno quando lamenti dei vizi procedurali*, quali ad esempio la violazione del diritto ad essere ascoltati, visto che esso è attribuito *solo a chi è parte del procedimento*. In simili casi, la Corte ha ritenuto che, se sia prescritto – in questo caso, si potrebbe affermare, ad opera dell'articolo 41 della Carta – che sia garantita la partecipazione di taluni soggetti, si presume che tali soggetti abbiano un interesse qualificato.[104]

Il nocciolo principale della questione sembra però essere la sussistenza di un interesse *diretto* o, in altre parole, «se la decisione impugnata produca effetti giuridici che modifichino in modo significativo la situazione giuridica della [ricorrente] e se riguardi direttamente quest'ultima ai sensi dell'articolo 263, quarto

100 L. Daniele, *Diritto dell'Unione europea: sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Settima edizione, Giuffrè, Milano 2020, p. 382-395.

101 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 40.

102 Corte giust., sentenza del 15 luglio 1963 (Grande Sezione), causa 25-62, *Plaumann & Co. c. Commissione della Comunità economica europea*, ECLI:EU:C:1963:17.

103 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 817.

104 Daniele, *Diritto dell'Unione europea* cit., p. 389-390; in giurisprudenza v. Corte giust., sentenza del 28 gennaio 1986, causa 169/84, *Compagnie française de l'azote (Cofaz) SA ed altri c. Commissione delle Comunità europee*, ECLI:EU:C:1986:42.

comma, TFUE».[105] Qui, il problema è che la decisione del comitato è un atto *preparatorio* o *intermedio* di un procedimento che si conclude con la decisione dell'autorità di controllo competente.[106] Per giurisprudenza costante della Corte, simili «provvedimenti provvisori diretti a preparare la decisione finale» non sono autonomamente impugnabili,[107] a meno che il provvedimento provvisorio non produca effetti giuridici autonomi in relazione ai quali non sia possibile assicurare una tutela giurisdizionale effettiva *mediante l'impugnazione dell'atto che conclude il procedimento*.[108] Nel caso di specie, la Corte ritiene però che tale eccezione non sussista, in quanto

> una tutela giurisdizionale effettiva nei confronti della decisione impugnata è, invece, assicurata alla [ricorrente] dai rimedi esperibili contro la decisione finale dell'autorità di controllo irlandese dinanzi al giudice nazionale, rimedi che consentono di esaminare la legittimità della decisione impugnata.[109]

Pertanto, non si ritiene praticabile la possibilità concessa dall'articolo 263 TFUE e il ricorso viene dichiarato irricevibile. In aggiunta, si può anche affermare che nemmeno l'ipotesi *sub* (*iii*) sembra essere praticabile, in quanto non appaiono soddisfatte nessuna delle due condizioni da essa postulate. Infatti, (*i*) secondo la giurisprudenza *Inuit*,[110] affinché un atto possa essere considerato «atto regolamentare», esso deve avere *portata generale* e, quindi, produrre «i suoi effetti giuridici nei confronti di categorie di persone considerate in maniera generale e astratta».[111] La decisione vincolante dell'EPDB che venga adottata a seguito della presentazione

105 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 41.

106 Ivi, § 42.

107 Corte giust., sentenza del 19 dicembre 2018 (Grande Sezione), causa C-219/17, *Silvio Berlusconi e Finanziaria d'investimento Fininvest SpA (Fininvest) c. Banca d'Italia e Istituto per la Vigilanza Sulle Assicurazioni (IVASS)*, ECLI:EU:C:2018:1023, § 47-51; Corte giust., sentenza del 26 gennaio 2010 (Grande Sezione), causa C-362/08 P, *Internationaler Hilfsfonds eV c. Commissione europea*, ECLI:EU:C:2010:40, § 52.

108 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 44; Corte giust., cause riunite C-463/10 P e C-475/10 P, *Deutsche Post e Germania/Commissione* cit., § 53-54; Corte giust., sentenza del 23 settembre 1986, causa 5/85, *AKZO Chemie BV e AKZO Chemie UK Ltd c. Commissione delle Comunità europee*, ECLI:EU:C:1986:328, § 20.

109 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 45.

110 Corte giust., sentenza del 3 ottobre 2013 (Grande Sezione), causa C-583/11 P, *Inuit Tapiriit Kanatami e altri c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:2013:625, § 56-61.

111 Corte giust., sentenza del 6 novembre 2018 (Grande Sezione), cause riunite da C-622/16 P a C-624/16 P, *Scuola Elementare Maria Montessori Srl c. Commissione europea, Commissione europea c. Scuola Elementare Maria Montessori Srl e Commissione europea c. Pietro Ferracci*, ECLI:EU:C:2018:873, § 29.

di un reclamo non pare poter essere sussunta in questa fattispecie, visto che essa produce effetti giuridici nei confronti di persone determinate. Inoltre, (*ii*) sarebbe necessario che tale atto non comporti *alcuna misura d'esecuzione*. Al contrario, come già spiegato in questo elaborato (v. *supra* par. 2.4) e come sostenuto anche dal Tribunale nel caso *WhatsApp Ireland*, l'autorità di controllo capofila esercita la propria discrezionalità «nel trarre le conseguenze dalle istruzioni impartite nella decisione impugnata».[112]

A questo punto, vi è un ultimo elemento da analizzare: il considerando 143 del GDPR. Esso si presenta come potenzialmente dirompente se confrontato con quanto sinora affermato dalla giurisprudenza. Infatti, esso afferma che

> [q]ualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla loro notifica, conformemente all'articolo 263 TFUE. Ove le decisioni del comitato si riferiscano direttamente e individualmente a un titolare del trattamento, a un responsabile del trattamento o al reclamante, quest'ultimo può proporre un ricorso per l'annullamento di tali decisioni e dovrebbe farlo entro due mesi dalla loro pubblicazione sul sito web del comitato, conformemente all'articolo 263 TFUE.

Visti i numerosi problemi appena presentati circa la legittimazione attiva, vi è da chiedersi a cosa stesse pensando il legislatore quando ha redatto questo considerando. In particolare, sembra difficile pensare, in assoluto, ad una decisione del comitato che sia indirizzata ad un individuo o per cui tale individuo sia direttamente ed individualmente interessato, visto che tali decisioni sono *sempre rivolte alle autorità di controllo*[113] e, quindi, difetterà il requisito dell'interesse diretto. Di certo il legislatore non ha affermato nulla di sbagliato, visto che egli subordina il ricorso per annullamento alla sussistenza delle condizioni di cui all'articolo 263. Forse, però la porzione del considerando appena citata rischia, questo sì, di non riferirsi ad alcuna fattispecie riscontrabile nella realtà. Dal canto suo, il Tribunale ricorda che un considerando «non può costituire di per sé una norma di tal genere e che il preambolo di un atto dell'Unione non ha valore giuridico vincolante»[114] e che

> nella specie, il considerando de quo non costituisce il fondamento di alcuna disposizione del regolamento 2016/679, come rilevato supra ai punti 32 e 35. Inoltre, una spiegazione

112 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 57-60.

113 Hofmann e Mustert, «Data protection» cit., p. 469; Hijmans, «Article 65» cit., p. 1025.

114 Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati* cit., § 71.

> contenuta nella motivazione di un regolamento non può prevalere sulle norme applicabili di diritto primario contenute nei Trattati, nella specie su quelle di cui all'articolo 263, primo e quarto comma, TFUE, la cui sostanza è peraltro parzialmente richiamata nel considerando in questione con l'indicazione, nella prima frase, che «[q]ualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE».[115]

La soluzione proposta dalla Corte è, invece, l'utilizzo dello strumento del rinvio pregiudiziale di validità. Infatti, i giudici osservano che la tutela giurisdizionale effettiva appena citata può essere ottenuta impugnando la decisione finale dell'autorità di controllo nazionale davanti al giudice nazionale, facendo valere un vizio di cd. «illegittimità derivata»:[116] il provvedimento nazionale sarebbe illegittimo, in quanto basato su un'illegittima decisione vincolante presa dall'EPDB. A questo punto, il giudice nazionale può – o, *rectius* (come si vedrà) *deve*, ancorché non giudice di ultima istanza – effettuare un rinvio pregiudiziale di validità e, così, permettere alla Corte di Giustizia di verificare la sussistenza di uno dei vizi previsti dall'articolo 263, paragrafo 2, TFUE. A tal riguardo, si deve precisare che, secondo il principio *Foto-Frost*, è escluso che sia il giudice nazionale stesso ad accertare l'invalidità della decisione vincolante, in quanto essa è un atto di un organismo dell'Unione.[117] Tale giudice, se ritiene fondata la doglianza, è invece *tenuto* ad effettuare il rinvio.[118] Ciò è ribadito anche dal considerando 143 del GDPR, secondo cui:

> […] se una decisione dell'autorità di controllo che attua una decisione del comitato è impugnata dinanzi a un'autorità giurisdizionale nazionale ed è in questione la validità della decisione del comitato, tale autorità giurisdizionale nazionale non ha il potere di invalidare la decisione del comitato, ma deve deferire la questione di validità alla Corte di giustizia ai sensi dell'articolo 267 TFUE quale interpretato dalla Corte di giustizia, ove ritenga la decisione non valida. […]

La dottrina si sofferma anche sulla possibilità che – in ossequio al principio stabilito nella nota sentenza *TWD Textilwerke Deggendorf*[119] – tale rinvio non

115 Ibidem.

116 F. Brito Bastos, «Derivative illegality in European composite administrative procedures», *Common Market Law Review*, 55, 1 (2018), p. 104 afferma che «*it is incontrovertibly possible that a preparatory measure adopted at EU level "contaminates" a subsequent final decision taken at national level*».

117 Corte giust., sentenza del 22 ottobre 1987, causa 314/85, *Foto-Frost c. Hauptzollamt Lübeck-Ost*, ECLI:EU:C:1987:452, § 15-19; proprio in relazione alla tutela dei dati personali v. Corte giust., causa C-362/14, *Schrems*, cit., § 61-62.

118 Corte giust., sentenza del 10 gennaio 2006 (Grande Sezione), causa C-344/04, *The Queen, ex parte International Air Transport Association e European Low Fares Airline Association c. Department for Transport*, ECLI:EU:C:2006:10, § 32.

119 Corte giust., sentenza del 9 marzo 1994, causa C-188/92, *TWD Textilwerke Deggendorf GmbH c. Repubblica Federale di Germania*, ECLI:EU:C:1994:90, § 26.

sia, tuttavia, possibile, in quanto il ricorrente abbia lasciato spirare il termine di due mesi previsto dall'articolo 263, paragrafo 6, TFUE, senza proporre ricorso di annullamento.[120] Tuttavia, la questione non appare come la più preoccupante, visto che – come rileva la stessa dottrina[121] – il principio *TWD* si applica solamente quando l'individuo «avrebbe potuto *senza alcun dubbio*» impugnare l'atto.[122] Viste le varie discussioni appena enunciate e i dubbi presentati dal Tribunale in *WhatsApp Ireland*, non sembra si possa rientrare in questo caso.

In conclusione, di certo la soluzione prospettata dal Tribunale si presenta in continuità con quanto affermato dalla Corte di Giustizia nel corso degli anni: la giurisprudenza non è mai stata permissiva nell'ammettere ricorsi diretti di annullamento da parte dei singoli. Ciò deve accompagnarsi, però, ad una critica: in relazione ai cd. provvedimenti "compositi", categoria in cui rientra la decisione finale dell'autorità di controllo, la dottrina ha sottolineato come sia più difficile garantire una tutela giurisdizionale effettiva.[123] Eliantonio fa presente che tale problema si manifesta con minore intensità proprio nelle procedure miste – come quella in esame – in cui il provvedimento preparatorio è preso a livello europeo e quello finale a livello nazionale, proprio in ragione della disponibilità del rimedio di cui all'articolo 267.[124] Tuttavia, come precisato dalla stessa, ciò non risolve tutti i vuoti di tutela, ad esempio perché il giudice nazionale potrebbe avere difficoltà a discernere quale sia l'effettivo contributo "comunitario" alla decisione nazionale e, quindi, stentare a capire cosa sia soggetto a *Foto-Frost* e cosa no.[125] Inoltre, il diritto ad una tutela giurisdizionale effettiva potrebbe essere pregiudicato qualora, impugnato il provvedimento finale, l'azione intentata non sia idonea a rilevare errori relativi a livelli diversi da quello in cui si prende la decisione e, allo stesso tempo, non siano dati rimedi nei confronti degli altri stadi del procedimento.[126]

120 Kotschy, «Article 78» cit., p. 1131.

121 Ibidem.

122 Corte giust., causa C-188/92, *TWD Textilwerke Deggendorf* cit., § 24.

123 M. Eliantonio, «Access to Justice in Composite Procedures for the Implementation of EU Law: the Story so Far», in *Questions choisies de droit européen des affaires / Selected Issues in European Business Law*, a cura di P. Van Creynenbreugel e J. Wildemeersch, Bruylant, Bruxelles 2023; Eliantonio e Vogiatzis, «Judicial and Extra-Judicial Challenges» cit.; Hofmann, «Multi-Jurisdictional Composite Procedures» cit.

124 Eliantonio, «Access to Justice in Composite Procedures» cit.

125 Ivi.

126 M. Eliantonio, «Judicial Review in an Integrated Administration: the Case of 'Composite Procedures'», *Review of European Administrative Law*, 7, 2 (2015), p. 78: «*Furthermore, if the challenge is directed towards the final measure of the decision-making process (and assuming that the applicant is challenging a reviewable act and has standing to bring the claim), the action may not be able to cover errors which occurred at other levels than the one which took the final decision, while, at the same time, access to court is barred for all the steps which took place before the final measure was issued*».

Anche Brito Bastos, definendo le procedure composite come «*an administrative crack in the EU's rule of law*» sottolinea come «*[c]omposite administrative procedures therefore generate, at the level of the member states, a serious gap from the point of view of three key requirements of the European Union's rule of law: the effective judicial protection of individuals, the judicial control of (national) public power, and the principle of administrative legality*».[127]

Infine, bisogna ricordare che, dal punto di vista procedurale, due rimedi analizzati non hanno un carattere completamente sovrapponibile in termini di tutela nei confronti dell'individuo. Infatti, ciò è vero quantomeno perché (*i*) solo il ricorso ex articolo 263 è veramente *a disposizione* del singolo[128] e (*ii*) rende disponibile un contraddittorio pieno con due gradi di giudizio.[129] Detto ciò, non sembra però che i vuoti di tutela giurisdizionale siano di enormità paragonabile a taluni casi – quali *Les Verts*[130] o *Chernobyl*[131] – che hanno portato la Corte a forzare l'interpretazione dei Trattati, ammettendo ricorsi per annullamento che, limitandosi ad una lettura letterale, parevano carenti di legittimazione. Anzi, tenendo conto di *Georgsmarienhütte*,[132] l'atteggiamento della Corte pare divenuto, addirittura, più restrittivo.

2.8 *I problemi relativi all'applicazione del GDPR nei procedimenti* non *transfrontalieri*

Prima di procedere verso la conclusione, si ritiene opportuno presentare alcuni dei problemi che l'applicazione del GDPR pone con riferimento ai procedimenti *non* transfrontalieri. Infatti, tale analisi è comunque utile, in quanto questi ultimi, pur non implicando la necessità che un certo caso concreto sia deciso concordemente tra più Stati membri, sono comunque rivelatori di un diverso trattamento di

127 F. Brito Bastos, «An Administrative Crack in the EU's Rule of Law: Composite Decision-making and Nonjusticiable National Law», *European Constitutional Law Review*, 16, 1 (2020), p. 65.

128 B. Cortese, «Rinvio pregiudiziale e ricorso di annullamento: parallelismi, intersezioni e differenze», in *Il rinvio pregiudiziale*, a cura di F. Ferraro e C. Iannone, Giappichelli, Torino 2020, p. 246.

129 Ivi, p. 248, 259.

130 Corte giust., sentenza del 23 aprile 1986, causa 294/83, *Parti écologiste "Les Verts" c. Parlamento europeo*, ECLI:EU:C:1986:166, § 35-38.

131 Corte giust., sentenza del 22 maggio 1990, causa C-70/88, *Parlamento europeo c. Consiglio delle Comunità europee*, ECLI:EU:C:1990:217.

132 Corte giust., sentenza del 25 luglio 2018 (Grande Sezione), causa C-135/16, *Georgsmarienhütte GmbH e a. c. Bundesrepublik Deutschland*, ECLI:EU:C:2018:582.

medesime situazioni giuridiche e fattuali, a seconda di quale sia l'Autorità di controllo cui l'interessato si deve rivolgere.[133]

Una prima differenza[134] attiene alle diverse condizioni di ammissibilità del reclamo presentato dall'interessato ex articolo 77 GDPR: *(i)* alcune autorità richiedono che il reclamo sia presentato con determinate formalità. Ad esempio, il Garante per la protezione dei dati personali impone che il reclamo sia obbligatoriamente presentato mediante posta elettronica certificata, raccomandata con ricevuta di ritorno o consegna a mano, escludendone l'invio tramite semplice email.[135] Ciò differisce dalla prassi di altre autorità: ad esempio, l'*Autoriteit Persoonsgegevens* (Autorità di controllo dei Paesi Bassi) permette di inviare il reclamo compilando un modulo online,[136] e così anche il *Datenschutzbehörde* (Austria)[137]; l'*Autorité de protection des données - Gegevenbeschermingsautoriteit* (Belgio) permette di caricare un modulo in formato .pdf sul proprio sito.[138] La *Commission nationale de l'informatique et des libertés* (Francia) permette di inviare il reclamo attraverso un modulo online[139], tuttavia richiede dapprima di creare un account – operazione possibile, lodevolmente, anche ai non cittadini francesi – o di utilizzare il sistema di identità digitale *FranceConnect*. Inoltre, viene richiesto di classificare il proprio reclamo all'interno di una delle categorie previste: qualora il proprio problema non rientri all'interno di queste categorie, viene domandato di contattare il «servizio di aiuto in linea».[140] È evidente che una prassi simile a quella dell'Autorità

133 H. C. Hofmann e L. Mustert, «Procedures Matter – What to Address in GDPR Reform and a new GDPR Procedural Regulation», *University of Luxembourg Law Research Paper*, 2 (2023), p. 2.

134 Per una sistematizzazione completa di queste differenze si veda il documento redatto da *NOYB - European Center for Digital Rights* al seguente link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation/F3390245_en (visitato il 22/02/2024). Molto utile è anche lo studio effettuato da G. González Fuster et al., *The right to lodge a data protection complaint : ok, but then what? An empirical study of current practices under the GDPR*, rapp. tecn., Data Protection Law Scholars Network (DPSN), Access Now, Fiesole 2022.

135 Si v. la corrispondente pagina sul sito del Garante: https://www.garanteprivacy.it/diritti/come-agire-per-tutelare-i-tuoi-dati-personali/reclamo (visitato il 22/02/2024).

136 Disponibile al seguente link https://klachten.autoriteitpersoonsgegevens.nl/ (visitato il 22/02/2024).

137 https://www.dsb.gv.at/Eingabeformular-online/Eingabeformular-online.html (visitato il 22/02/2024).

138 https://www.autoriteprotectiondonnees.be/citoyen/agir/introduire-une-plainte (visitato il 22/02/2024).

139 https://www.cnil.fr/fr/plaintes

140 Viene restituito il seguente messaggio: «*Votre problème n'est pas listé parmi ces cas de plaintes ? Vous pensez qu'il s'agit bien d'un manquement à la règlementation en matière de protection des données à caractère personnel ? Vérifiez d'abord si une réponse à votre problème existe dans notre service d'aide en*

italiana finisce per rendere più gravoso l'esercizio del diritto, in quanto non tutti i cittadini sono dotati di PEC (strumento che, peraltro, non esiste negli altri Stati membri), per ottenere la quale è necessario pagare un corrispettivo. Peraltro, tale prassi si pone in contrasto con la norma di cui all'articolo 57, paragrafo 2, GDPR, la quale impone alle autorità di controllo di agevolare la proposizione dei reclami «tramite misure quali un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione».[141]

(*ii*) Inoltre, altre autorità pongono come condizione di ammissibilità il previo esercizio dei diritti previsti dagli articoli da 15 a 22 del GDPR. A tal riguardo, è necessario notare che l'articolo 77, paragrafo 1, GDPR pone come unica condizione per l'esercizio del diritto di presentare un reclamo il fatto che l'interessato «ritenga che il trattamento che lo riguarda violi il [GDPR]». Pertanto, si ritiene che l'apposizione di tale ulteriore condizione di ammissibilità, non trovando un sottostante elemento di diritto positivo, sia da considerarsi non conforme con il regolamento.[142] Peraltro, ciò ha la conseguenza di ritardare il momento in cui può essere presentato il reclamo di almeno un mese, ossia il tempo, previsto dall'articolo 12, paragrafo 3, GDPR, entro il quale il titolare deve rispondere alla richiesta di accesso.[143] Tale prassi non affligge però il Garante italiano, in quanto l'articolo 15, comma 3, del Regolamento 1/2019[144] prevede che il reclamante – che non abbia ancora esercitato i diritti di cui agli articoli da 15 a 22 GDPR – sia invitato a rivolgersi al titolare del trattamento, ma *solamente quando il reclamo stesso lamenti la violazione proprio di tali diritti*.

Questi pochi esempi pratici sono, dunque, rivelatori del fatto che un medesimo diritto – in questo caso, quello di cui all'articolo 77 – è sottoposto a diversi standard di tutela, a seconda di quella che sia l'Autorità di controllo adita. E ciò nonostante la norma del diritto dell'Unione non sia contenuta in una direttiva, ma in un regolamento, conferendo così efficacia diretta al diritto in essa previsto.

Tuttavia, bisogna ricordare che – in relazione alla determinazione delle modalità di «tutela dei diritti spettanti ai singoli in forza delle norme comunitarie *aventi*

ligne.» e non sembra possibile continuare con il reclamo.

141 González Fuster et al., *The right to lodge a data protection complaint* cit., p. 10-11.

142 In questo senso v. Tribunal Supremo, sentenza del 19 luglio 2022, n. 1039/2022, ECLI:ES:TS:2022:3207.

143 Si v. il documento di *NOYB* cit.

144 Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con Deliberazione del 4 aprile 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9107633.

efficacia diretta»[145] – vige il principio di autonomia istituzionale (o procedurale). Si tratta di un principio in vigore anche in questo caso, in quanto in sede di redazione del GDPR si è ritenuto di non armonizzare le norme procedurali, reputando che queste ultime ricadessero all'interno della competenza degli Stati membri.[146]

Preliminarmente, è necessario precisare che tale principio cardine, ad onor del vero, si è sviluppato in seno alla Corte quasi esclusivamente in relazione a questioni di natura processuale, e non – come nel caso in esame – relative alla disciplina del procedimento amministrativo. Tuttavia, la dottrina ritiene che, pur esistendo delle sottili differenze tra il principio di «autonomia procedurale» e quello di «autonomia istituzionale», le due nozioni siano pressoché coincidenti.[147] Inoltre, è stato osservato[148] che la Corte, con riferimento alla disciplina del procedimento amministrativo,[149] ha ripreso la medesima posizione (che verrà di seguito illustrata) dapprima adottata per quanto riguarda l'autonomia procedurale in senso stretto.[150] Nel caso *Rewe*, la Corte, da una parte, ha affermato che

> in mancanza di una specifica disciplina comunitaria, è l'ordinamento giuridico interno di ciascuno Stato membro che designa il giudice competente e stabilisce le modalità procedurali delle azioni giudiziali intese a garantire la tutela dei diritti spettanti ai singoli in forza delle norme comunitarie aventi efficacia diretta.[151]

D'altra parte, essa osserva che tale principio non è assoluto, in quanto esso vale purché siano rispettati (*i*) il principio di equivalenza e (*ii*) il principio di effettività.[152] In base al primo, per continuare ad usare le parole della Corte in *Rewe*, le modalità definite dal diritto nazionale «non possono […] essere meno favorevoli di quelle relative ad analoghe azioni del sistema processuale nazionale». Il secondo

145 Corte giust., sentenza del 16 dicembre 1976, 33/76, *Rewe-Zentralfinanz eG e Rewe-Zentral AG contro Landwirtschaftskammer für das Saarland*, ECLI:EU:C:1976:188, § 5, corsivo aggiunto.

146 L. C. Drechsler, «Op-Ed: "Walking the line between procedural autonomy and effective legal remedies in the General Data Protection Regulation (C-132/21, *Nemzeti Adatvédelmi és Információszabadság Hatóság*)"», *EU Law Live* (gennaio 2023).

147 Si v. D.-U. Galetta e J. Ziller, «L'independance des juges et le droit de l'Union Européenne du point de vue l'autonomie istitutionnelle (et procedurale) des etats membres», in *Les valeurs de l'Union Européenne*, a cura di F. Péraldi Leneuf, Pedone, Paris 2020, secondo cui «*les deux notions coïncident […] au moins en ce qui concerne leur raison d'être et la structure de raisonnement qui les caractérise. C'est-à-dire que, même si ce n'est pas exactement de la même chose qu'il s'agit, les deux sont néanmoins très étroitement liées, de telle manière qu'il ne vaut pas la peine d'essayer de le séparer d'une manière artificielle*».

148 R. Widdershoven, «National Procedural Autonomy and General EU Law Limits», *Review of European Administrative Law*, 12, 2 (2019), p. 9.

149 Corte giust., causa C-349/07, *Sopropé* cit., § 38.

150 *Ex multis* v. Corte giust., causa 33/76, *Rewe*, cit.

151 Ivi, § 5.

152 Daniele, *Diritto dell'Unione europea* cit., p. 320.

principio, invece, prevede che tali modalità non possano essere tali da rendere praticamente impossibile o eccessivamente difficile l'esercizio di diritti derivanti da norme dell'Unione.[153]

Ora, tornando al diritto della protezione dei dati, si può affermare che il primo di questi principi non venga in rilievo, in quanto – essendo la materia completamente uniformata a seguito dell'entrata in vigore del GDPR – non è possibile effettuare una distinzione tra diritto comunitario e diritto interno, poiché tutti i diritti in materia di protezione dei dati sono attribuiti dal diritto dell'Unione. L'esame della questione dovrà quindi concentrarsi sul principio di effettività. A questo proposito, la Corte ha affrontato il tema dell'autonomia procedurale in relazione al diritto della protezione dei dati un'unica volta, nella causa *Budapesti Elektromos Művek*.[154] Il caso di specie verteva sul rapporto tra il diritto di presentare un reclamo (art. 77 GDPR), quello ad un ricorso giurisdizionale effettivo contro l'autorità di controllo (art. 78 GDPR) e contro il titolare del trattamento (art. 79 GDPR). Si tratta, quindi, di un ambito diverso da quello oggetto del presente paragrafo. Tuttavia, è comunque utile richiamare alcuni passi della sentenza, in particolare ove si ricorda che

> [i]n assenza di una disciplina dell'Unione in materia, spetta a ciascuno Stato membro, in forza del principio di autonomia processuale degli Stati membri, stabilire le modalità delle procedure amministrative e quelle relative alla procedura giurisdizionale intese a garantire la tutela dei diritti spettanti agli amministrati in forza del diritto dell'Unione.[155]
>
> Ciò premesso, le modalità di attuazione […] non dovrebbero mettere in discussione l'effetto utile e la tutela effettiva dei diritti garantiti da tale regolamento.[156]
>
> Infatti, tali modalità non devono essere meno favorevoli di quelle che riguardano ricorsi simili previsti per la protezione dei diritti che derivano dall'ordine giuridico interno (principio di equivalenza), né essere strutturate in modo da rendere in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dall'ordinamento giuridico dell'Unione (principio di effettività).[157]

Invece, non vi è giurisprudenza che si sia pronunciata circa i limiti posti dalle autorità di controllo per l'esercizio del diritto alla presentazione di un reclamo. Resta, quindi, da vedere che atteggiamento adotterà la Corte qualora dovesse valutare la rispondenza delle prassi presentate in questo paragrafo con il principio di effettività. Quello che si può dire è che, di sicuro, esse rendono *più difficile*

153 Ibidem.
154 Corte giust., sentenza del 12 gennaio 2023, causa C-132/21, *BE c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2023:2.
155 Ivi, § 45.
156 Ivi, § 46.
157 Ivi, § 50.

l'esercizio del diritto. Il tema che i giudici dovranno, eventualmente, affrontare è se esse raggiungano, però, la soglia dell'*eccessiva* difficoltà.

Peraltro, la dottrina ha sottolineato come il principio di autonomia procedurale valga solo in assenza di norme di diritto dell'Unione che disciplinino la stessa materia:[158] tralasciando qui la questione del se il legislatore europeo sia autorizzato ad intervenire in una certa materia ai sensi dell'articolo 5 TUE, si può affermare che – una volta che esso sia intervenuto con una norma in contrasto con il diritto nazionale – quest'ultima vada disapplicata in forza del principio del primato del diritto dell'Unione.[159] Questa osservazione si ritiene possa valere almeno in relazione al caso sub (*ii*) appena presentato: le norme (o le prassi) nazionali che prevedono ulteriori requisiti per la presentazione del reclamo diversi da quelli di cui all'articolo 77 GDPR si pongono in contrasto *diretto* con una fonte di diritto comunitario, e pertanto andrebbero disapplicate sia dai giudici che dalle autorità di controllo[160] nazionali. La medesima conseguenza si potrebbe trarre in relazione alla norma di cui all'articolo 57, paragrafo 2, GDPR, circa la mancata messa a disposizione di un modulo elettronico per la proposizione dei reclami.[161]

2.9 *Le possibili soluzioni: il ruolo della Commissione*

I problemi sinora enunciati sono molti e complessi, e di conseguenza complesse sono anche le loro soluzioni. Di seguito si tenterà però di proporre degli spunti di riflessione su alcuni modi con cui questi problemi potrebbero essere risolti.

Una prima soluzione, proposta da Gentile e Lynskey, parte dalla constatazione per cui, ex articolo 17 TUE, la Commissione, in qualità di guardiana dei Trattati, deve vigilare affinché gli Stati membri non violino le obbligazioni derivanti dal diritto primario.[162] Per far ciò, l'articolo 258 TFUE le attribuisce il potere di promuovere un ricorso per infrazione dinnanzi alla Corte di Giustizia. Si tratta quindi dell'esercizio di una competenza generale della Commissione, derivante direttamente dal Trattato sul funzionamento, e non da diritto secondario dell'Unione

158 Widdershoven, «National Procedural Autonomy» cit., p. 13.

159 Si v. ibidem che richiama Corte giust., sentenza del 18 luglio 2007 (Grande Sezione), causa C-119/05, *Ministero dell'Industria, del Commercio e dell'Artigianato c. Lucchini SpA*, ECLI:EU:C:2007:434, § 61.

160 Corte giust., causa C-119/05, *Lucchini* cit., § 39; Corte giust., sentenza del 9 settembre 2003, causa C-198/01, *Consorzio Industrie Fiammiferi (CIF) c. Autorità Garante della Concorrenza e del Mercato*, ECLI:EU:C:2003:430, § 49; Corte giust., sentenza del 22 giugno 1989, causa 103/88, *Fratelli Costanzo SpA c. Comune di Milano*, ECLI:EU:C:1989:256, § 31.

161 Più in generale, sul tema si v. González Fuster et al., *The right to lodge a data protection complaint* cit., p. 16-17.

162 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 826.

e, segnatamente, dal GDPR. Infatti, esso non prevede, almeno con riferimento all'ambito in esame,[163] alcun ruolo significativo della Commissione.

Si è consapevoli che si tratta, probabilmente, di una sorta di *extrema ratio*, stante il grado di conflittualità istituzionale che essa normalmente comporta. Inoltre la valutazione circa l'attivazione o meno della procedura di infrazione è rimessa all'esclusiva discrezionalità della Commissione,[164] ed implica dunque elementi di natura politica oltre che giuridica.

Tuttavia, si ritiene che si tratti comunque di una soluzione percorribile: il considerando 135 del GDPR precisa che «[t]ale meccanismo [di coerenza] non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati». Inoltre, ad essa non osta il fatto che l'infrazione sia commessa non dal potere esecutivo dello Stato, ma da un'articolazione, quale l'autorità per la protezione dei dati, che gode (o dovrebbe godere) di completa indipendenza dal governo. Infatti, per giurisprudenza costante della Corte,[165] lo Stato membro è chiamato a rispondere anche in relazione a comportamenti imputabili a poteri indipendenti rispetto a quello esecutivo.[166]

È possibile concentrarsi su due ordini di violazioni che potrebbero dare origine alla procedura di infrazione.[167] Un primo ambito riguarda la condotta di quelle autorità di controllo che, dinnanzi ad una determinata violazione, ritengono – in maniera assolutamente discrezionale – di non agire o di agire solo parzialmente. Si tratta di un fenomeno sovrapponibile al cd. «*selective enforcement*»: una certa autorità focalizza le proprie risorse solo su particolari settori o certi tipi di titolari del trattamento.[168] Tale atteggiamento è criticabile e viola il diritto comunitario sia primario che derivato. Infatti, non solo le autorità sono competenti ad esercitare i poteri di cui alla sezione 2 del capo VI, ma hanno l'*obbligo* di esercitarli.[169]

163 La Commissione ha, invece, un ruolo più preminente con riferimento ad altri ambiti del GDPR. Si pensi, ad esempio, al potere di approvare una decisione di adeguatezza ex articolo 45 GDPR.

164 Daniele, *Diritto dell'Unione europea* cit., p. 366; in giurisprudenza *ex multis* v. Corte giust., ordinanza del 28 gennaio 2015, causa C-411/14 P, *Romano Pisciotti c. Commissione europea*, ECLI:EU:C:2015:48, § 11; Corte giust., sentenza del 14 febbraio 1989, causa 247/87, *Star Fruit Company SA c. Commissione delle Comunità europee*, ECLI:EU:C:1989:58, § 11.

165 Corte giust., sentenza del 4 ottobre 2018, causa C-416/17, *Commissione europea c. Repubblica francese (anticipo d'imposta)*, ECLI:EU:C:2018:811, § 107; Corte giust., sentenza del 9 dicembre 2003, causa C-129/00, *Commissione delle Comunità europee c. Repubblica italiana*, ECLI:EU:C:2003:656, § 29; Corte giust., sentenza del 5 maggio 1970, causa 77/69, *Commissione delle Comunità europee c. Regno del Belgio*, ECLI:EU:C:1970:34, § 15.

166 Daniele, *Diritto dell'Unione europea* cit., p. 360.

167 Ricordando comunque che l'oggetto del ricorso può riguardare il mancato rispetto di un qualsiasi obbligo di diritto primario o secondario dell'Unione, salvo eccezioni, v. ivi, p. 361-364.

168 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 820.

169 H. Hijmans, «Article 55 Competence», in *The EU General Data Protection Regulation (GDPR): A*

Ciò risulta dal tenore letterale della norma di cui all'articolo 57, paragrafo 1: se la versione italiana o francese non sono particolarmente chiarificatrici, ciò emerge più limpidamente da quella inglese («each supervisory authority *shall* on its territory»)[170] e tedesca («*muss* jede Aufsichtsbehörde in ihrem Hoheitsgebiet»). Giustamente, Hijmans osserva che, poiché le autorità non sono dotate di infinite risorse economiche e di personale, esse devono – anche in ragione della loro indipendenza – necessariamente stabilire delle priorità, in maniera tale da agire con effettività.[171] Tuttavia, si ritiene che la definizione delle priorità debba comunque avvenire in maniera ragionevole; ad esempio, concentrandosi sulle violazioni ritenute più gravi e che raggiungono un numero molto elevato di interessati.

È vero che la Corte ha esplicitamente stabilito che la discrezionalità dell'autorità sia limitata solo in un caso – ossia quando si tratti di esaminare un reclamo – osservando che «incombe [su] tale autorità [il dovere di] esaminare detta domanda *con tutta la diligenza richiesta*»[172] (v. *supra* par. 2.3.3). Tuttavia, non sembra possibile affermare che, al di fuori dell'ambito dei reclami, le autorità possano determinare le priorità in maniera completamente libera: ciò potrebbe trasformarsi in un comportamento arbitrario, di sicuro non consentito.[173] Esse devono essere consapevoli che – nel quadro attuale, in cui la disciplina è dettata da una fonte di natura regolamentare – non stanno più attuando il diritto nazionale, ma sono «*agents of European law*».[174] In questo senso, discende dal principio di leale collaborazione, di cui all'articolo 4, paragrafo 3, TUE, l'obbligo in capo alle stesse di (*i*) astenersi dal facilitare la violazione del diritto dell'Unione[175] e di (*ii*) assicurare che il diritto comunitario venga efficacemente implementato.[176] Afferma la Corte,

Commentary, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 907; H. Hijmans, «Article 57 Tasks», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020, p. 933.

170 L. Mustert, «The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?», *European Data Protection Law Review*, 9, 4 (2023), p. 455.

171 Hijmans, «Article 57» cit., p. 933-934.

172 Corte giust., causa C-362/14, *Schrems* cit., § 63.

173 H. Hijmans, «Understanding the Role of Independent, Effective and Accountable DPAs: New Branches of Government in Between the Union and the Member States», in *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, a cura di H. Hijmans, Springer International Publishing, Cham 2016, p. 384.

174 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 821.

175 J. Temple Lang, «The Principle of Sincere Cooperation, the Charter and Digitalisation», in *General principles of EU law and the EU digital order*, a cura di U. Bernitz et al., Kluwer Law International, Alphen aan den Rijn 2020, p. 41.

176 In dottrina v. ivi, p. 36; in giurisprudenza v. Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit., § 53: «Secondo una giurisprudenza costante, in forza di tale principio, nelle materie rientranti nel diritto dell'Unione, gli Stati membri, ivi incluse

nel caso *Facebook Ireland e Schrems*, che l'autorità «è tenuta, *in applicazione del diritto dell'Unione*, a reagire in modo appropriato al fine di porre rimedio all'inadeguatezza constatata, e ciò indipendentemente dall'origine o dalla natura di tale inadeguatezza»,[177] precisando che «[b]enché la scelta del mezzo appropriato e necessario spetti all'autorità di controllo, […] detta autorità *è comunque tenuta ad assolvere al suo compito di vigilare sul pieno rispetto del RGPD con tutta la diligenza richiesta*».[178] Nonostante ciò sia stato osservato con riferimento a casi originati dalla presentazione di reclami, si ritiene che le parole siano estendibili alla generalità dei compiti delle autorità di controllo.

Infine, è bene ricordare che il *selective enforcement* rischia di generare un fenomeno di *forum shopping*, qualora emerga che una certa autorità tenda a favorire determinate categorie di titolari del trattamento. Si avvererebbe così il rischio paventato dall'AG Bobek, ossia che si generino

> «covi» normativi per alcuni operatori che, dopo aver effettivamente scelto essi stessi la propria autorità nazionale di regolamentazione, localizzando su tale base il loro stabilimento principale all'interno dell'Unione, anziché essere controllati, sarebbero di fatto protetti piuttosto efficacemente da una determinata ACC nei confronti delle altre autorità di regolamentazione.[179]

Tale opinione è condivisa proprio dalla Corte nella successiva sentenza, con parole che vale la pena riportare:

> […] discende in particolare dall'articolo 51, paragrafo 1, del regolamento 2016/679 che le autorità di controllo sono incaricate di sorvegliare l'applicazione di tale regolamento, in particolare, al fine di tutelare i diritti fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali. Ne consegue che […] le norme sulla ripartizione delle competenze decisionali tra l'autorità di controllo capofila e le altre autorità di controllo, previste in detto regolamento, lasciano impregiudicata la responsabilità gravante su ciascuna di tali autorità di contribuire ad un livello elevato di protezione di detti diritti, nel rispetto di tali norme nonché dei requisiti di cooperazione e di assistenza reciproca ricordati al punto 52 della presente sentenza.[180]

le loro autorità amministrative, devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, in particolare, agli atti delle istituzioni dell'Unione, nonché astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione»; v. anche Corte giust., sentenza del 1° agosto 2022 (Grande Sezione), cause riunite C-14/21 e C-15/21, *Sea Watch eV c. Ministero delle Infrastrutture e dei Trasporti e a.*, ECLI:EU:C:2022:604, § 156; Corte giust., sentenza del 7 novembre 2013, causa C-518/11, *UPC Nederland BV c. Gemeente Hilversum*, ECLI:EU:C:2013:709, § 59.

177 Corte giust., causa C-311/18, *Facebook Ireland e Schrems* cit., § 111, corsivo aggiunto.

178 Ivi, § 112, corsivo aggiunto.

179 Conclusioni dell'AG Bobek, causa C-645/19, *Facebook Ireland Limited e a.* cit., § 124.

180 Corte giust., causa C-645/19, *Facebook Ireland Limited e a.* cit., § 67.

> Ciò significa, in particolare, che il meccanismo dello «sportello unico» *non può in alcun caso comportare che un'autorità nazionale di controllo, in particolare l'autorità di controllo capofila, non assuma la responsabilità, che le incombe in forza del regolamento 2016/679, di contribuire ad un'efficace tutela delle persone fisiche contro violazioni dei loro diritti fondamentali* ricordati al punto precedente della presente sentenza, *pena l'incoraggiare una pratica di* forum shopping*, in particolare da parte dei titolari del trattamento, al fine di eludere tali diritti fondamentali e l'applicazione effettiva delle disposizioni di detto regolamento che vi danno attuazione*.[181]

Un ulteriore campo è quello attinente all'irrogazione delle sanzioni. Nel paragrafo 2.4 si è illustrato il problema e si è anticipato che, nei tre casi analizzati, secondo la dottrina preferibile la sanzione mancava del requisito della dissuasività. Ebbene, indipendentemente dal ruolo più o meno incisivo dell'EPDB, sussiste in capo alle autorità di controllo l'obbligo di irrogare delle sanzioni dissuasive. In primo luogo, ciò è imposto dall'articolo 83, comma 1, GDPR, secondo cui «[o]gni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie […] siano *in ogni singolo caso* effettive, proporzionate e dissuasive» (corsivo aggiunto). Dal tenore letterale della norma risulta che, pur fissando i paragrafi successivi dei criteri specifici per la determinazione dell'importo della sanzione, in ogni caso essa deve, in concreto, rispondere ai requisiti di effettività, proporzionalità e dissuasività. Ciò è confermato anche dalle linee guida dell'EPDB in materia di calcolo delle sanzioni.[182]

Pare quindi proponibile un ricorso per infrazione qualora l'autorità di controllo, anche se formalmente rispettando l'intervallo fissato dal regolamento, eviti di irrogare una sanzione dissuasiva, ossia che «induc[a] l'individuo ad astenersi dal violare gli scopi e le norme di diritto dell'Unione».[183] Come affermato dalla Corte di Giustizia, «per le persone […] deve esistere un serio rischio in caso di un'infrazione alle norme […] di essere scoperte e di vedersi infliggere sanzioni adeguate».[184] Ebbene, nei casi analizzati (e soprattutto nei primi due), risulta

181 Ivi, § 68, corsivi aggiunti.

182 Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR, versione 2.1, adottate il 24 maggio 2023, `https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_it_0.pdf`: «Le autorità di controllo possono valutare la possibilità di aumentare la sanzione pecuniaria se ritengono che l'importo non sia sufficientemente dissuasivo» (§ 144) e «La singola determinazione di una sanzione pecuniaria deve sempre basarsi su una valutazione umana di tutte le circostanze pertinenti del caso e deve essere effettiva, proporzionata e dissuasiva in relazione al caso di specie» (§ 145).

183 Ivi, § 143.

184 Corte giust., sentenza del 12 luglio 2005 (Grande Sezione), causa C-304/02, *Commissione delle Comunità europee c. Repubblica francese*, ECLI:EU:C:2005:444, § 37. Per un altro caso di procedura di infrazione per violazione del requisito della dissuasività si v. Corte giust., sentenza del 21 settembre 1989, causa 68/88, *Commissione delle Comunità europee c. Repubblica ellenica*, ECLI:EU:C:1989:339, § 22-25.

difficile sostenere che sanzioni di importo estremamente basso, se confrontato con il fatturato annuo (es. 0,08%), siano idonee a raggiungere lo scopo appena enunciato. Al riguardo, è possibile richiamare le parole dell'Avvocato Generale Geelhoed nel caso C-304/02, riguardanti un ambito totalmente diverso (la pesca), ma comunque particolarmente significative:

> [i]l risultato che gli Stati membri debbono raggiungere […] è, pertanto, quello di garantire […] che, in caso di mancata osservanza, i pescatori incorrano nel serio rischio di essere scoperti *e di subire sanzioni che, come minimo, li priveranno di tutti i benefici economici derivanti dalla violazione delle disposizioni* in tema di pesca. L'attività di controllo e la minaccia di azioni repressive debbono generare una *pressione sufficiente da rendere l'inadempimento non allettante sotto il profilo economico*, in modo da garantire che la situazione prevista dalle disposizioni rilevanti in materia di pesca venga realizzata nella pratica.[185]

Ancora una volta, non sembra sostenibile la tesi per cui tali importi siano in grado di creare la «pressione sufficiente» appena citata.

2.10 *(segue) La proposta di regolamento di armonizzazione procedurale*

Se la prima proposta si basava sul diritto vigente, la seconda si riferisce ad una proposta di regolamento, in particolare la «Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679», presentata dalla Commissione il 4 luglio 2023. Trattandosi di una soluzione *de iure condendo*, si presenteranno qui solo taluni aspetti, consapevoli che il testo potrà poi essere modificato durante la procedura legislativa.

L'intenzione della Commissione di presentare una simile proposta sembra essere stata salutata in maniera favorevole da parte della dottrina. Infatti, quest'ultima aveva già in precedenza individuato come una delle maggiori cause di applicazione non ottimale del GDPR proprio la mancanza di norme procedurali dettagliate che regolino i doveri di cooperazione tra le autorità.[186] Gentile e Lynskey hanno proposto l'introduzione di norme procedurali di diritto derivato proprio al fine di risolvere i problemi generati dal meccanismo di sportello unico e da quello di coerenza,[187] osservando che: *(i)* l'avvicinamento delle legislazioni tramite linee guida dell'EPDB non sembra essere sufficiente, stante il carattere non vincolante delle stesse e il fatto che, comunque, possono riguardare solo la procedura davanti all'EPDB e non quella dinnanzi alle autorità nazionali;[188] *(ii)* ciò è gia avvenuto

185 Conclusioni dell'AG Geelhoed presentate il 29 aprile 2004, causa C-304/02, *Commissione delle Comunità europee c. Repubblica francese*, ECLI:EU:C:2004:274, § 39, corsivi aggiunti.

186 Hofmann e Mustert, «Data protection» cit., p. 466.

187 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 828.

188 Ibidem.

con riguardo al diritto della concorrenza,[189] ad esempio con il regolamento (CE) 773/2004;[190] (*iii*) la base giuridica da utilizzare potrebbe essere quella di cu all'articolo 16, paragrafo 2, TFUE.[191] Se, come detto, l'idea di un regolamento procedurale non sembra dispiacere alla dottrina, in relazione all'effettivo contenuto della proposta, sono state, invece, sollevate molte perplessità. Infatti, si è ritenuto il testo, sotto certi aspetti, debole e inidoneo a fronteggiare i problemi già esposti; anzi, si è rilevato che, talvolta, esso, più che risolverli, sembra esasperarli.

(*A*) Per quanto riguarda l'ambito della presentazione dei reclami, la Commissione rileva che le autorità «interpretano in modo diverso le prescrizioni relative alla forma di un reclamo, al coinvolgimento dei reclamanti nella procedura e al rigetto dei reclami»[192] (v. par. 2.8), e ciò ha la conseguenza di far sì che il livello di tutela sia diverso «a seconda del luogo in cui il reclamo viene proposto o di quale autorità di protezione dei dati sia l'autorità capofila per un determinato caso».[193] A tal proposito, la proposta, con riferimento ai reclami transfrontalieri, prevede che debba essere utilizzato un modulo di reclamo, precisando che «ai fini della ricevibilità del reclamo *non sono necessarie ulteriori informazioni*» (art. 3, par. 1 e cons. 4). Ciò potrebbe contribuire a chiarire quanto sostenuto nel paragrafo 2.8.

(*B*) Con riferimento alla collaborazione tra le varie autorità, la dottrina ha sottolineato come il meccanismo di cooperazione e coerenza sia il meno "proceduralizzato" del GDPR.[194] Ciò, secondo Mustert, porta – per le ragioni esaminate nei paragrafi precedenti – l'autorità capofila ad avere un ruolo troppo ingombrante nell'attuale sistema di enforcement.[195] A tal proposito, la proposta, (*i*) ricorda che «la cooperazione tra le autorità di protezione dei dati prima della presentazione di un progetto di decisione da parte dell'autorità di protezione dei dati capofila è insufficiente»[196] e (*ii*) che le autorità molto spesso non si scambiano le «informazioni utili», anche perché l'individuazione delle stesse è rimessa all'autorità capofila[197] (v. par. 2.3.1) e (*iii*) non sono stabiliti precisi termini per la conclusione

189 Ibidem.

190 Regolamento (CE) n. 773/2004 della Commissione, del 7 aprile 2004, relativo ai procedimenti svolti dalla Commissione a norma degli articoli 81 e 82 del trattato CE, GU L 123, 27/04/2004, pp. 18-24.

191 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 828-829.

192 Proposta di regolamento di armonizzazione procedurale cit., p. 2.

193 Ivi, pp. 2-3.

194 Hofmann e Mustert, «Procedures Matter» cit.; v. la stessa Proposta di regolamento di armonizzazione procedurale cit., p. 3, secondo cui «la procedura di cooperazione di cui all'articolo 60 GDPR è descritta a grandi linee».

195 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 457.

196 Proposta di regolamento di armonizzazione procedurale cit., p. 3.

197 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 457.

delle varie fasi del meccanismo di cooperazione.[198] *(iv)* Ciò porta alla situazione patologica circa l'individuazione dell'ambito di indagine illustrata al paragrafo 2.3.2.

Per ovviare a questi problemi, innanzitutto, l'articolo 8 della proposta stabilisce, al paragrafo 1 il dovere per l'autorità capofila di aggiornare periodicamente le altre autorità di controllo interessate in merito all'indagine e fornire loro quanto prima tutte le informazioni pertinenti divenute disponibili. La disposizione, in realtà, non aggiunge poi molto rispetto all'articolo 60, paragrafo 1, GDPR, perché utilizza sempre l'ambigua espressione «informazioni rilevanti».[199] Più utile è il paragrafo 2, il quale individua tutta una serie di informazioni che devono ritenersi incluse nella categoria appena citata. Tra queste vi sono anche «le informazioni sull'avvio di un'indagine su una presunta violazione del regolamento (UE) 2016/679»: ciò vale a ribadire la necessità che l'autorità capofila debba coinvolgere le altre autorità *appena venga a conoscenza della violazione*, e non in uno stadio avanzato della procedura come avvenuto nei casi *Twitter* e *WhatsApp*.

L'articolo 9 prevede, poi, che – sempre in una fase non avanzata della procedura – l'autorità capofila rediga una «sintesi delle questioni chiave», riguardante anche «l'individuazione preliminare dell'ambito dell'indagine, in particolare le disposizioni del regolamento (UE) 2016/679 interessate dalla presunta violazione su cui si svolgerà l'indagine». Entro quattro settimane, le autorità interessate possono formulare osservazioni (art. 9, par. 3). Di particolare interesse è la norma di cui all'articolo 10, paragrafo 4, la quale prevede che qualora *(i)* il caso sia basato su un reclamo e *(ii)* una o più autorità non raggiungono un consenso sulla determinazione dell'ambito di indagine, l'autorità capofila debba chiedere una decisione vincolante d'urgenza ex articolo 66 GDPR, presumendosi soddisfatte le condizioni di cui all'articolo 66, paragrafo 3 del GDPR.[200] Si tratta di una innovazione utile, in quanto permette di raggiungere sin da subito un accordo sull'ambito di indagine *collegialmente in sede di comitato*, cosicché poi si eviterà l'insorgere di ulteriori controversie.[201] A questa parte della proposta possono, però, anche essere mosse alcune critiche: *(i)* non si comprende bene perché restringere questo rimedio ai soli casi basati su reclami, e non anche alle indagini iniziate d'ufficio.[202]

198 Proposta di regolamento di armonizzazione procedurale cit., p. 4.

199 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 457.

200 Su tale procedura d'urgenza si veda più ampiamente L. Georgieva, «Article 66 Urgency procedure», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner et al., Oxford University Press, New York 2020.

201 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 457.

202 F. Brito Bastos e P. Pałka, «Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?», *European Constitutional Law Review*, 19, 3 (2023), p. 508.

Come si è analizzato nel paragrafo 2.3.3, talune autorità – segnatamente, quella irlandese – hanno la tendenza ad iniziare una propria indagine ufficiosa, anziché dar seguito ai reclami ricevuti e, in questo modo, potrebbero facilmente escludere l'operatività della norma in esame.[203] Pertanto, questo punto, forse, andrebbe ripensato, al fine di evitare che l'esasperante prassi appena enunciata sia ancora di più incoraggiata. Inoltre, *(ii)* sarebbe più opportuno prevedere che la procedura possa essere iniziata anche dalle autorità interessate, e non solo dalla capofila,[204] così da evitare eventuali condotte dilatorie di quest'ultima.

Continuando nell'analisi delle norme che presidiano la cooperazione tra le autorità, non è scevro da dubbi anche l'articolo 18 della proposta, il quale stabilisce delle condizioni per la presentazione delle «obiezioni pertinenti e motivate». Vengono dettati, innanzitutto, dei requisiti sostanziali: le obiezioni devono *(i)* basarsi «esclusivamente sugli elementi fattuali figuranti nel progetto di decisione» (art. 18, par. 1, lett. a) e non modificare «la portata delle accuse sollevando punti che equivalgono all'individuazione di ulteriori accuse di violazione del regolamento (UE) 2016/679 o che modificano la natura intrinseca delle accuse mosse» (art. 18, par. 1, lett. b). Inoltre, dal punto di vista formale, ciascuna obiezione *(ii)* non deve superare la lunghezza di tre pagine e non deve contenere allegati (art. 18, par. 1, lett. a); *(iii)* il disaccordo deve essere formulato «in termini sufficientemente chiari, coerenti e precisi» (art. 18, par. 1, lett. b). Questa disciplina è stata criticata in dottrina, in quanto limita la possibilità per le autorità interessate di obiettare al progetto di decisione,[205] peraltro fissandolo a requisiti di dubbia ragionevolezza quale un limite di pagine. Non solo la proposta non contribuisce a rafforzare il ruolo delle autorità interessate. Anzi, essa sembra andare proprio nella direzione opposta di rafforzamento dell'autorità capofila.[206] Vi è da chiedersi se – viste tutte le criticità connesse al ruolo (più che talvolta disfunzionale) di queste ultime, specie di quella irlandese – era questo l'orientamento che fosse più opportuno perseguire.

(*C*) Un ulteriore ambito di intervento è quello dei diritti procedurali del titolare del trattamento e dell'interessato reclamante. È questo il campo dove la (comprensibilmente poca) dottrina ha probabilmente espresso le sue critiche più aspre. Effettivamente, tali perplessità paiono fondate, per le ragioni che si diranno di seguito.

Innanzitutto, secondo una prima opinione, la proposta non avrebbe dovuto, in assoluto, occuparsi di aspetti riguardanti i singoli, ma solo dei rapporti tra le varie

203 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 458.
204 Ibidem.
205 Ivi, p. 459.
206 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 507-508.

autorità di controllo. Infatti, secondo tale tesi, la relazione individuo-autorità di controllo può essere efficacemente regolata a livello nazionale, secondo le norme procedurali di ciascuno Stato membro.[207]

Passando ad analizzare il contenuto di questa parte della proposta, si nota che essa dedica molto più spazio ai *soggetti dell'indagine* rispetto che al *reclamante*, generando così una situazione particolarmente sbilanciata a favore dei primi.[208] In particolare, ai reclamanti viene data sì la possibilità di presentare osservazioni alle constatazioni preliminari, ma non in relazione al progetto di decisione revisionato.[209] Solamente se il provvedimento è di totale o parziale rigetto viene concesso un termine, non inferiore a tre settimane, entro il quale il reclamante può comunicare le sue opinioni per iscritto (art. 12, par. 2).

Suscita significative perplessità la norma di cui all'articolo 12, paragrafo 3, secondo cui, qualora non pervengano le osservazioni di cui al paragrafo precedente entro il termine previsto, il reclamo si considera come rigettato. Non è facile comprendere quale sia la *ratio* di questa norma: di certo non si può affermare che essa debba essere rinvenuta nella sopravvenuta mancanza di interesse del reclamante,[210] anche considerato il fatto che si tratta di un rimedio che non richiede la difesa tecnica e che dovrebbe essere disponibile a tutti gli interessati *indipendentemente dalle loro conoscenze giuridiche*. L'unica ragione che viene in mente, collegata a motivi deflattivi del carico di lavoro delle autorità di controllo,[211] non pare, sinceramente, andare verso una tutela effettiva del diritto di cui agli articoli 8 della Carta e 16 del TFUE.

Quello che, forse, lascia ancora più interdetti è la ragione posta dalla Commissione alla base di questo sbilanciamento tra le due posizioni di reclamante e titolare. Infatti, il considerando 25 così recita:

> un'indagine condotta da un'autorità di controllo su una possibile violazione del regolamento […] *non costituisce un procedimento in contraddittorio* tra il reclamante e le parti oggetto dell'indagine. Si tratta di una procedura avviata da un'autorità di controllo, di propria iniziativa o sulla base di un reclamo, nell'adempimento dei propri compiti ai sensi dell'articolo 57, paragrafo 1, del regolamento (UE) 2016/679. Le parti oggetto dell'indagine e il reclamante *non si trovano dunque nella stessa situazione procedurale* e quest'ultimo non può invocare i diritti della difesa quando la decisione non pregiudica la sua posizione giuridica.

207 Si v. l'opinione espressa da Max Schrems in M. Van den Poel, *Taking GDPR enforcement really seriously: What to expect from the GDPR Procedural Regulation?*, Workshop Summary, Brussels Privacy Hub Working Paper, gennaio 2024, p. 4.

208 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 460-462.

209 Ivi, p. 461.

210 Ibidem.

211 Ibidem.

> Il coinvolgimento del reclamante nella procedura contro le parti oggetto dell'indagine non può compromettere il diritto di queste ultime di essere ascoltate.[212]

Ciò porta a concludere che i reclamanti non debbano considerarsi parti della procedura.[213] Questa conclusione è fortemente criticabile per varie ragioni. Certo, è vero che il procedimento davanti all'autorità di controllo ha come fine primario uno scopo di natura pubblicistica, cioè l'accertamento e la conseguente sanzione delle violazioni del GDPR. Per ripristinare la specifica lesione causata da tale violazione in capo all'interessato restano sempre disponibili i rimedi civilistici. Tuttavia, come già esposto (v. *supra* par. 2.3.3), «la procedura di reclamo, che non è simile a quella di una petizione, è concepita come un meccanismo idoneo a salvaguardare efficacemente i diritti e gli interessi delle persone coinvolte».[214] Tale opinione della Corte mostra come il reclamo, oltre a ricoprire la funzione pubblicistica già citata, sia anche *strumento di tutela dei diritti dell'interessato*. Ciò comporta che non sia ragionevole sbilanciare in questo modo le posizioni: il titolare è pregiudicato nella sua posizione qualora venga accertata una violazione e irrogata una sanzione, *ma anche l'interessato può vedere leso il proprio diritto alla protezione dei dati qualora il reclamo venga, erroneamente, rigettato*.

Di fatto, affermare che l'interessato si trovi in una posizione degradata rispetto a quella del titolare significa ritornare alla tesi – squalificata, però, dalla Corte in *SCHUFA Holding* – per cui il reclamo sia una petizione, avendo quindi l'unica funzione di segnalare all'autorità una possibile violazione. Peraltro, se questa fosse la tesi, non avrebbe alcun senso prevedere per l'interessato un rimedio giurisdizionale effettivo contro la decisione dell'autorità che lo riguardi (si badi bene: *che lo riguardi*, non *che rigetti il suo reclamo*) nella forma di un sindacato giurisdizionale pieno:[215] in tale sede, peraltro, l'interessato acquista appieno la natura di parte sostanziale del processo.

A ben vedere, il considerando 25 non erra quando afferma che il reclamante «non può invocare i diritti della difesa quando la decisione non pregiudica la sua posizione giuridica». Il punto è che, poi, la parte "prescrittiva" del regolamento ritiene che la sua posizione giuridica possa essere lesa solamente quando il reclamo viene rigettato. Ciò, come già più volte esposto, è errato: al reclamante dovrebbe essere permesso di esprimere la propria posizione *in ogni caso*, poiché anche in caso di accoglimento del reclamo, egli potrebbe dissentire dal contenuto del provvedimento, *in quanto ritiene che esso non tuteli appieno i suoi diritti*.

212 Proposta di regolamento di armonizzazione procedurale cit., cons. 25, corsivi aggiunti.
213 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 461.
214 Corte giust., cause riunite C-26/22 e C-64/22, *SCHUFA Holding (Esdebitazione)* cit., § 58.
215 Ivi, § 70.

In aggiunta, la dottrina osserva che, anche vedendo come parti del procedimento i soli soggetti sottoposti ad indagine, l'idea della Commissione di concedere quasi tutti i diritti procedurali solo a questi ultimi non sembra conforme con il diritto primario dell'Unione.[216] Mustert evidenzia come il richiamo della Commissione all'articolo 41 della Carta sia inconferente, per il fatto che esso non si applica agli Stati membri ex articolo 51, paragrafo 1, della Carta.[217] Sempre secondo questa dottrina, tale richiamo avrebbe la conseguenza di escludere i reclamanti dal diritto di essere sentiti, in quanto la disposizione prevede «il diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale *che le rechi pregiudizio*».[218]

Piuttosto, come già precisato nel presente elaborato al paragrafo 2.5, la Commissione avrebbe dovuto riferirsi al diritto ad una buona amministrazione *in quanto principio generale di diritto dell'Unione*.[219] Tale principio è applicabile anche agli Stati membri quando attuano il diritto dell'Unione. Ciò che rileva maggiormente, è però che, ai fini della sua attribuzione, non è necessario che il procedimento conduca *ad una decisione a lui indirizzata*, ma è sufficiente che esso «possa sfociare in un atto per essa lesivo».[220] Pertanto, la circostanza che la decisione sia indirizzata al titolare (in quanto accoglie il reclamo) o all'interessato (in quanto lo respinge) non dovrebbe costituire criterio dirimente per l'attribuzione del diritto ad intervenire nel procedimento.[221]

In conclusione, l'intento generale della Commissione di dettare norme più specifiche sul tema è lodevole. Tuttavia, i contenuti della proposta lasciano aperte numerose perplessità e sono suscettibili di ampio miglioramento. Allo stato attuale, la proposta sembra troppo sbilanciata a favore dei titolari del trattamento e pare rendere ancora più difficile un'efficace e tempestiva tutela del diritto alla protezione dei dati personali,[222] attribuito ad ogni individuo dall'articolo 8 della Carta e dall'articolo 16 del Trattato sul funzionamento. Nell'attribuzione di diritti procedurali alle parti, la proposta non si sforza di facilitare l'esercizio degli stessi. Anzi, essa finisce, molto spesso, con il subordinare tali prerogative (soprattutto

216 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 462.
217 Ibidem.
218 Ivi, p. 462. Tuttavia, sul punto si è già ribadito come anche la decisione di accoglimento possa essere pregiudizievole per l'interessato.
219 Ivi, p. 462.
220 Corte giust., causa C-32/95 P, *Lisrestal e a.* cit., § 21.
221 Mustert, «The Commission Proposal for a New GDPR Procedural Regulation» cit., p. 462.
222 NOYB, «GDPR Procedures Regulation: Commission Proposal is an attack on users' rights in GDPR procedures» (04/07/2023), https://noyb.eu/en/gdpr-procedures-regulation-stripping-citizens-procedural-rights (visitato il 11/03/2024).

quelle del reclamante) alla discrezionalità – o meglio, alla «benevolenza» – dell'autorità capofila.[223] Inoltre, nel rapporto tra autorità di controllo capofila, da una parte, e autorità interessate ed EPDB, dall'altra, la proposta, lungi dal mitigare il ruolo – giudicato unanimemente dalla dottrina come troppo preponderante – della prima, sembra, piuttosto, consolidarlo.[224] Poiché lo scopo del meccanismo di cui agli articoli 60 e seguenti del GDPR è il raggiungimento di un livello *uniforme* di tutela dei dati personali, vien da chiedersi come un simile rafforzamento possa perseguire tale fine di armonizzazione.

223 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 505-506: «*it is striking how the procedural rights of parties under investigation, and especially of complainants, are placed at the discretion – at the goodwill – of lead supervisory authorities. Complainants, for example, will enjoy the right to access administrative case files but only if the lead supervisory authority "considers that it is* necessary*" (emphasis added) to share documents contained in them for complainants to be able to make their views known effectively. A lead authority that revises a draft decision after receiving other authorities' objections will be required to observe the right to be heard. That is, of course, if the lead authority decides that a hearing is convenient […]*».

224 Van den Poel, *Taking GDPR enforcement really seriously* cit., p. 2; Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 507.

3

L'enforcement del Digital Services Act: quali prospettive?

3.1 *Introduzione*

Una volta analizzato il meccanismo di *enforcement* del Regolamento generale sulla protezione dei dati, il presente capitolo si propone di comprendere come il legislatore abbia concepito il sistema di attuazione del Digital Services Act. Sin da subito, si può anticipare che le scelte compiute per questo nuovo regolamento sono state in parte simili e in parte diverse rispetto a quelle adottate con il GDPR.

In particolare, viene confermata l'idea per cui ad attuare il diritto comunitario debbano essere, innanzitutto, gli Stati membri, per mezzo di autorità indipendenti. Analogamente, è stata prevista l'istituzione di un meccanismo di cooperazione e coerenza, volto a (tentare di) assicurare che l'attuazione a livello nazionale non vanifichi gli sforzi di uniformazione che uno strumento di natura regolamentare comporta. Come si vedrà nel paragrafo 3.4, i ruoli dei due comitati – Comitato europeo per la protezione dei dati e Comitato europeo per i servizi digitali – non sono completamente sovrapponibili, per le differenze che verranno *infra* presentate.

La principale differenza tra i due meccanismi sta, però, nel ruolo di primo piano che il DSA accorda alla Commissione europea, alla quale vengono riservati significativi compiti di vigilanza con riferimento alle «piattaforme di dimensioni molto grandi» (VLOP) e ai «motori di ricerca molto grandi» (VLOSE) (per la cui definizione si rimanda al paragrafo 1.3).

L'analisi di queste tematiche procederà nel seguente modo: dapprima si presenteranno i diversi attori che intervengono nel meccanismo di *enforcement* del DSA, capendo quali siano le competenze e i poteri a ciascuno attribuiti (parr. 3.2, 3.3, 3.4, 3.5). A tal riguardo, ci si occuperà specificamente di comprendere quale sia l'entità del ruolo affidato al neo-costituito comitato europeo per i servizi digitali sia sufficientemente (par. 3.4), nonché di criticare la scelta della Commissione europea quale principale *enforcer* del DSA (par. 3.7). Inoltre, sarà indagata la compatibilità con il diritto primario del potere più penetrante previsto dal DSA, ossia quello di

restringere l'accesso ad una piattaforma (par. 3.6). Infine, a partire dalla recente sentenza *Meta c. Bundeskartellamt*, si tenterà di capire in che modo le diverse autorità che regolano le piattaforme digitali possano (e debbano) efficacemente collaborare tra loro (par. 3.8).

3.2 *La suddivisione di competenze tra l'UE e gli Stati membri*

Prima procedere con ulteriori analisi, è necessario approfondire brevemente come il DSA abbia ripartito le competenze tra le istituzioni dell'Unione europea e le autorità degli Stati membri. A questo riguardo, norma cardine è l'articolo 56 DSA. Il principio generale da esso posto è quello per cui tale potere viene affidato alle autorità nazionali. In particolar modo, come già previsto dal GDPR, viene sancita la competenza dello Stato membro ove il fornitore del servizio ha il suo stabilimento principale (art. 3, par. 1, lett. n), art. 56, par. 1 e cons. 123 DSA). Si deve ritenere che anche qui la norma sia ispirata al principio del paese d'origine e ne condivida la *ratio* (già illustrata nel capitolo introduttivo).

Tuttavia, alla Commissione vengono riservati penetranti compiti di vigilanza. In particolare, essa è (*i*) competente, in via *esclusiva*, per l'attuazione e la vigilanza circa gli obblighi specifici a carico di VLOP e VLOSE, individuati, in aggiunta a quelli ordinari, dalla sezione 5 del capo III del regolamento (art. 56, par. 2, DSA). Inoltre, (*ii*) essa è dotata di una competenza *concorrente* con riferimento al rispetto degli altri obblighi – cioè, quelli imposti a tutti i fornitori del servizio – da parte di tali piattaforme molto grandi[1] (art. 56, par. 3, DSA). In relazione a quest'ultimo aspetto, l'articolo 56, paragrafo 4, DSA prevede un meccanismo che può essere definito di *pre-emption*: Stati membri e Commissione condividono il potere di vigilanza in questo ambito; tuttavia, *qualora vi sia un intervento della Commissione* in relazione ad una certa violazione, è precluso alle autorità nazionali di agire con riferimento alla medesima violazione. In altre parole, gli Stati membri possono intervenire *solo se non vi ha già provveduto la Commissione*. La *ratio* di una simile disciplina viene illustrata dal considerando 125, secondo cui

> [a]i fini dell'efficienza, per evitare duplicazioni e garantire il rispetto del principio del ne bis in idem, dovrebbe spettare alla Commissione valutare se ritiene opportuno esercitare tali competenze condivise in un determinato caso e, una volta avviato il procedimento, gli Stati membri non dovrebbero più avere la capacità di farlo.[2]

1 E. Priolo, «Coordinatori dei servizi digitali, Commissione e sanzioni», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 219.

2 Il considerando 125 premette quanto segue: «[d]a un lato, in molti casi la Commissione potrebbe essere in una posizione migliore per affrontare le violazioni sistemiche commesse da tali fornitori,

3.3 *I coordinatori dei servizi digitali*

Come si è detto, i compiti di attuazione del DSA sono ripartiti tra istituzioni comunitarie e Stati membri. Con riferimento a questi ultimi, l'articolo 49, paragrafo 1, stabilisce che essi designino una o più «autorità competenti», «incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del [DSA]». Il paragrafo 2 prevede che una delle autorità competenti appena citate debba essere designata quale «coordinatore dei servizi digitali» (detto anche «DSC», *Digital Services Coordinator*). Si tratta del ruolo più rilevante, in quanto tale autorità (*i*) è responsabile di tutte le questioni relative all'applicazione del regolamento (art. 49, par. 2, DSA); (*ii*) ha compiti di coordinamento tra le altre autorità competenti eventualmente designate (art. 49, par. 2, DSA); (*iii*) dovrebbe «fungere da punto di contatto unico con riguardo a tutte le questioni relative all'applicazione del presente regolamento per la Commissione, il comitato, i coordinatori dei servizi digitali degli altri Stati membri nonché per le altre autorità competenti dello Stato membro in questione» (cons. 110).

Gli Stati membri dovevano effettuare tali designazioni entro il 17 febbraio 2024 (art. 49, par. 3, DSA). La tendenza generale a livello europeo è stata quella di non istituire un'*ulteriore* autorità, ma di attribuire le funzioni ad un ente *già esistente*. Per quanto riguarda l'Italia, l'articolo 15, comma 1, del decreto-legge 123/2023[3] ha designato come DSC l'Autorità per le garanzie nelle comunicazioni (AGCOM), individuando come ulteriori autorità competenti l'Autorità per la concorrenza e il mercato e il Garante per la protezione dei dati personali. Per quanto riguarda gli altri Stati membri,[4] alcuni hanno seguito la stessa strada dell'Italia, nominando quale DSC l'autorità responsabile per la regolazione delle comunicazioni, come ad esempio la Francia (*Autorité de régulation de la communication audiovisuelle et numérique*), il Belgio (*Belgisch Instituut voor postdiensten en telecommunicatie-Institut belge des services postaux et des télécommunications*), la Germania (*Bundesnetzagentur*

come quelle che riguardano più Stati membri o infrazioni gravi e ripetute o la mancata istituzione dei meccanismi efficaci richiesti dal presente regolamento. D'altro canto, le autorità competenti dello Stato membro in cui è situato lo stabilimento principale di [una VLOP] o [un VLOSE] potrebbero essere in una posizione migliore per affrontare singole violazioni che siano commesse da tali fornitori e che non sollevino problemi sistemici o transfrontalieri».

3 Decreto-legge 15 settembre 2023, n. 123, recante «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonchè per la sicurezza dei minori in ambito digitale» (GU n. 216 del 15/09/2023), convertito con modificazioni dalla L. 13 novembre 2023, n. 159 (GU 14/11/2023, n. 266).

4 Si v. l'utile tabella predisposta dalla Stiftung Neue Verantwortung (05/02/2024), `https://www.stiftung-nv.de/en/publication/overview-digital-services-coordinators-europe` (visitato il 26/03/2024).

für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen)[5] e l'Austria (*Kommunikationsbehörde Austria*). Altri hanno invece attribuito tale ruolo all'autorità per la concorrenza, ad esempio i Paesi Bassi (*Autoriteit Consument en Markt*), il Lussemburgo (*Autorité de la concurrence*) e la Spagna (*Comisión Nacional de los Mercados y la Competencia*). Una scelta diversa è stata effettuata dall'Irlanda, la quale ha optato per la dissoluzione della *Broadcasting Authority of Ireland* e per l'istituzione di una nuova autorità, denominata «*Coimisiún na Meán*».[6] Resta da vedere come gli Stati membri attueranno, in concreto, il regolamento e quali di queste scelte si riveleranno più efficaci.[7]

Per quanto riguarda i poteri del DSC, la loro disciplina è rinvenibile all'articolo 51. Si tratta di una serie piuttosto ampia di prerogative, che include poteri di indagine (ottenere informazioni, effettuare o ordinare ispezioni, chiedere spiegazioni) e di esecuzione (ordinare la cessazione delle violazioni, imporre sanzioni pecuniarie e penalità di mora, adottare misure provvisorie).

Un potere piuttosto significativo risulta essere quello di cui all'articolo 51, paragrafo 3, comma 1, lettera b): il DSC può chiedere all'autorità giudiziaria competente del suo Stato membro di (*i*) ordinare la restrizione temporanea dell'accesso *al servizio interessato dalla violazione* da parte dei destinatari o, solo se ciò non sia tecnicamente fattibile, (*ii*) la restrizione dell'accesso all'*intera interfaccia online* del fornitore sulla quale ha luogo la violazione. Come si può comprendere, si tratta di un potere potenzialmente in grado di impattare significativamente sui diritti e le libertà delle persone interessate. Difatti, esso è concepito come *extrema ratio*[8] dal legislatore, il quale lo subordina a stringenti condizioni. Innanzitutto, la restrizione non può essere ordinata dall'autorità amministrativa stessa, ma deve

5 A questo riguardo, Corte giust., sentenza del 2 settembre 2021, causa C-718/18, *Commissione europea c. Repubblica federale di Germania*, ECLI:EU:C:2021:662 ha sollevato dubbi circa l'indipendenza del Bundesnetzagentur, v. anche L. Kaschny e S. Lavrijssen, «The Independence of National Regulatory Authorities and the European Union Energy Transition», *International and Comparative Law Quarterly*, 72, 3 (2023). Il tema è rilevante considerando quello che si esporrà nel par. 3.7.

6 Si v. il comunicato stampa presente sul sito del *Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media* (22/02/2023), https://www.gov.ie/en/press-release/1713e-unpublished-minister-for-tourism-culture-arts-gaeltacht-sport-and-media-catherine-martin-td-signs-orders-to-formally-establish-coimisiun-na-mean-and-commence-key-provisions-of-the-online-safety-and-media-regulation-act-2022/ (visitato il 26/03/2024).

7 Si v. le raccomandazioni esposte da J. Jaursch, «Platform Oversight: Here is what a Strong Digital Services Coordinator Should Look», in *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications*, a cura di J. Hoboken et al., Verfassungsbooks, Berlin 2023.

8 I. Castellucci e F. Coppola, «Il sistema sanzionatorio decentrato del DSA: dinamica dell'apparato istituzionale», *Diritto di Internet*, 1 (2023), p. 53.

essere da essa richiesta al giudice: si prevede qui una riserva di giurisdizione.[9] Inoltre, devono sussistere i seguenti requisiti: siano stati esauriti tutti gli altri poteri previsti dall'articolo 51 senza che la violazione sia cessata; tale violazione causi un danno grave e costituisca un «reato grave che comporta una minaccia per la vita o la sicurezza delle persone». Le misure disposte devono essere proporzionate alla natura, alla gravità, alla reiterazione e alla durata della violazione e non devono limitare indebitamente l'accesso alle informazioni lecite da parte dei destinatari del servizio interessato (art. 51, par. 3, co. 2, DSA).

Per quanto riguarda la durata di tali misure, è previsto un termine di *quattro settimane*, prorogabile di ulteriori periodi della stessa durata (art. 51, par. 3, co. 3, DSA). La dottrina ha sollevato significative perplessità circa la scelta del legislatore di prevedere un termine fisso, posto che, in taluni casi, potrebbe essere sufficiente un periodo inferiore per evitare il «grave danno».[10] La stessa dottrina, con tesi che qui si condivide, sottolinea come una simile disciplina difficilmente si concilia con il principio di proporzionalità, sancito dallo stesso articolo 52 DSA[11] ma anche, più significativamente, dall'articolo 5 TUE. Bisogna chiedersi, se tale norma possa essere annullata dalla Corte di Giustizia nel caso in cui tale questione le venga sottoposta ex articolo 263 o 267, paragrafo 1, lettera b), TFUE.[12]

Inoltre, ai sensi dell'articolo 53, i destinatari del servizio possono presentare un reclamo al DSC per lamentare la violazione di una o più norme del regolamento. Si tratta di una significativa novità se confrontata con la direttiva 2000/31/CE, in quanto quest'ultima non prevedeva alcun obbligo in capo agli Stati membri di concedere un simile strumento in capo ai privati.[13] In dottrina si è sottolineato come un simile cambio di passo sia sintomo della volontà del legislatore europeo di favorire – al pari di altre fonti comunitarie, quali il GDPR – il cd. «utente debole», la cui protezione è uno dei principali obiettivi della disciplina.[14] Altra dottrina fa però una precisazione: da un lato, il GDPR trova la sua base giuridica in un'apposita norma del TFUE, la quale pone come obiettivo principale – pur con tutti i *caveat* illustrati nel capitolo introduttivo – la tutela di un diritto fondamentale dell'individuo, cioè il diritto alla protezione dei dati personali. Dall'altra, il

9 F. G. Murone, «Il Digital Service Act e il contrasto ai contenuti illeciti (pt. II)», *Ius in Itinere* (28 febbraio 2022).

10 Sabia, «L'enforcement pubblico del Digital Services Act» cit., p. 97; Castellucci e Coppola, «Il sistema sanzionatorio decentrato del DSA» cit., p. 54.

11 Sabia, «L'enforcement pubblico del Digital Services Act» cit., p. 97; Castellucci e Coppola, «Il sistema sanzionatorio decentrato del DSA» cit., p. 54.

12 Circa la rispondenza di tali misure all'articolo 10 CEDU e all'articolo 11 della Carta, si v. il paragrafo 3.6.

13 Priolo, «Coordinatori dei servizi digitali» cit., p. 211.

14 Castellucci e Coppola, «Il sistema sanzionatorio decentrato del DSA» cit., p. 52.

regolamento (UE) 2022/2065, pur mirando anche alla protezione dei diritti dell'individuo, vede come base giuridica l'articolo 114 TFUE ed ha come scopo principale la regolazione di una porzione di mercato interno, cioè i servizi digitali.[15]

Il reclamo va presentato al DSC «dello Stato membro in cui il destinatario del servizio è situato o è stabilito»: si tratta di una formulazione parzialmente diversa da quella del GDPR (v. *supra* par. 2.2), in quanto, in questo caso, non si richiama il criterio della residenza/luogo di lavoro/violazione, ma si utilizza il generale concetto dell'«essere situati» o «stabiliti».[16] Della disciplina per i casi in cui il reclamo sia presentato ad un'autorità diversa dal DSC ove il fornitore ha lo stabilimento principale si dirà in seguito (v. par. 3.4).

La disciplina del procedimento di gestione del reclamo contenuta nel DSA è piuttosto laconica. L'articolo 53 si limita a sancire il diritto delle parti «di essere ascoltate» e di «ricevere informazioni adeguate sullo stato del reclamo». Tale indicazione è sicuramente utile per ribadire la sussistenza di tali diritti, ma – soprattutto la prima – non aggiunge nulla di innovativo, poiché il diritto di essere ascoltati è previsto dall'articolo 41 della Carta e costituisce principio generale del diritto comunitario (v. par. 2.5). Il medesimo articolo prevede che tali diritti siano esercitati «conformemente al diritto nazionale», rimettendo quindi la disciplina degli stessi al diritto (amministrativo) di ogni Stato membro, al quale spetterà determinare i tempi per la conclusione del procedimento, il significato del silenzio, quali siano i rimedi giurisdizionali in caso di inerzia o di rigetto del reclamo.[17] Da questo punto di vista, spetta sicuramente al legislatore europeo la facoltà di rimettere tale disciplina ai legislatori nazionali. Anzi, ciò è anche in linea con il principio di autonomia procedurale ed amministrativa degli Stati membri. Tuttavia, siano permesse due critiche: *(i)* il GDPR adotta una scelta differente, in quanto sancisce specificamente alcuni diritti, in particolare il diritto a presentare un ricorso giurisdizionale effettivo contro la decisione dell'autorità o contro la sua inerzia (art. 78 GDPR). È vero che, comunque, tale diritto sarebbe previsto dall'articolo 47 della Carta. Tuttavia, l'articolo 78 GDPR fornisce delle specifiche aggiuntive (come, ad esempio, quale sia il termine dopo il quale l'autorità si debba considerare inerte). Il punto rilevante è che lo fa *con norma direttamente applicabile nei confronti degli individui*, in quanto sufficientemente chiara, precisa ed

15 M. Borgobello, «Digital Services Act, è il mercato interno il vero protagonista», *Agenda Digitale* (23 dicembre 2022), (visitato il 20/12/2023); in generale, sui limiti all'uso dell'art. 114 TFUE si v. il capitolo introduttivo alla nota 5 (p. 6) e la dottrina e la giurisprudenza ivi citata.

16 Correttamente viene richiamato anche il criterio dello stabilimento, visto che, a differenza del GDPR ove gli interessati possono essere solo persone fisiche, nel DSA «destinatari del servizio» possono essere anche le persone giuridiche.

17 Priolo, «Coordinatori dei servizi digitali» cit., p. 212.

incondizionata. Ciò fornisce già una prima garanzia concreta a vantaggio dei singoli, senza che per essa sia necessario un intervento a livello nazionale. *(ii)* La seconda critica si ricollega alla prima. Come si è notato nel capitolo 2 (e, in particolare, nel paragrafo 2.8), pur in presenza di una fonte di natura regolamentare e direttamente attributiva di un diritto nei confronti dei singoli, le prassi con cui le autorità di controllo garantiscono il diritto di cui all'articolo 77 GDPR differiscono notevolmente da Stato a Stato. Ebbene, è ragionevole supporre che, per quanto riguarda il DSA, non essendo armonizzate nemmeno tali condizioni minime, le differenze saranno ancora più ampie. Anche in questo senso, richiamando la tesi presentata in precedenza, il DSA sembra mostrarsi un po' meno sensibile verso la tutela dei diritti fondamentali.

3.4 *Il comitato europeo per i servizi digitali: un ruolo meramente consultivo?*

L'articolo 61 del DSA prevede l'istituzione di un «gruppo consultivo indipendente di coordinatori dei servizi digitali», denominato «comitato europeo per i servizi digitali». Esso è composto dai DSC di ogni Stato membro, rappresentati da funzionari di alto livello (art. 62, par. 1, DSA) ed è presieduto dalla Commissione (art. 62, par. 2, DSA), la quale ha anche compiti di assistenza amministrativa (art. 62, par. 4, DSA). Per quanto riguarda le modalità decisionali, ogni Stato membro dispone di un voto, mentre la Commissione non ha diritto di voto (art. 62, par. 3, DSA); il comitato adotta i propri atti a maggioranza semplice (a differenza dell'EPDB che, come si è visto, decide con maggioranza qualificata dei due terzi).

Tralasciati questi aspetti relativi alla struttura del comitato, più interessante è analizzare quale sia il suo ruolo nell'ambito dell'attuazione del regolamento. Tale ruolo viene esplicitato già dalla norma di apertura della sezione III (art. 61), la quale definisce il comitato come «gruppo consultivo» e gli attribuisce il compito di «fornire consulenza» ai DSC e alla Commissione al fine di raggiungere i seguenti obiettivi (art. 61, par. 2, DSA): *(i)* contribuire all'applicazione coerente del regolamento e alla cooperazione efficace dei DSC e della Commissione; *(ii)* «coordinare e contribuire agli orientamenti e all'analisi della Commissione, dei coordinatori dei servizi digitali e di altre autorità competenti sulle questioni emergenti nel mercato interno in relazione alle materie disciplinate [dal DSA]»; *(iii)* assistere i DSC e la Commissione nella vigilanza sulle VLOP.

È dunque chiaro che il legislatore individua il comitato come un organismo essenzialmente di consulenza, il cui obiettivo principale è quello di assicurare un'applicazione coerente ed uniforme del DSA tra i vari Stati membri.[18] A questo

18 V. M. Pavese, «Comitato: nozione, disciplina applicabile», in *Digital services act e Digital markets*

riguardo, il presente paragrafo si propone di indagare se (*i*) il ruolo del comitato sia, effettivamente, meramente consultivo e, se sì, (*ii*) qualora tale ruolo sia sufficiente per garantire un'applicazione uniforme del regolamento. Dal punto di vista metodologico, l'analisi sarà condotta presentando le norme del DSA che disciplinano il "meccanismo di coerenza", confrontandole con le rispettive disposizioni previste dal GDPR. Infatti, quest'ultimo rappresenta, quantomeno in merito ai servizi digitali, il punto di riferimento per tali tipologie di meccanismi.

Come già illustrato nel paragrafo 3.1, per la vigilanza e l'applicazione del DSA è competente lo Stato membro ove è situato lo stabilimento principale del fornitore (art. 56, par. 1, DSA). Per primo, è possibile esaminare il caso in cui sia presentato un reclamo ad un DSC diverso da quello dello Stato membro ove vi è lo stabilimento principale del fornitore del servizio. A questo riguardo, la disciplina dettata dal DSA risulta poco dettagliata: l'articolo 53 prevede semplicemente che il DSC che riceve il reclamo lo debba valutare e «se del caso» trasmetterlo al DSC del luogo di stabilimento, accompagnandolo, se ritenuto opportuno, da un parere. Secondo una parte della dottrina, con questo regolamento il legislatore comunitario ha voluto allontanarsi dal meccanismo di sportello unico individuato dal GDPR, a causa delle problematiche che esso comporta.[19] In realtà, non pare che si possa intravedere una simile intenzione. Infatti, dal combinato disposto tra l'articolo 53, appena citato, e l'articolo 56, paragrafo 1, secondo cui «[l]o Stato membro in cui è situato lo stabilimento principale del fornitore di servizi intermediari dispone di poteri *esclusivi* per la vigilanza e l'applicazione del presente regolamento», sembra potersi trarre il principio per cui il reclamo non possa essere "trattenuto" dal DSC ove è situato il reclamante, ma debba essere in ogni caso trasmesso a quello del luogo di stabilimento, in quanto quest'ultimo è *esclusivamente* competente per la vigilanza su tale fornitore.

D'altra parte, è vero che, in questo ambito, il legislatore pare essere stato eccessivamente laconico: sarebbe stato apprezzabile un maggior sforzo nel regolare un procedimento importante come quello dei reclami a carattere transfrontaliero.[20] Tale esigenza è emersa con riferimento al GDPR, in relazione al quale – pur in presenza di norme più dettagliate circa i rapporti tra le varie autorità in caso di simili reclami (v. art. 60 GDPR) – la dottrina ha manifestato la necessità di stabilire

act: definizioni e prime applicazioni dei nuovi regolamenti europei, a cura di L. Bolognini et al., Giuffrè, Milano 2023, p. 200.

19 Priolo, «Coordinatori dei servizi digitali» cit., p. 211.

20 A questo riguardo, non risulta che ciò sia il risultato di una riluttanza degli Stati membri nel regolare questo aspetto. Infatti, già l'articolo 43 della Proposta DSA presentava una formulazione molto breve e nulla diceva in materia.

in modo ancora più preciso gli aspetti procedurali e la Commissione ha ritenuto di proporre, proprio a questo scopo, un nuovo regolamento (v. *supra* par. 2.10).

Nell'ottica di una cooperazione transfrontaliera tra i vari coordinatori, l'articolo 58 prevede che possano essere rivolte al DSC competente talune *richieste*. In particolare, *(i)* qualora la Commissione non abbia già avviato un'indagine sul medesimo tema e *(ii)* il DSC di uno Stato membro abbia ragione di sospettare che uno specifico fornitore abbia violato regolamento *producendo ripercussioni negative sui destinatari del servizio in tale Stato membro*, tale DSC può chiedere al coordinatore competente di valutare la questione e adottare le misure necessarie per il rispetto del DSA.

Inoltre, *(i)* qualora la Commissione non abbia già avviato un'indagine sul medesimo tema e *(ii)* *almeno tre* DSC abbiano ragione di sospettare che ragione di sospettare che uno specifico fornitore abbia violato regolamento *producendo ripercussioni negative sui destinatari del servizio in tali Stati membri*, *il comitato* può chiedere al coordinatore competente di valutare la questione e adottare le misure necessarie per il rispetto del DSA.

A norma del paragrafo 4 dell'articolo 58, il coordinatore cui sono rivolte tali richieste deve *tenerle «nella massima considerazione»* e, ai sensi del paragrafo 5, comunicare senza ingiustificato ritardo, e comunque entro due mesi dal ricevimento della richiesta, la valutazione della presunta violazione nonché una spiegazione delle misure eventualmente adottate.

Qualora tale comunicazione non pervenga nel termine previsto, oppure esso non concordi con le valutazioni o le misure adottate dal DSC, il comitato, ex articolo 59, potrà deferire la questione alla Commissione. A seguito di tale deferimento, essa avrà il dovere di valutare la richiesta entro due mesi e, se ritiene di non concordare con la posizione del coordinatore competente in quanto la valutazione o le misure adottate sono insufficienti per garantire l'effettiva applicazione del DSA o incompatibili con esso, comunica il proprio parere al DSC, chiedendogli di *riesaminare la questione* (art. 59, par. 3, c. 1, DSA). Tale DSC deve «tenere nella massima considerazione» il parere e la richiesta di riesame della Commissione (art. 59, par. 3, c. 2, DSA).

La disamina deve essere completata con l'articolo 63, paragrafo 2, il quale prevede che un DSC, qualora intenda non seguire i pareri, le richieste o le raccomandazioni adottate dal comitato, debba *giustificare tale scelta* «fornendo una spiegazione sulle indagini, le azioni e le misure che hanno attuato nell'ambito delle relazioni previste dal presente regolamento o al momento di adottare le decisioni pertinenti».

È discutibile come la disciplina sinora presentata sia effettivamente in grado di assicurare coerenza ed uniformità al sistema. Il ruolo del comitato può essere

definito come genuinamente consultivo, nel senso che i suoi poteri si limitano all'emanazione di pareri che non sono, tuttavia, vincolanti. Infatti, è vero che il DSA prevede la necessità per il coordinatore di «tenere nella massima considerazione» le richieste del comitato o della Commissione e che il parere possa essere disatteso motivando. Tuttavia, non sono presenti norme volte a rendere possibile al comitato di imporre *coattivamente* la propria posizione su quella del DSC competente. La dottrina concorda con questa tesi, sottolineando come il comitato non abbia alcun potere decisionale, sanzionatorio o prescrittivo nei confronti degli Stati membri e delle loro autorità che adottino decisioni difformi dai pareri, raccomandazioni o richieste adottate dallo stesso.[21]

Ciò differisce da quanto previsto in materia di protezione dei dati. Infatti, l'articolo 65 GDPR prevede che l'EPDB emani dei veri e propri pareri *vincolanti*, i quali *devono* essere seguiti dall'autorità di controllo cui sono indirizzati. Qualora ciò non avvenga, si può ipotizzare che *(i)* la decisione dell'autorità che si discosti dal parere possa essere impugnata davanti al competente giudice nazionale, il quale procederà ad annullarla. Inoltre, come si è visto nel paragrafo 2.9, *(ii)* è possibile che la Commissione promuova un ricorso per infrazione nei confronti di tale Stato membro. Tirando le somme, se il GDPR non prevede la possibilità di dipartire dalla posizione presa dall'EPDB ex articolo 65, l'articolo 63 DSA concede tale facoltà quando il dissenso sia motivato. È ben vero che anche lo scostamento da un parere non vincolante può essere causa di annullamento della decisione del coordinatore, qualora, appunto, la motivazione fornita da quest'ultima per essersi discostata sia viziata.[22] Tuttavia, la percorribilità di questa soluzione è dipendente dai diritti nazionali e lascia aperto un margine di incertezza circa la valutazione che il giudice potrà fare.

È per queste ragioni – unite al ruolo centrale della Commissione nel DSA, invece assente nel GDPR – che devono essere lette con attenzione alcune posizioni dottrinali, secondo cui sarebbe possibile «intravedere una volontà di coerenza legislativa» tra DSA e GDPR.[23] Infatti, se ciò può essere vero con riferimento al funzionamento dell'assistenza reciproca e alle indagini comuni (ambiti cui, a dire il vero, tale dottrina sembra specificamente riferirsi), nonché per quanto riguarda la composizione dei due organi,[24] altrettanto non si può affermare con riferimento

21 Pavese, «Comitato» cit., p. 201.

22 Con riferimento al diritto amministrativo italiano si v. M. Occhiena e N. Posteraro, «Pareri e attività consultiva della pubblica amministrazione: dalla decisione migliore alla decisione tempestiva», *Il diritto dell'economia*, 100, 3 (2019), p. 48-49.

23 Priolo, «Coordinatori dei servizi digitali» cit., p. 215.

24 Sabia, «L'enforcement pubblico del Digital Services Act» cit., p. 102.

al meccanismo di coerenza sin qui presentato, proprio in ragione della diversità di ruoli dei due comitati.

In conclusione, tornando al DSA, il sistema individuato non sembra andare nella direzione di favorire una tempestiva ed uniforme applicazione del regolamento in esame e fa chiedere all'interprete per quale motivo il legislatore non abbia voluto adottare una disciplina più stringente nei confronti dei DSC, specie dopo l'esperienza del GDPR, ove si è notata la reticenza delle autorità di controllo a seguire le indicazioni dell'EPDB. L'unica consolazione sta nel fatto che, come si vedrà (v. *infra* parr. 3.5 e 3.7), in relazione ai casi che, in tema di protezione dei dati, hanno suscitato le maggiori problematiche – ossia quelli riguardanti le cd. *big tech*, quasi tutte sottoposte alla vigilanza dell'Irlanda – questi sono sottoposti, in quanto VLOP, ad un ruolo penetrante della Commissione e, dunque, parzialmente indifferenti ai problemi sinora illustrati.

3.5 *I poteri della Commissione: presentazione generale*

Come si è anticipato, il DSA attribuisce alla Commissione europea – per le ragioni che verranno poi esaminate al paragrafo 3.7 – significativi poteri in materia di applicazione e vigilanza dello stesso, soprattutto nei confronti delle VLOP. Innanzitutto, a norma dell'articolo 67, la Commissione può – al fine di svolgere efficacemente gli altri compiti – richiedere alla VLOP o a soggetti terzi di fornire, entro un termine ragionevole, informazioni relative ad una presunta violazione. Tale potere può essere esercitato o mediante una «semplice richiesta» o tramite una decisione. La norma non specifica quale sia il criterio per optare per l'uno o per l'altro strumento. Le uniche due indicazioni che vengono fornite sembrano essere le seguenti: *(i)* con una decisione è possibile anche imporre una penalità di mora ex articolo 76 DSA; *(ii)* sempre con riferimento alla decisione, il paragrafo 4 precisa che la Commissione deve «[indicare] inoltre il diritto di chiedere il riesame della decisione alla Corte di giustizia dell'Unione europea».

In relazione a quest'ultimo punto, esso non deve essere interpretato nel senso di limitare la possibilità di ricorrere alla Corte solo nei confronti di una decisione *e non di una semplice richiesta*. Infatti, ciò significherebbe ammettere che la Commissione possa scegliere, senza alcuno specifico criterio, che alcuni provvedimenti non possano essere oggetto di ricorso davanti ad un giudice. Ciò sarebbe in violazione del diritto ad un rimedio giurisdizionale effettivo di cui all'articolo 47 della Carta. Bisogna ricordare che, per giurisprudenza costante della Corte, nessun atto adottato nell'ambito del sistema istituzionale dell'Unione può sfuggire al controllo giurisdizionale di legittimità, qualora tale atto sia diretto a produrre

effetti giuridici nei confronti dei terzi.[25] Inoltre, la giurisprudenza ha affermato l'irrilevanza del *nomen iuris* dell'atto ai fini della sua impugnabilità,[26] dovendosi guardare alla *sostanza* dell'atto per determinare se esso produce tali effetti giuridici.[27] Più in generale, la Corte ha ribadito che «l'azione di annullamento deve potersi esperire nei confronti di qualsiasi provvedimento adottato dalle istituzioni (indipendentemente dalla sua natura e dalla sua forma) che miri a produrre effetti giuridici».[28]

Il procedimento di accertamento della violazione (e, successivamente, di irrogazione di una sanzione) viene avviato a norma dell'articolo 66 e termina con una «decisione di non conformità» ex articolo 73. In base al primo, quando sussista il sospetto che un fornitore abbia violato talune disposizioni del DSA, la Commissione avvia il procedimento e ne dà notifica ai DSC, al comitato e al fornitore stesso (art. 66, par. 2, c. 1 DSA). Ciò ha anche l'effetto di «esonerare» i DSC dai loro poteri di vigilanza, a norma dell'articolo 56, paragrafo 4 (art. 66, par. 2, c. 3 DSA).

Successivamente, la Commissione deve comunicare le proprie constatazioni preliminari alla VLOP, spiegando le misure che intende adottare o che ritiene che il fornitore dovrebbe adottare (art. 73, par. 2, DSA). La trasmissione di tali constatazioni preliminari è funzionale a garantire al fornitore il diritto di difesa. Infatti, l'articolo 79 prevede che, prima di adottare una decisione definitiva, la Commissione debba dare la possibilità al fornitore di essere ascoltato in merito alle costatazioni preliminari e alle misure che la Commissione intende adottare. A tale scopo, il fornitore può presentare le proprie osservazioni entro un termine fissato dalla Commissione nelle constatazioni, comunque non inferiore a 14 giorni (art. 79, par. 2, DSA). Il paragrafo 3 dell'articolo 79 prevede che la Commissione possa porre alla base della sua decisione finale *solo le obiezioni in merito alle quali le parti hanno avuto la possibilità di esprimersi*: la norma viene ritenuta dalla dottrina molto rilevante,[29] e ciò a ragione, in quanto contribuisce a rendere effettivo il diritto di partecipazione al procedimento e pone in capo alla Commissione l'onere di redigere molto attentamente le constatazioni preliminari. Tornando all'articolo 73,

25 Daniele, *Diritto dell'Unione europea* cit., p. 378; in giurisprudenza si v. Corte giust., causa C-294/83, *Parti écologiste Les Verts* cit.

26 Trib. UE, sentenza dell'8 maggio 2018, causa T-283/15, *Esso Raffinage c. Agenzia europea per le sostanze chimiche*, ECLI:EU:T:2018:263, § 49; Trib. UE, sentenza del 4 marzo 2015, causa T-496/11, *Regno Unito di Gran Bretagna e Irlanda del Nord c. Banca centrale europea (BCE)*, ECLI:EU:T:2015:133, § 30.

27 Corte giust., sentenza del 20 febbraio 2018 (Grande Sezione), causa C-16/16 P, *Regno del Belgio c. Commissione europea*, ECLI:EU:C:2018:79, § 32.

28 Corte giust., sentenza del 16 giugno 1993, causa C-325/91, *Repubblica francese c. Commissione delle Comunità europee*, ECLI:EU:C:1993:245, § 9.

29 Priolo, «Coordinatori dei servizi digitali» cit., p. 223.

come si è detto, il procedimento si conclude con una decisione di non conformità, con la quale la Commissione ordina al fornitore di adottare le misure necessarie entro un termine ivi fissato (art. 73, par. 3, DSA).

Con la medesima decisione, la Commissione può anche infliggere al fornitore sanzioni pecuniarie di diverso importo. In particolare, qualora tale fornitore (*i*) violi le pertinenti disposizioni del presente regolamento, (*ii*) non rispetti una decisione che dispone misure provvisorie a norma dell'articolo 70, oppure (*iii*) non si conformi a un impegno reso vincolante da una decisione adottata a norma dell'articolo 71, l'importo potrà essere «non superior[e] al 6% del fatturato totale realizzato a livello mondiale su base annua dal fornitore nell'esercizio precedente». Un limite massimo minore (dell'1% del fatturato annuo mondiale) è previsto in relazione a violazioni ritenute meno gravi, in particolare per il caso in cui le VLOP: (*i*) forniscano informazioni inesatte, incomplete o fuorvianti in risposta a una semplice richiesta o a una richiesta formulata mediante decisione ai sensi dell'articolo 67; (*ii*) non rispondano alla richiesta di informazioni formulata mediante decisione entro il termine stabilito; (*iii*) omettano di rettificare, entro il termine fissato dalla Commissione, le informazioni inesatte, incomplete o fuorvianti fornite da un membro del personale, oppure omettano o rifiutino di fornire informazioni complete; (*iv*) rifiutino di sottoporsi a un'ispezione a norma dell'articolo 69; (*v*) non rispettino i provvedimenti adottati dalla Commissione a norma dell'articolo 72; oppure (*vi*) non rispettino le condizioni di accesso al fascicolo della Commissione a norma dell'articolo 79, paragrafo 4. L'articolo 81 DSA ricorda che, come già previsto dall'articolo 261 TFUE, la Corte di giustizia conosce delle controversie relative alle sanzioni (e alle penalità di mora di cui all'articolo 76) *anche nel merito*.

3.6 *La restrizione dell'accesso ex articolo 82 DSA*

Merita un'accurata analisi l'articolo 82, rubricato «Richieste di restrizione dell'accesso e cooperazione con i giudici nazionali». Il paragrafo 1 prevede che (*i*) qualora siano stati esauriti tutti i poteri previsti dalla sezione 4 del capo IV per far cessare una violazione e (*ii*) quest'ultima persista (*iii*) causando un danno grave, (*iv*) il quale non possa essere evitato mediante l'esercizio di altri poteri previsti dal diritto dell'Unione o nazionale, la Commissione possa *chiedere al DSC del luogo di stabilimento del fornitore* in questione di agire ai sensi dell'articolo 51, paragrafo 3. Quest'ultima norma, già analizzata nel paragrafo 3.3, prevede il potere del DSC di chiedere all'autorità giudiziaria competente di ordinare la restrizione dell'accesso alla piattaforma. Si deve osservare che il legislatore ha attribuito ai giudici nazionali, e non alla Commissione, il potere di restringere l'accesso. Si tratta, sicuramente, di una scelta da accogliere con favore. Infatti, anche in ragione della circostanza

per cui la Commissione non è un'istituzione indipendente (v. *infra* par. 3.7), appare molto più opportuno concedere tale potere all'autorità giudiziaria, dotata dei requisiti di indipendenza e terzietà. Questo in ragione della natura molto penetrante di simili provvedimenti restrittivi dell'accesso, i quali sono potenzialmente idonei a ledere i diritti fondamentali dell'individuo, in particolare il diritto di manifestare liberamente il proprio pensiero.

A tal riguardo, si deve richiamare la giurisprudenza della Corte europea dei diritti dell'uomo, la quale si è più volte pronunciata circa la compatibilità di simili provvedimenti con l'articolo 10 CEDU. Quest'ultima norma mira a tutelare la libertà di espressione e dispone che l'esercizio della stessa possa essere limitato solo (*i*) quando ciò sia previsto dalla legge, (*ii*) per mezzo di «misure necessarie, in una società democratica», (*iii*) alla tutela di determinati valori, quali la sicurezza nazionale, l'integrità territoriale, la difesa dell'ordine e la prevenzione dei reati, la protezione della reputazione o dei diritti altrui. In particolare, la Corte EDU ha precisato che Internet riveste un ruolo importante nell'accrescere le possibilità di accesso alle notizie da parte del pubblico e nel diffondere le informazioni in generale,[30] con l'avvertenza che tale libertà è concessa a tutti gli individui (siano essi persone fisiche o giuridiche) e si applica sia al contenuto delle informazioni che al mezzo di diffusione delle stesse.[31]

Nel caso *Ahmet Yıldırım c. Turchia* la Corte – ribadendo che «*the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest*»[32] – ha esaminato la compatibilità con l'articolo 10 CEDU di una misura emanata da un tribunale turco, la quale aveva disposto il blocco agli accessi dell'*intera* piattaforma *Google Sites*,[33] ivi incluso il sito del ricorrente. L'opinione dei giudici di Strasburgo è, innanzitutto, che un provvedimento simile sia una misura restrittiva della libertà di cui all'articolo 10.[34] La Corte ritiene violato il requisito della riserva di legge, in quanto, pur esistendo alla base una norma del diritto turco, essa era eccessivamente indeterminata. Infatti, quest'ultima non limitava il potere del giudice, non imponendogli di effettuare un bilanciamento

30 Corte EDU, sentenza del 10 marzo 2009, *Times Newspapers Ltd c. Regno Unito*, ECHR:2009:0310JUD000300203, § 27.

31 Corte EDU, sentenza del 13 febbraio 2003, *Çetin e a. c. Turchia*, ECHR:2003:0213JUD004015398, § 57.

32 Corte EDU, sentenza del 18 dicembre 2012, *Ahmet Yıldırım c. Turchia*, ECHR:2012:1218JUD000311110, § 54.

33 Per un caso simile riguardante la piattaforma *YouTube* si v. Corte EDU, sentenza del 1 dicembre 2015, *Cengiz e a. c. Turchia*, ECHR:2015:1201JUD004822610.

34 Ivi, § 55.

degli interessi e non disponendo che egli dovesse bloccare solo *la specifica pagina web oggetto della violazione*.[35] Inoltre, il giudice non avrebbe considerato il fatto che un simile provvedimento, rendendo grandi quantità di informazioni non accessibili, ha sostanzialmente limitato i diritti degli utenti di Internet e generato significativi effetti collaterali.[36]

Tale argomentazione è stata ribadita anche successivamente nel caso *Vladimir Kharitonov c. Russia*[37] il quale, in maniera simile al precedente, aveva ad oggetto un cd. «*wholesale blocking*», ossia il blocco di un'intera piattaforma a seguito della ritenuta contrarietà alla legge di una singola pagina. Anche in questo caso, la Corte di Strasburgo ha ritenuto sussistente una violazione dell'articolo 10 CEDU, pressoché per le stesse motivazioni di *Yıldırım*, se non fosse che qui la situazione si presentava ancora più grave poiché il blocco era stato ordinato non da un giudice ma da un'autorità governativa (*Roskomnadzor*).[38]

Pertanto, le condizioni poste dalla Corte EDU per considerare i provvedimenti in esame legittimi sembrano essere le seguenti: la restrizione deve essere disposta (*i*) in base alla legge – la quale deve essere sufficientemente precisa, tanto da non lasciare in capo al giudice un margine di arbitrarietà – e (*ii*) da parte di un giudice (ovviamente, terzo ed imparziale), mediante un procedimento che assicuri che le parti siano sentite. Inoltre, (*iii*) esse devono essere quanto più "mirate" possibile, dovendo andare a colpire solo la specifica pagina oggetto della violazione e non tutto il sito.[39]

Dal punto di vista della Carta dei diritti fondamentali dell'Unione europea, l'articolo 11 della stessa sancisce il diritto di ogni persona alla libertà di espressione. Una limitazione di tale diritto è consentita solo rispettando quanto previsto dall'articolo 52, paragrafo 1, il quale fissa, secondo la Corte, una «triplice condizione»:[40]

35 Ivi, § 64.

36 Ivi, § 66.

37 Corte EDU, sentenza del 23 giugno 2020, *Vladimir Kharitonov c. Russia*, ECHR:2020:0623JUD001079514; per un commento in dottrina si v. E. Izyumenko, «European Court of Human Rights rules that collateral website blocking violates freedom of expression», *Journal of Intellectual Property Law & Practice*, 15, 10 (2020).

38 Ivi, § 43: «*Roskomnadzor gave effect to a decision by which a drug-control agency had determined the content of the offending website to be illegal. Both the original determination and Roskomnadzor's implementing orders had been made without any advance notification to the parties whose rights and interests were likely to be affected. The blocking measures had not been sanctioned by a court or other independent adjudicatory body providing a forum in which the interested parties could have been heard*».

39 Ciò, si deve ritenere, è richiesto anche dal principio di proporzionalità, espresso nell'articolo 10 CEDU dalla formula «misure necessarie in una società democratica».

40 Trib. UE, sentenza del 27 febbraio 2014, causa T-256/11, *Ahmed Abdelaziz Ezz e a. c. Consiglio dell'Unione europea*, ECLI:EU:T:2014:93, § 197.

(*i*) essere prevista dalla legge,[41] ossia avere un «fondamento normativo»[42]; (*ii*) perseguire un obiettivo di interesse generale, riconosciuto come tale dall'Unione;[43] (*iii*) non essere eccessiva, nel senso che, da una parte, essa deve essere necessaria e proporzionata allo scopo prefissato e, dall'altra, non ledere il contenuto essenziale del diritto.[44] Come si nota, tali condizioni sono sostanzialmente identiche a quelle previste dalla CEDU,[45] così come lo è anche la giurisprudenza della Corte di giustizia dell'Unione europea. Innanzitutto, nel caso *UPC Telekabel Wien*, la Corte ha affermato che

> le misure adottate dal fornitore di accesso ad Internet devono essere rigorosamente mirate, nel senso che devono servire a porre fine alla violazione arrecata da parte di un terzo al diritto d'autore o a un diritto connesso, senza pregiudizio degli utenti di Internet che ricorrono ai servizi di tale fornitore al fine di accedere lecitamente ad informazioni. Nel caso contrario, l'ingerenza di detto fornitore di accesso nella libertà di informazione di tali utenti sarebbe ingiustificata alla luce dell'obiettivo perseguito.[46]

Inoltre, in *Polonia c. Parlamento e Consiglio*, la Corte – giudicando sulla compatibilità di una norma che impone agli intermediari un certo tipo di monitoraggio dei contenuti con l'articolo 11 della Carta – ha, innanzitutto, ritenuto che una simile misura sia, effettivamente, idonea ad incidere sul diritto alla libera manifestazione del pensiero.[47] Successivamente, ha reputato, però, tale restrizione giustificata, andando a verificare le tre condizioni appena enunciate.[48] Ritengono i giudici che:

41 Corte giust., sentenza del 1 luglio 2010, causa C-407/08 P, *Knauf Gips KG c. Commissione europea*, ECLI:EU:C:2010:389, § 91.

42 Trib. UE, causa T-256/11, *Ezz e a./Consiglio* cit., § 198.

43 Trib. UE, sentenza del 4 dicembre 2015, causa T-273/13, *Mohammad Sarafraz c. Consiglio dell'Unione europea*, ECLI:EU:T:2015:939, § 182; Trib. UE, causa T-256/11, *Ezz e a./Consiglio* cit., § 199.

44 Trib. UE, causa T-273/13, *Sarafraz/Consiglio* cit., § 184; Trib. UE, causa T-256/11, *Ezz e a./Consiglio* cit., § 200; Corte giust., sentenza del 3 settembre 2008 (Grande Sezione), cause riunite C-402/05 P e C-415/05 P, *Yassin Abdullah Kadi e Al Barakaat International Foundation c. Consiglio dell'Unione europea e Commissione delle Comunità europee*, ECLI:EU:C:2008:461, § 355, 360.

45 Trib. UE, sentenza del 27 luglio 2022 (Grande Sezione), causa T-125/22, *RT France c. Consiglio dell'Unione europea*, ECLI:EU:T:2022:483, § 146.

46 Corte giust., sentenza del 27 marzo 2014, causa C-314/12, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, § 56; per una critica a questa pronuncia si v. C. Angelopoulos, «Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape», *Journal of Intellectual Property Law & Practice*, 9, 10 (2014), p. 817, in cui l'autrice osserva che la Corte si rifiuta di pronunciarsi su come bilanciare i diritti fondamentali degli individui e demanda tale operazione agli intermediari.

47 Corte giust., sentenza del 26 aprile 2022 (Grande Sezione), causa C-401/19, *Repubblica di Polonia c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:2022:297, § 55-58.

48 Ivi, § 63.

(*i*) tale restrizione sia prevista dalla legge,[49] (*ii*) «rispond[a] all'esigenza di proteggere i diritti e le libertà altrui»,[50] (*iii*) rispetti il contenuto essenziale del diritto alla libertà di espressione e d'informazione[51] e non lo limiti in modo sproporzionato.[52]

Prima di passare a verificare se tali condizioni siano sussistenti anche con riferimento alle restrizioni di cui all'articolo 82 DSA (e, di conseguenza, anche di cui all'articolo 51, paragrafo 3, DSA), sono doverose alcune premesse. La prima attiene all'applicabilità della CEDU (e della giurisprudenza della Corte EDU) anche alle istituzioni dell'Unione. A tal riguardo, senza dubbio bisogna rispondere affermativamente, ricordando che l'articolo 52, paragrafo 3, così recita: «Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione». Difatti, nel caso *Polonia c. Parlamento e Consiglio* appena citato, la Corte di giustizia ha affermato che «[c]ome risulta dalle spiegazioni relative alla Carta dei diritti fondamentali […] , e conformemente all'articolo 52, paragrafo 3, della Carta, i diritti garantiti dall'articolo 11 di quest'ultima hanno significato e portata identici a quelli garantiti dall'articolo 10 della CEDU»[53] e si è più volte richiamata alla giurisprudenza della Corte EDU, per trarne i principi *supra* presentati.[54]

La seconda precisazione attiene invece alla diversa natura dei casi davanti alla Corte EDU rispetto a quelli giudicati dalla Corte di giustizia. Infatti, si può notare come i primi – soprattutto quelli che vedevano come convenuta la Federazione Russa – avevano ad oggetto Stati non membri dell'Unione europea in cui non è garantito lo Stato di diritto, cosicché, in tali casi, i giudici avrebbero «analizza[to] la libertà di espressione come scudo nei confronti delle autorità statali che, in ragione delle opinioni assunte da un soggetto, adottino provvedimenti persecutori nei suoi confronti».[55] Tale considerazione è sicuramente vera; ciò non toglie, però, che i principi in essi stabiliti siano validi in generale.

Passando all'articolo 82, si deve ritenere che questo risponda ai requisiti finora enunciati. Innanzitutto, (*i*) la restrizione è prevista dalla legge (in questo caso, dal DSA); (*ii*) è disposta da un giudice all'esito di un procedimento che prevede l'esercizio del diritto di difesa delle parti (anche se, bisogna osservare, la parte che

49 Ivi, § 72.
50 Ivi, § 82.
51 Ivi, § 76.
52 Ivi, § 84.
53 Ivi, § 44.
54 Ivi, § 46, 68.
55 A. Maffeo, «Misure restrittive contro la Russia: il Tribunale rigetta la richiesta di sospensione di *RT France*», *Eurojus*, 2 (2022), p. 311.

viene lesa del diritto all'informazione non è tanto la VLOP quanto *l'individuo* che, tramite essa, manifesta il proprio pensiero o si informa); *(iii)* mira a perseguire un obiettivo di interesse generale, cioè evitare un danno grave e fare sì che venga cessata una condotta che costituisce un reato grave che comporta una minaccia per la vita e la sicurezza delle persone (art. 51, par. 3, lett. b), DSA). *(iv)* Il requisito della proporzionalità è quello che deve essere indagato con più accuratezza. Infatti, si è già detto *supra* (v. par. 3.3), come in dottrina abbia suscitato qualche perplessità la previsione di un termine fisso di quattro settimane, non modificabile da parte dell'autorità giudiziaria. A parte tale dubbio, bisogna osservare come il combinato disposto tra l'articolo 82, paragrafo 1, e l'articolo 51, paragrafo 3, lettera b), individui una serie di requisiti molto stringenti affinché sia possibile adottare una simile restrizione. Essa si configura come un'*extrema ratio*, essendo, dunque, adottabile solo nel momento in cui altri provvedimenti non siano efficaci. Peraltro, l'articolo 51, paragrafo 3, comma 2, dispone esplicitamente che «[l]e misure disposte devono essere proporzionate alla natura, alla gravità, alla reiterazione e alla durata della violazione e non devono limitare indebitamente l'accesso alle informazioni lecite da parte dei destinatari del servizio interessato».

3.7 *Il ruolo di* enforcer *della Commissione: una valutazione critica*

Come si è visto, nell'impianto del DSA la Commissione riveste un ruolo centrale per quanto riguarda l'applicazione del regolamento, soprattutto con riferimento al campo delle VLOP, ove è titolare di competenze esclusive.[56] L'attribuzione alla Commissione di ruoli di vigilanza ed, eventualmente, sanzionatori, è, se si assume una prospettiva ampia, un fenomeno non nuovo: si veda, in particolare, l'ambito del diritto della concorrenza. Allo stesso tempo, però, questa scelta si presenta come innovativa dal punto di vista della regolazione dei servizi digitali, in quanto in questo campo il legislatore aveva generalmente optato per un modello di *enforcement* decentrato (si veda, tra tutti, quello del GDPR illustrato nel capitolo 2).

Con riferimento alle VLOP, la *ratio* principale dell'individuazione di un meccanismo di *enforcement* centralizzato deve essere ricondotta alla volontà di evitare i problemi che si sono posti (e che si pongono ancora oggi) in relazione all'attuazione di varie norme dell'Unione, in particolare del GDPR.[57] Si è visto, infatti, che

56 Sabia, «L'enforcement pubblico del Digital Services Act» cit., p. 112.

57 I. Buri, «A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer», in *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications*, a cura di J. Hoboken et al., Verfassungsbooks, Berlin 2023, p. 77; I. Buri e J. van Hoboken, «The DSA supervision and enforcement architecture», *DSA Observatory*

l'attuazione transfrontaliera[58] di quest'ultimo si presenta – specie nei confronti proprio di quei titolari del trattamento che rientrano all'interno della categoria delle VLOP, pressoché tutti aventi stabilimento principale in Irlanda – come non ottimale, per le ragioni ampiamente illustrate nel capitolo precedente.

Tali intenti accentratori del legislatore riposano, sicuramente, su ragioni più che valide e giustificate, tanto che in dottrina si sono manifestate simili tendenze accentratrici anche in relazione al GDPR.[59] Tuttavia, il presente paragrafo tenterà di sostenere come – fermo restando quanto appena affermato – l'errore in cui sia caduto il legislatore del DSA è di aver diretto tale accentramento a favore della Commissione. Ciò (*i*) sia perché tale scelta si presenta come irragionevole, se confrontata con quanto previsto per il DSC; (*ii*) sia perché, da un punto di vista strategico-opportunistico, è questionabile che la Commissione sia effettivamente l'istituzione che più efficacemente rispetto ad ogni altra può attuare il DSA.

Per comprendere il primo punto, si deve partire dalla seguente considerazione: l'articolo 50, paragrafo 1, del DSA, prevede che i coordinatori dei servizi digitali svolgano i loro compiti «in modo imparziale» e che gli Stati membri assicurino che il proprio coordinatore dei servizi digitali «disponga di sufficiente autonomia per gestire il suo bilancio […] al fine di non incidere negativamente sull'indipendenza del coordinatore dei servizi digitali». Inoltre, il paragrafo 2 del medesimo articolo specifica che:

> [n]ello svolgimento dei loro compiti e nell'esercizio dei loro poteri in conformità del presente regolamento, i coordinatori dei servizi digitali agiscono in piena indipendenza. Essi non devono subire alcuna influenza esterna, diretta o indiretta, e non sollecitano né accettano istruzioni da altre autorità pubbliche o da privati.

Si tratta di previsioni del tutto analoghe a quelle previste in relazione al diritto alla protezione dei dati, in particolare dall'articolo 52 GDPR e dall'articolo 28 della previgente direttiva 95/46/CE. A tal riguardo, è possibile recuperare la giurisprudenza della Corte di giustizia, in quanto si deve ritenere che i principi da essa enunciati siano applicabili anche al requisito di indipendenza fissato dal DSA. In *Commissione c. Germania*,[60] la Corte ha, innanzitutto, ricordato che le autorità

(24 giugno 2022), (visitato il 13/10/2023).

58 Ci si riferisce qui all'attuazione transfrontaliera, in quanto il parallelismo viene effettuato nei confronti delle VLOP, le quali – coinvolgendo più di 45 milioni di utenti – quasi sicuramente sono attive in più di uno Stato membro.

59 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit.

60 Corte giust., sentenza del 9 marzo 2010 (Grande Sezione), causa C-518/07, *Commissione europea c. Repubblica federale di Germania*, ECLI:EU:C:2010:125; si v. anche i successivi casi Corte giust., sentenza del 8 aprile 2014 (Grande Sezione), causa C-288/12, *Commissione europea c. Ungheria*, ECLI:EU:C:2014:237; Corte giust., sentenza del 16 ottobre 2012 (Grande Sezione), causa C-614/10, *Commissione europea c. Repubblica d'Austria*, ECLI:EU:C:2012:631.

di controllo sono «le custodi dei menzionati diritti e libertà fondamentali»[61] e, pertanto, «[a] tale fine esse devono essere sottratte a qualsiasi influenza esterna, *compresa quella, diretta o indiretta, dello Stato o dei Länder*, e non solamente essere poste al riparo dall'influenza degli organismi controllati».[62] È, quindi, necessario che il potere esecutivo non possa, in alcun modo, esercitare un'influenza sull'attività dell'autorità. Ciò, innanzitutto, perché lo svolgimento indipendente delle funzioni dell'autorità può essere ostacolato dal «solo rischio che le autorità di vigilanza possano esercitare un'influenza politica sulle [sue] decisioni».[63] Inoltre, osservano i giudici, tale influenza potrebbe comportare che il governo tenda a «privilegiare interessi economici nell'applicazione di dette disposizioni da parte di talune società importanti, da un punto di vista economico, per il Land o la regione».[64]

Come si è detto, questi requisiti, seppur enunciati con riferimento al diritto della protezione dei dati, devono ritenersi estensibili anche alle autorità nazionali che attuano il DSA.

Ebbene, dopo aver fatto tutte queste osservazioni, si constata che una parte dell'attuazione del regolamento in esame – una *grande* parte, visto che le VLOP sono le piattaforme più usate dagli utenti – è, tuttavia, demandata ad un soggetto che *indipendente non è*: la Commissione europea. Essa, dovendo avere l'avallo del Parlamento europeo ed detenendo il potere esecutivo dell'Unione, si presenta come un'istituzione fortemente politicizzata.[65] Si assiste, dunque, al fenomeno per cui il legislatore europeo, dopo aver prescritto stringenti requisiti di indipendenza nei confronti delle autorità nazionali, attribuisce il compito di attuare il DSA – nella sua parte più complessa e impattante nei confronti dei destinatari – ad un soggetto non indipendente.

A questo proposito, sono necessarie alcune precisazioni. Bisogna riconoscere che alla Commissione europea sono già attribuiti significativi poteri di *enforcement* in altri ambiti, soprattutto in quello della concorrenza, tanto che, con riferimento al DSA, la stessa afferma che «disporrà di poteri esecutivi analoghi a quelli di

61 Ivi, § 23.
62 Ivi, § 25, corsivo aggiunto.
63 Ivi, § 36.
64 Ivi, § 35.
65 Sulla progressiva politicizzazione della Commissione si v. A. Wille, «The politicization of the EU Commission: democratic control and the dynamics of executive selection», *International Review of Administrative Sciences*, 78, 3 (2012); si v. anche Buri, «A Regulator Caught Between Conflicting Policy Objectives» cit., p. 79; N. Nugent e M. Rhinard, «The 'political' roles of the European Commission», *Journal of European Integration*, 41, 2 (2019); C. Rauh, «EU politicization and policy initiatives of the European Commission: the case of consumer policy», *Journal of European Public Policy*, 26, 3 (2019).

cui dispone nell'ambito dei procedimenti antitrust».[66] Per la verità, anche con riferimento a quest'ultimo campo sono sorti, in passato, dubbi circa l'affidamento di compiti di *enforcement* in capo alla Commissione, proprio in ragione della sua natura (anche) politica.[67] Tuttavia, tali dubbi – comprese le istanze per la creazione di un'apposita agenzia europea per la concorrenza – paiono ora essersi sopiti, soprattutto in ragione del fatto che la DG Concorrenza gode di una significativa autonomia dal Collegio dei commissari e, pertanto, «agisce già come se fosse un'agenzia».[68]

Quello che sembra più importante precisare è che – almeno in una prospettiva *de iure (primario) condito* – questa discussione rischia, forse, di trasformarsi in puramente ipotetica se si considera che, in questa materia, è il diritto primario stesso (art. 105 TFUE) ad affidare alla Commissione il compito di attuare gli articoli 101 e 102 TFUE,[69] rendendola «responsabile dall'attuazione e dell'orientamento della politica comunitaria della concorrenza».[70] Invece, con riferimento al DSA, l'attribuzione di competenze penetranti in capo alla Commissione non appare necessitata da alcuna norma dei Trattati.

I due ambiti non sembrano muoversi su piani completamente sovrapponibili anche per un altro motivo: è possibile sostenere che le *ratio* sottostanti all'individuazione del requisito dell'indipendenza siano diverse. Come acutamente rilevato da Wils, nell'ambito della protezione dei dati viene richiesta una «*completa* indipendenza», nozione che si può verosimilmente ritenere diversa da quella di mera e semplice «indipendenza» prevista dal diritto della concorrenza.[71] Difatti, secondo dottrina e giurisprudenza, quest'ultima nozione è da intendersi, principalmente, come indipendenza dagli operatori economici e dai loro interessi.[72] Nel caso c.d. «*Terminali di telecomunicazione*», la Corte ha precisato che la neces-

66 Così si legge sul comunicato stampa della Commissione europea del 23 febbraio 2024, `https://ec.europa.eu/commission/presscorner/detail/it/qanda_20_2348` (visitato il 23/03/2024).

67 G. Monti, «Independence, Interdependence and Legitimacy: The EU Commission, National Competition Authorities, and the European Competition Network», *EUI working papers LAW*, 01 (2014), p. 8-9.

68 Ivi, p. 10.

69 W. P. J. Wils, «Independence of Competition Authorities: The Example of the EU and Its Member States», *World Competition*, 42, 2 (2019), p. 151, 164.

70 Trib. UE, sentenza del 18 settembre 1992, causa T-24/90, *Automec Srl c. Commissione delle Comunità europee*, `ECLI:EU:T:1992:97`, § 73, che così continua: «l'art. 89, n. 1, del Trattato le affida il compito di vigilare sull'applicazione dei principi fissati dagli artt. 85 e 86 e la normativa emanata in base all'art. 87 le attribuisce poteri estesi».

71 Wils, «Independence of Competition Authorities» cit., p. 156.

72 ivi, p. 159; T. Hüttl, «The content of 'complete independence' contained in the Data Protection Directive», *International Data Privacy Law*, 2, 3 (2012), p. 143.

sità «di evitare che la concorrenza sia alterata e di assicurare l'uguaglianza delle opportunità fra i vari operatori»[73] comporta l'attribuzione delle competenze in materia di concorrenza «ad un ente indipendente *dalle imprese pubbliche o private che offrono beni e/o servizi concorrenti nel settore*».[74] Nel successivo caso *Decoster*, l'accento è rimasto sull'indipendenza tra autorità regolatrice e impresa (in questo caso, pubblica) che opera nel settore regolato.[75] Successivamente, si è ritenuto di ampliare questo concetto, includendovi anche un'indipendenza dal governo o, più in generale, dal potere politico. Se ciò è vero, bisogna, tuttavia, considerare che lo scopo principale dell'individuazione di una simile indipendenza politica sembra essere il perseguimento di una maggior *efficacia* di regolazione del settore.[76]

Invece, con riferimento alle autorità per la protezione dei dati, è sicuramente vero che «[l]a garanzia d'indipendenza […] è diretta ad assicurare che il controllo […] sia *efficace e affidabile*».[77] Tuttavia, vi è un altro elemento da considerare, ossia che l'esercizio dei poteri da parte di tali autorità è in grado di impattare – in senso favorevole o contrario – sui diritti fondamentali dell'individuo. Afferma la Corte che «[l]'istituzione, negli Stati membri, di autorità di controllo indipendenti costituisce […] un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali»,[78] essendo stata disposta «al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità».[79]

È in questo senso che deve essere interpretato anche il requisito di indipendenza fissato dal DSA. Negli ambiti attinenti alla libertà dei media (e, più in generale, di ciò che possa diffondere pensieri ed informazioni) e alla protezione dei dati personali, cui anche il DSA pertiene, normalmente vi è un'autorità indipendente,[80] in quanto i poteri esercitati da quest'ultima sono in grado di incidere sui diritti e le libertà fondamentali, quali la libertà di manifestazione del pensiero e il diritto alla protezione dei dati personali. Anche i poteri conferiti ai sensi del DSA sono in grado di incidere su simili valori. Ciò è vero anche senza tener conto del potere

73 Corte giust., sentenza del 19 marzo 1991, causa C-202/88, *Repubblica francese c. Commissione delle Comunità europee*, ECLI:EU:C:1991:120, § 4.

74 Ibidem, corsivo aggiunto.

75 Corte giust., sentenza del 27 ottobre 1993, causa C-69/91, *Procedimento penale contro Francine Decoster, in Gillon*, ECLI:EU:C:1993:853, § 5, 15-16, 19.

76 G. Eckert, «L'indépendance des autorités de régulation économique à l'égard du pouvoir politique», *Revue française d'administration publique*, 143, 3 (2012), p. 632-633.

77 Corte giust., causa C-362/14, *Schrems* cit., § 41, corsivo aggiunto.

78 Corte giust., causa C-288/12, *Commissione/Ungheria* cit., § 48.

79 Corte giust., causa C-362/14, *Schrems* cit., § 41.

80 B. Wagner e H. Janssen, «A first impression of regulatory powers in the Digital Services Act», *Verfassungsblog* (4 gennaio 2021), (visitato il 11/12/2023).

più penetrante, quello di restrizione dell'accesso, il quale è affidato ai giudici nazionali (v. *supra* par. 3.6). Difatti, attraverso l'esercizio di poteri di altra sorta – quali il potere di adottare misure cautelari (art. 70), i poteri di vigilanza rafforzata nei confronti delle VLOP (art. 75) e, più in generale, anche il potere di adottare decisioni di non conformità (art. 73) – la Commissione può influenzare in maniera penetrante le modalità con le quali i fornitori organizzano la propria piattaforma e, conseguentemente, modificare la portata dei diritti fondamentali che il DSA mira a proteggere, primo tra tutti il diritto alla libera manifestazione del pensiero.

Se le tesi finora riportate non hanno convinto, l'interessante analisi proposta da Buri mostra come l'attribuzione di simili competenze alla Commissione si presenta critica anche da un punto di vista efficientistico, in quanto potrebbe portare ad un'attuazione del DSA non ottimale. Infatti, molto frequentemente la Commissione raccoglie presso di sé una pluralità di ruoli, spesso rispondenti ad obiettivi potenzialmente in tensione tra di loro (ad esempio, promozione del mercato interno e del commercio internazionale contro protezione dei diritti fondamentali).[81]

Secondo l'autrice, un esempio di tale tensione si può rilevare in relazione alle decisioni di adeguatezza previste per il trasferimento di dati personali verso paesi terzi.[82] Si deve infatti ricordare che l'articolo 45 GDPR attribuisce alla Commissione il potere di autorizzare tale trasferimento tramite una propria decisione, qualora il paese terzo assicuri un adeguato livello di protezione. Dunque, si può comprendere come, in questi casi, la Commissione si trovi ad essere, da una parte, promotrice degli scambi commerciali tra due paesi – favorendo il flusso di dati verso un paese terzo – e, dall'altra, sia individuata dal legislatore dell'Unione come istituzione che deve fare da garante a che tali dati non siano trasferiti se non in presenza di un livello di protezione dei dati «sostanzialmente equivalente»[83] a quello presente nell'Unione. Il fatto che questa situazione comporti un problema dal punto di vista della tutela del diritto alla protezione dei dati personali è testimoniato dalla cd. «saga Schrems», ove la Corte di giustizia si è trovata ad annullare per due volte la decisione di adeguatezza della Commissione che autorizzava il trasferimento dei dati verso gli Stati Uniti, segnatamente dapprima la decisione «*Approdo Sicuro*»[84] e successivamente la decisione «*Scudo per la privacy*».[85] Anche

81 Buri, «A Regulator Caught Between Conflicting Policy Objectives» cit., p. 80.

82 Ivi, p. 81-82.

83 Corte giust., causa C-362/14, *Schrems* cit., § 73.

84 Decisione della Commissione 2000/520/CE del 26 luglio 2000 cit.

85 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, GU L 207, 01/08/2016, pp. 1–112.

in relazione alla decisione di adeguatezza «*EU-US Data Privacy Framework*»,[86] adottata recentemente e ora in vigore, sussistono significativi dubbi circa la sua compatibilità con i principi *Schrems*.[87]

A questo riguardo, parte della dottrina ipotizza che il potere di determinare il contenuto di una decisione di adeguatezza debba essere sostanzialmente spostato in capo all'EPDB, su modello di quanto avviene per l'ambito finanziario.[88] Le ragioni fornite sono quelle finora presentate: «*[t]he dramtic double-failure of the Commission in the Safe Harbour and the Privacy Shield regimes, which were invalidated by the CJEU for having violated the essence of EU fundamental rights, including the right to an effecive remedy*»[89] ha mostrato i problemi della Commissione a condurre simili valutazioni, incapacità che si ritiene derivi da «*its 'political capture', i.e. the Commission's mixing of foreign trade concerns with fundamental rights protection*».[90]

3.8 *Il coordinamento delle diverse autorità di regolazione dell'ambito digitale a partire dalla sentenza* Meta Platforms c. Bundeskartellamt

L'effettività dei meccanismi di *enforcement* sinora presentati deve essere analizzata anche dal punto di vista della cooperazione di autorità tra di loro *diverse*: autorità di controllo per la protezione dei dati, coordinatori dei servizi digitali, autorità per la concorrenza. Tale analisi è utile in quanto esse sono incaricate dell'attuazione di discipline non identiche, ma tra di loro compenetrate, cosicché una medesima fattispecie concreta (patologica) potrebbe essere presa in considerazione da vari punti di vista. In un ambito, come quello in esame, in cui si sono frequentemente

86 Decisione di esecuzione (UE) 2023/1795 della Commissione del 10 luglio 2023 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali, GU L 231, 20/09/2023, pp. 118–229.

87 NOYB ha già annunciato azioni volte a far invalidare anche questa decisione, si v. NOYB, «New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". *noyb* will challenge the decision.» (10/07/2023), `https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu` (visitato il 25/03/2024); in dottrina si v. S. Batlle e A. van Waeyenberge, «EU–US Data Privacy Framework: A First Legal Assessment», *European Journal of Risk Regulation*, 15, 1 (2024), p. 199-200; A. Ortega Giménez, «¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU.» *Cuadernos de Derecho Transnacional*, 16, 1 (2024); T. Gottschalk, «The EU-US Data Privacy Framework (DPF) – A Blueprint for International Data Transfers?», *European Data Protection Law Review*, 9, 4 (2023), p. 453.

88 Hofmann e Mustert, «Procedures Matter» cit., p. 5.

89 Ibidem.

90 Ibidem.

verificati problemi di attuazione pratica, l'utilizzo della tecnica appena enunciata può essere, in effetti, uno strumento utile al fine di fronteggiare con più fermezza alcune pratiche che il diritto considera scorrette. D'altra parte, però, un agire scoordinato di vari soggetti – che vadano tutti in una stessa direzione o meno – deve essere scongiurato, in quanto può portare ad un'individuazione e perseguimento degli illeciti riscontrati non ottimale. Il presente paragrafo si occuperà, quindi, di comprendere come possano interagire tra di loro le varie autorità sia all'interno di un medesimo Stato membro, sia a livello comunitario.

L'analisi di questa tematica trova un caposaldo nella rilevante pronuncia della Corte di giustizia *Meta Platforms c. Bundeskartellamt*.[91] In questo caso, la Corte ha avuto occasione, per la prima volta, di pronunciarsi sulla possibilità, per un'autorità della concorrenza, di addurre, quale fondamento per ritenere violato il diritto della concorrenza, la presenza di una violazione del GDPR, accertata, di fatto, dalla medesima autorità. In altre parole, la Corte ha avuto modo di stabilire se, e a che condizioni, sia possibile adoperare il diritto della concorrenza al fine di contrastare fattispecie concrete, le quali si presentano come contrarie al GDPR e, *di conseguenza*, anche al diritto della concorrenza.

Il caso di specie ha avuto origine da una decisione del *Bundeskartellamt* (autorità federale garante della concorrenza della Germania) del 6 febbraio 2019,[92] con la quale veniva accertato un abuso di posizione dominante ad opera di Meta Platforms Inc, Meta Platforms Ireland Ltd e Facebook Deutschland GmbH. Le argomentazioni addotte dall'autorità strettamente connesse al diritto della concorrenza esulano dal tema del presente elaborato e non saranno dunque esaminate. Invece, per quanto qui interessa, la linea argomentativa del Bundeskartellamt è stata la seguente: (*i*) ai sensi del diritto tedesco e, in particolare, a norma dell'articolo 19 del *Gesetz gegen Wettbewerbsbeschränkungen* (legge contro le restrizioni della concorrenza, *GWB*), l'utilizzo di condizioni contrattuali sleali può costituire un abuso di posizione dominante;[93] (*ii*) la «*Data Policy*» e la «*Cookies Policy*» adottate da Facebook sono parte integrante dei c.d. «termini e condizioni» di erogazione

91 Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit.

92 Bundeskartellamt, decisione B6-22/16 del 6 febbraio 2019, disponibile in inglese al seguente link: `https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5`.

93 P. J. VAN DE WAERDT, «Meta v Bundeskartellamt: Something Old, Something New», *European Papers*, 8, 3 (2023), p. 1080; v. anche I. GRAEF, «Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment», *Maastricht Journal of European and Comparative Law*, 30, 3 (2023), p. 3, la quale segnala che il Bundesgerichtshof ha più volte sostenuto che «*the German prohibition of abuse of dominance in Section 19(1) GWB can also be invoked in cases where one party dictates contractual terms that breach civil law principles or constitutionally protected rights*».

del servizio, in quanto gli utenti *devono* acconsentirvi prima di poter usare il servizio;[94] *(iii)* pertanto, anche *privacy policies* "sleali" possono integrare l'abuso di posizione dominante; *(iv)* il trattamento di taluni dati personali è avvenuto in assenza di un'idonea base giuridica di cui agli articoli 6 e 9, paragrafo 2, GDPR;[95] *(v)* pertanto, sussiste un abuso di posizione dominante.[96]

A seguito del rinvio pregiudiziale operato dall'*Oberlandersgericht Düsseldorf* (Tribunale superiore del Land di Düsseldorf) – cui le società oggetto della decisione si erano rivolte per impugnare il provvedimento del BKartA – il caso è stata sottoposto alla Corte di giustizia. Il primo tema, centrale, è il seguente: può un'autorità garante della concorrenza, al fine di ritenere sussistente un abuso di posizione dominante ex articolo 102 TFUE, accertare – seppur in via *incidentale* – una violazione del GDPR? In altre parole, poteva il BKartA usare motivazioni di diritto della protezione dei dati per accertare una violazione del diritto della concorrenza?[97] Inoltre, strettamente connesso al primo tema, vi è il fatto che l'autorità di controllo capofila non fosse situata *in Germania*, ma in un altro Stato membro (Irlanda): in che modo e a che condizioni le autorità per la protezione dei dati – capofila ed interessate – devono essere coinvolte?

A tale proposito, la Corte ricorda, innanzitutto, che – in base al meccanismo di sportello unico – il GDPR prevede una suddivisione delle competenze tra l'autorità di controllo capofila e le altre autorità interessate, le quali cooperano ai sensi dell'articolo 60.[98] Tuttavia, osservano i giudici, tali norme non si rivolgono alle autorità garanti della concorrenza[99] e, più in generale, «né il RGPD né altri strumenti del diritto dell'Unione stabiliscono norme specifiche sulla cooperazione tra un'autorità nazionale garante della concorrenza e le autorità nazionali di controllo interessate o l'autorità di controllo capofila».[100] Da ciò si deduce che

> nessuna disposizione [del GDPR] vieta alle autorità nazionali garanti della concorrenza di constatare, nell'ambito dell'esercizio delle loro funzioni, la non conformità a tale regolamento di un trattamento di dati effettuato da un'impresa in posizione dominante e tale da costituire un abuso di tale posizione.[101]

Anzi, la Corte sembra ritenere un simile scenario non solo consentito, ma anche auspicabile. Infatti, poiché «l'accesso ai dati personali e la possibilità di trattamento

94 Bundeskartellamt, decisione B6-22/16 cit., § 561, 564-566.
95 Ivi, § 629-630.
96 Ivi, § 871.
97 Van de Waerdt, «Meta v Bundeskartellamt» cit., p. 1085.
98 Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit., § 40.
99 Ivi, § 42.
100 Ivi, § 43.
101 Ibidem.

di tali dati sono diventati *un parametro significativo della concorrenza fra imprese dell'economia digitale*»[102] e considerando che «la conformità […] di detto comportamento alle disposizioni del RGPD può costituire, se del caso, un *importante indizio* […] per stabilire se siffatto comportamento costituisca un ricorso a mezzi su cui s'impernia la concorrenza normale»,[103]

> escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e *potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione*.[104]

Tale possibilità concessa alle autorità garanti della concorrenza presenta, tuttavia, alcune controindicazioni. Infatti, anche nonostante si osservi che «le autorità di controllo, da un lato, e le autorità nazionali garanti della concorrenza, dall'altro, esercitano *funzioni diverse e perseguono obiettivi e compiti ad esse propri*»,[105] sussiste comunque il rischio che vi siano *divergenze* tra le due autorità in merito all'interpretazione del GDPR.[106]

A questo riguardo, la Corte osserva che, pur non essendo rinvenibili norme specifiche dirette a regolare questo ambito, l'attività delle autorità antitrust non deve considerarsi senza limiti. Infatti, ciò non toglie che le varie autorità nazionali, quando applicano il diritto dell'Unione (incluso il GDPR), siano «tutte vincolate dal principio di leale cooperazione sancito all'articolo 4, paragrafo 3, TUE».[107] In base a tale principio, l'autorità della concorrenza deve, innanzitutto, verificare se tale comportamento o un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila o, ancora, della Corte. Qualora fosse questo il caso, la prima non potrebbe discostarsi da tale decisione.[108] Qualora invece non vi sia stata alcuna decisione, l'autorità deve consultare le altre autorità al fine di fugare i propri dubbi e comprendere se attendere una decisione di queste.[109]

102 Ivi, § 51, corsivo aggiunto.
103 Ivi, § 47, corsivo aggiunto.
104 Ivi, § 51, corsivo aggiunto. Graef, «Meta platforms» cit., p. 7 sottolinea come fosse già accaduto che la Corte di giustizia ritenesse rilevante l'inosservanza di altre norme per accertare la violazione del diritto della concorrenza, ad es. in Corte giust., sentenza del 14 marzo 2013, causa C-32/11, *Allianz Hungária Biztosító Zrt. e a. c. Gazdasági Versenyhivatal*, ECLI:EU:C:2013:160 e Corte giust., sentenza del 6 dicembre 2012, causa C-457/10 P, *AstraZeneca AB e AstraZeneca plc c. Commissione europea*, ECLI:EU:C:2012:770.
105 Ivi, § 44, corsivo aggiunto.
106 Ivi, § 55.
107 Ivi, § 53.
108 Ivi, § 56.
109 Ivi, § 57.

La cooperazione tra le autorità non è, tuttavia, a senso unico. Difatti, se l'autorità della concorrenza è tenuta a quanto appena enunciato, le autorità per la protezione dei dati sono tenute a dare un riscontro entro termini ragionevoli su come intendano procedere (ad esempio, se l'autorità nazionale intenda inoltrare il reclamo all'autorità capofila, oppure se l'autorità capofila intenda aprire un'indagine sull'argomento).[110] In mancanza di tale riscontro, l'autorità della concorrenza può proseguire la propria indagine.[111] Nel caso di specie, si rileva che il BKartA aveva richiesto, sin da subito, la collaborazione di tutte le autorità competenti, ossia *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (Commissario federale per la protezione dei dati e la libertà d'informazione), *Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (Commissario per la protezione dei dati e la libertà d'informazione di Amburgo) e *Data Protection Commission* (Autorità di controllo irlandese), senza che esse avessero sollevato alcuna obiezione.[112] Pertanto, la Corte ritiene che il BKartA abbia soddisfatto i propri obblighi in materia di leale cooperazione.[113]

Come si è detto, la pronuncia in esame è molto rilevante e, per certi versi, rivoluzionaria. Essa, infatti, riconosce valido quanto sinora teorizzato da quella dottrina che sosteneva come – in presenza di un sistema di *enforcement* del diritto della protezione dei dati poco dissuasivo, soprattutto nei confronti delle *big tech* – tali condotte si sarebbero potute più efficacemente affrontare con gli strumenti del diritto della concorrenza.[114] D'altro lato, tuttavia, essa si riferisce ad un caso piuttosto specifico, in cui: (*i*) l'autorità della concorrenza aveva chiesto *sin da subito* la collaborazione delle altre autorità coinvolte dello Stato membro di

110 Ivi, § 58.
111 Ivi, § 59.
112 Ivi, § 60.
113 Ivi, § 61.
114 Per una più ampia discussione sul tema in dottrina si v. *ex multis* A. Kuenzler, «What competition law can do for data privacy (and vice versa)», *Computer Law & Security Review*, 47 (2022); W. Kerber, «Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law», *The Antitrust Bulletin*, 67, 2 (2022); D. Lypalo, «Can Competition Protect Privacy? An Analysis Based on the German Facebook Case», *World Competition*, 44, 2 (2021); K. Wiedemann, «Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary», *IIC - International Review of Intellectual Property and Competition Law*, 52, 7 (2021); F. Costa-Cabral e O. Lynskey, «Family ties: The intersection between data protection and competition in EU law», *Common Market Law Review*, 54, 1 (2017); C. Kuner et al., «When two worlds collide: the interface between competition law and data protection», *International Data Privacy Law*, 4, 4 (2014); M. Kuschewsky e D. Geradin, «Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges», *World Competition*, 37, 1 (2014).

appartenenza,[115] nonché dell'autorità capofila, e *(ii)* quest'ultima non aveva dato alcuna risposta.

Ciò lascia aperti una serie di interrogativi, relativi ad ipotesi più sfumate di quella sinora analizzata. Ad esempio: qualora, invece, l'autorità per la protezione dei dati competente desse una sua risposta, quali sarebbero i margini di scostamento dalla stessa concessi all'autorità della concorrenza? La domanda sorge perché la Corte afferma che quest'ultima «non potrebbe discostarsene, *pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza*».[116] In dottrina, si è osservato[117] come ciò sia conforme a quella tendenza del diritto della concorrenza – condivisa anche dalla Corte con giurisprudenza costante – di dotarsi di definizioni autonome rispetto ad altri ambiti del diritto che utilizzino il medesimo termine.[118] Inoltre, si è evidenziato come quest'ultima precisazione potrebbe portare, ad esempio, a considerare come abuso di posizione dominante una situazione relativa a un trattamento di dati personali considerato «sleale», ancorché non in violazione del GDPR.[119]

Inoltre, occorre considerare che, oltre alle autorità della concorrenza, la necessità di collaborare potrebbe insorgere, proprio, tra DSC e autorità per la protezione dei dati. Infatti, come si è evidenziato nel primo capitolo, numerosi sono i punti di intersezione tra le due discipline. A tal proposito, il legislatore europeo, proprio come nel caso appena analizzato, non ha ritenuto di proceduralizzare tale collaborazione. Al contrario, nella sua opinione sulla Proposta DSA, il Garante europeo per la protezione dei dati aveva raccomandato al legislatore di emendare la Proposta stabilendo una collaborazione istituzionalizzata e strutturata tra le varie istituzioni e dettando le condizioni alle quali il DSC avrebbe avuto il potere-dovere di consultare le altre autorità.[120]

Dal canto suo, il legislatore italiano, all'articolo 15, comma 2, DL 159/2023, ha previsto quanto segue:

> L'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per

115 Van de Waerdt, «Meta v Bundeskartellamt» cit., p. 1079.
116 Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit., § 56, corsivo aggiunto.
117 Graef, «Meta platforms» cit., p. 9.
118 Ad es. per la definizione di «impresa» si v. Corte giust., sentenza del 14 marzo 2019, causa C-724/17, *Vantaan kaupunki c. Skanska Industrial Solutions Oy e a.*, ECLI:EU:C:2019:204, § 47; Corte giust., sentenza del 23 aprile 1991, causa C-41/90, *Klaus Höfner e Fritz Elser c. Macrotron GmbH*, ECLI:EU:C:1991:161, § 21-22.
119 Graef, «Meta platforms» cit., p. 9.
120 Garante europeo della protezione dei dati, *Opinion 1/2021* cit., § 87-89.

> le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione.[121]

La norma non è di grande aiuto, visto che si limita a sancire un generale dovere di collaborazione tra le autorità. Più utile sarà forse la stipula di tali protocolli di intesa, qualora questa avverrà.

Più in generale, vi è da affermare, quindi, la necessità che il legislatore intervenga al fine di regolare con specifiche norme le condizioni e le modalità con le quali le autorità siano tenute a cooperare. Infatti, in un ambito come quello del meccanismo di cooperazione e coerenza tra le autorità per la protezione dei dati, già alquanto proceduralizzato dagli articoli 60 e seguenti del GDPR, si è notata la reticenza di talune autorità, esposta nel capitolo 2, a collaborare tra loro, nonostante la presenza di specifici obblighi fissati dalle norme appena citate.

Nel frattempo, il richiamo fatto dalla Corte al principio di leale collaborazione non deve, però, essere svalutato. Infatti, in assenza di specifiche norme, esso è, comunque, idoneo a generare in capo agli Stati membri e alle loro autorità *veri e propri obblighi*.[122] Tali obblighi impongono agli Stati membri – incluse le loro autorità amministrative[123] – di (*i*) «rispettarsi e assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati»,[124] (*ii*) di «adottare tutte le misure atte a garantire la portata e l'efficacia del diritto comunitario»[125] (*iii*) e di astenersi «da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione».[126] Ebbene, è evidente che già questo principio è idoneo a vietare tutta una serie di comportamenti delle autorità – come, ad esempio,

121 Si v. la disposizione pressoché analoga del § 50f del GWB tedesco, riportata in Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit., § 25: «Le autorità garanti della concorrenza, le autorità di regolamentazione, il responsabile federale della protezione dei dati e della libertà di informazione, i responsabili regionali della protezione dei dati e le autorità competenti ai sensi dell'articolo 2 dell'*EU-Verbraucherschutzdurchführungsgesetz* [(legge per l'attuazione del diritto dell'Unione europea in materia di tutela dei consumatori)] possono, indipendentemente dalla procedura scelta, scambiarsi informazioni, compresi dati personali e segreti tecnici e commerciali, nella misura necessaria per l'assolvimento dei rispettivi compiti e utilizzare tali informazioni nell'ambito delle loro procedure».

122 M. Klamert, «Article 4 TEU», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer et al., Oxford University Press, New York 2019, p. 49.

123 Corte giust., causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)* cit., § 53.

124 Corte giust., cause riunite C-14/21 e C-15/21, *Sea Watch* cit., § 156.

125 Corte giust., sentenza del 16 ottobre 2003, causa C-339/00, *Irlanda c. Commissione delle Comunità europee*, ECLI:EU:C:2003:545, § 71.

126 Corte giust., sentenza del 28 aprile 2011, causa C-61/11 PPU, *Hassen El Dridi, alias Soufi Karim*, ECLI:EU:C:2011:268, § 56.

non coinvolgere *sin da una fase iniziale* del procedimento le altre autorità, non condividere l'un l'altra tutte le informazioni rilevanti, non rispettare le decisioni dell'autorità competente – che, dunque, devono ritenersi squalificati *anche in assenza di una specifica disposizione del diritto dell'Unione che li vieti*. Infatti, adottando simili condotte, non solo si viola il dovere di collaborazione in sé e per sé *sub* (*i*), ma si finisce, mediatamente, per minare l'attuazione efficace e coerente del diritto dell'Unione, infrangendo così anche gli obblighi illustrati ai punti (*ii*) e (*iii*).

CONCLUSIONI

Nel corso del presente elaborato, si è rilevato come i due regolamenti esaminati mirino a dettare una regolazione efficiente dell'«ambito digitale» *lato sensu* inteso, chi dal punto di vista della tutela dei dati personali, chi da quello della regolazione dei servizi digitali. Le norme contenute in DSA e GDPR, lette astrattamente, paiono conferire agli individui significativi diritti e stabilire stringenti obblighi per chi eroga il servizio o tratta i dati.

L'esperienza del Regolamento generale sulla protezione dei dati ha, tuttavia, dimostrato come la situazione nella pratica sia ben diversa. Infatti, il sistema di *enforcement* ideato dal legislatore del 2016 ha mostrato, in questi anni, tutte le sue debolezze, cosicché esso fatica a garantire a ciascun individuo una concreta ed efficace protezione del diritto di cui agli articoli 8 della Carta e 16 TFUE.

Nel corso del capitolo 2, si sono presentate le molteplici problematiche connesse all'attuazione del GDPR, evidenziando come – pur esistendo situazioni patologiche anche in casi meramente "domestici" – esse siano esacerbate dalla caratteristica *transfrontaliera* del trattamento. In particolare, si è sostenuto come le esigenze di cooperazione tra le autorità e di coerenza tra le loro decisioni, cui mirano gli articoli 60 e seguenti, siano messe in difficoltà, soprattutto, dal modello di *enforcement* decentrato imperniato sul meccanismo di sportello unico, definito da Gentile e Lynskey, come «*deficient by design*».[1]

Ciò è vero, innanzitutto, per la sua natura *decentralizzata*.[2] Esso, infatti, affidandosi completamente alle autorità di ciascuno Stato membro, connota in maniera eccessivamente nazionale l'attuazione del GDPR, anche quando essa riguarda un trattamento *transfrontaliero* e, quindi, interessati *di altri Stati membri*. Ciò perché, mancando una procedura dettagliata definita a livello europeo, la gestione del procedimento si basa sulle norme di diritto amministrativo proprie dello Stato,[3] le quali assumono, pertanto, un ruolo decisivo. Inoltre, l'esperienza ha mostrato come l'(eccessivo) affidamento riposto sulle autorità di controllo abbia

1 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit.
2 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 494.
3 Ivi, p. 495.

comportato l'emersione di un'influenza preponderante di priorità nazionali, anziché europee, nell'attuazione transfrontaliera del GDPR: secondo la dottrina, «*some NSAs continue to act as agents of national law rather than agents of European law when they apply data protection law*».[4] Infine, poiché il decentramento frammenta l'*enforcement* in una pluralità di ordinamenti nazionali, ciò fa sì che una medesima situazione fattuale possa essere trattata diversamente a seconda dello Stato membro: si verificherebbe qui una lesione del principio di uguaglianza, poiché il medesimo diritto fondamentale verrebbe protetto diversamente,[5] nonché del divieto di discriminazione sulla base della nazionalità, qualora si confronti la situazione dei cittadini dello Stato membro cui appartiene l'autorità capofila con i cittadini degli altri Stati membri.[6]

La *natura "cooperativa"* del meccanismo,[7] lungi dal riuscire a garantire l'uniformità auspicata, sembra più che altro avere assunto la funzione di contrastare le istanze di regolazione al ribasso di talune autorità di controllo (si veda, ad esempio, quanto illustrato in tema di sanzioni nel par. 2.4). Inoltre, l'ulteriore carico burocratico generato dall'attivazione del meccanismo OSS e di coerenza comporta ritardi nell'adozione della decisione finale, giustificati da uno scarso miglioramento del contenuto della decisione finale.[8] Infine, la natura di procedura composita del meccanismo comporta significative preoccupazioni dal punto di vista dei diritti procedurali garantiti alle parti (v. parr. 2.5, 2.6 e 2.7).

Da ultimo, come ha mostrato anche l'analisi condotta nel capitolo 2 (in particolare, v. parr. 2.3 e 2.4), dai casi pratici che si sono sinora verificati è possibile dedurre come una grande parte dell'inabilità dei meccanismi sinora descritti di porre fine alle violazioni derivi, soprattutto, dal *ruolo eccessivamente dominante dell'autorità di controllo capofila*.

Brito Bastos e Pałka evidenziano come tale dominanza distorca ancora di più la corretta applicazione del GDPR nei casi che gli autori definiscono come di «*European concern*», ossia casi la cui soluzione incide sui diritti fondamentali di una gran parte di residenti negli Stati membri.[9] Tale affermazione è supportata,

4 Gentile e Lynskey, «The Transnational Enforcement of the GDPR» cit., p. 821.
5 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 494, 501.
6 Hofmann, «Multi-Jurisdictional Composite Procedures» cit., nota 91.
7 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 494.
8 Ad esempio, l'esperienza in materia di sanzioni ha mostrato come, molto spesso, la decisione finale, adottata a seguito del parere vincolante ex articolo 65 GDPR, pur migliorando rispetto al progetto iniziale, comunque faticava a soddisfare il requisito della dissuasività della decisione.
9 Più precisamente, i casi di «*European concern*», vengono definiti come quelli che *(i)* coinvolgono un ampio numero di Stati membri (e, quindi, un ampio numero di interessati); *(ii)* impattano significativamente sui diritti fondamentali; *(iii)* la cui soluzione si presenta come complessa. Più ampiamente, si v. Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 497-499.

innanzitutto, dal fatto che, nonostante il trattamento dei dati, in tali casi, riguardi *tutti gli interessati dell'Unione*, la supervisione è, comunque, affidata all'autorità di un solo Stato membro.[10] È, dunque, chiara la stortura che si crea: nonostante venga in gioco il diritto fondamentale alla protezione dei dati dei residenti *di tutti gli Stati membri*, la sua protezione è affidata ad una sola autorità di controllo.

La situazione è aggravata dal fatto che, molto spesso, l'individuazione di tale autorità è rimessa alla scelta (forse, *rectius*, all'arbitrio) proprio *del soggetto regolato*. Infatti, in questi casi, il titolare del trattamento è, solitamente, una società, c.d. *big tech*, avente la sede principale in uno Stato terzo. È evidente che, per operare nell'Unione, tali società dovranno scegliere uno degli Stati membri ove collocare il proprio «stabilimento principale». Nell'effettuare questa scelta, esse sono completamente libere, cosicché, probabilmente, finiranno per orientarsi verso «*the best, the most sympathetic, or even the least efficient administration*».[11]

Di fatto, questo si traduce nella possibilità per tali titolari di scegliere *artificiosamente* da quale autorità vogliano essere regolati. In questo senso, è inutile nascondere la forte appetibilità dell'Irlanda, la quale presenta un sistema fiscale favorevole, l'inglese come lingua principale e, appunto, una acclarata "benevolenza" delle istituzioni dello Stato – ivi compresa l'autorità di controllo, definita «*Big Tech-friendly*»[12] – nei confronti di tali operatori, proprio per gli elevati introiti economici che questi ultimi generano per il paese.[13]

Tutti questi motivi mostrano, ad avviso dello scrivente, come sia necessario – quantomeno per i casi di maggiore rilevanza (appunto, di *European concern*) – abbandonare il meccanismo di sportello unico basato sull'*enforcement* decentrato. Infatti, esso – nato come erede di un concetto relativo al mercato interno, ossia il principio del paese d'origine – si presenta sempre più inadatto a garantire un'efficace ed uniforme tutela del diritto alla protezione dei dati: un meccanismo che rende, spesso, eccessivamente difficile, se non impossibile, per gli interessati ottenere la tutela dei propri diritti deve *necessariamente* essere sottoposto a qualche forma di cambiamento. Nel panorama attuale, se deve esservi un soggetto sottoposto al rischio di dover «"fare il giro" delle aule di giustizia [o delle autorità di controllo] dell'Unione europea»,[14] esso non deve essere, di certo, il singolo individuo, ma la grande società dotata di tutte le idonee risorse economiche ed organizzative per affrontare procedimenti in più Stati membri.

10 Ivi, p. 499.
11 V. ibidem che cita E. Chiti, «The Governance of Compliance», in *Compliance and the Enforcement of EU Law*, a cura di M. Cremona, Oxford University Press, Oxford 2012, p. 41-42.
12 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 503.
13 Ivi, p. 502-503.
14 Conclusioni dell'AG Bobek, causa C-645/19, *Facebook Ireland Limited e a.* cit., § 105.

D'altra parte, le esigenze di uniformità e coerenza nell'applicazione del regolamento non permettono, sicuramente, di ritornare verso un meccanismo che, per così dire, potremmo definire "a 27 sportelli". Posta questa premessa, le soluzioni possibili possono essere varie. Rimanendo nel campo del diritto vigente, è necessario che l'EPDB non rinunci al suo ruolo di garante della coerenza del diritto alla protezione dei dati all'interno dell'Unione. Inoltre, è auspicabile che il comitato continui la tendenza manifestata con l'ultima decisione vincolante (v. par. 2.4) e sia sempre meno timido nell'opporsi a progetti di decisione che non assicurino la dovuta efficacia al diritto dell'Unione.

Invece, in una prospettiva *de iure condendo*, nel paragrafo 2.10 si è spiegato come convinca poco la proposta della Commissione volta ad armonizzare le regole procedurali con riferimento ai trattamenti transfrontalieri. Sono più persuasive le argomentazioni di quella parte della dottrina che ha manifestato, invece, tendenze accentratrici, ritenendo che talune competenze – segnatamente, quelle relative ai "grandi casi" di rilevanza europea – dovrebbero essere affidate non più agli Stati membri, ma gestite a livello europeo. Ricollegandosi a quanto appena affermato circa l'abbandono del meccanismo OSS, si può dar conto dell'opinione di Brito Bastos e Pałka. Essi sostengono come una qualche forma di accentramento sia non solo opportuna, ma anche richiesta dal diritto primario e, segnatamente, dall'articolo 8 della Carta e 16 TFUE, proprio perché l'effettività delle autorità di controllo è strettamente connessa all'effettività del diritto alla protezione dei dati in sé e per sé.[15]

Per quanto riguarda l'autorità a cui affidare tali competenze, è evidente che essa non potrà essere la Commissione. Nel paragrafo 3.7, si è sostenuto come essa, non essendo un'istituzione indipendente, sia inidonea a ricoprire il ruolo di *enforcer* del DSA. A maggior ragione, ciò vale per il GDPR, posto che, in questo caso, il requisito della «completa indipendenza» è fissato direttamente dal diritto primario (art. 8 Carta e art. 16 TFUE).

Nel capitolo 3, si è spiegato come l'attuazione del Digital Services Act sia stata concepita come condivisa tra le autorità nazionali e la Commissione europea, con un ruolo molto incisivo di quest'ultima nel caso sia coinvolta una VLOP. Si è, inoltre, sostenuto che l'attribuzione di importanti compiti a tale istituzione sia criticabile, in quanto la sua non indipendenza pone problemi sia dal punto di vista giuridico che di opportunità.

Ulteriormente, si è evidenziato come il DSA pare aver imparato solo parzialmente dalle lezioni date dal GDPR. L'attribuzione di un ruolo solamente consultivo al comitato europeo per i servizi digitali, lasciando ai DSC la possibilità di dipartire

15 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 510-511.

dal suo parere (seppur motivando), sembra non fronteggiare con sufficiente forza le esigenze di coerenza ed uniformità, quasi che il legislatore non si fosse reso conto del ruolo troppo ingombrante assunto delle autorità di controllo nel caso del GDPR.

Le significative interconnessioni tra DSA e GDPR illustrate nel capitolo 1 hanno fatto emergere la necessità di coordinare tutte le autorità coinvolte, pena l'ottenere una regolazione disorganica e sub-ottimale dei servizi digitali. A tal riguardo, si è rilevato come, se i principi dettati dalla Corte in *Meta c. Bundeskartellamt* pongono una prima base, sarebbe, forse, auspicabile un intervento del legislatore (dell'Unione, chiaramente), volto a dare concretezza al principio di leale collaborazione di cui all'articolo 4, paragrafo 3, TFUE.

Tale esigenza è a maggior ragione pressante se si considera che il 13 marzo 2024 il Parlamento europeo, a seguito della proposta della Commissione del 24 aprile 2021,[16] ha approvato in via definitiva il c.d. «*AI Act*»,[17] il quale istituisce un ulteriore sistema di *enforcement*, costituito, a livello europeo da un «ufficio per l'IA» (art. 64), un «comitato europeo per l'intelligenza artificiale» (artt. 65-66), un «forum consultivo» (art. 67), un «gruppo di esperti scientifici indipendenti» (artt. 68-69) e, a livello nazionale, da un'«autorità di notifica» e un'«autorità di vigilanza del mercato» (art. 70).

Quest'ultima novella aggiunge complessità ad un insieme di discipline già di per sé elaborato. De Gregorio e Demková sottolineano come sia difficile, soprattutto per un individuo, districarsi tra il groviglio di diritti e rimedi concessi da GDPR, DSA e AI Act.[18] Infatti, una medesima fattispecie concreta potrebbe essere fronteggiata, potenzialmente, dal punto di vista di tutti e tre i regolamenti. L'individuo dovrà, dunque, scegliere quale rimedio attivare, dovendo, peraltro, rivolgersi a diverse autorità (nel caso italiano, Garante per la protezione dei dati, AGCOM e, probabilmente, AGCM[19]).

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

17 Si v. il comunicato stampa sul sito del Parlamento europeo (13/03/2024), https://www.europarl.europa.eu/news/it/press-room/20240308IPR19015/il-parlamento-europeo-approva-la-legge-sull-intelligenza-artificiale (visitato il 01/04/2024). In attesa della pubblicazione nella Gazzetta Ufficiale, il testo definitivo è disponibile al seguente link: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf.

18 G. De Gregorio e S. Demková, «The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe», *CGSL Working Papers*, 3 (2024), p. 3-4.

19 F. Meta, «AI Act, tensione Governo-Garante Privacy. Stanzione: "Autorità di controllo sia indipendente"», *Corriere Comunicazioni* (25 marzo 2024), (visitato il 01/04/2024).

La dottrina appena citata ritiene che queste novità possano aggravare la già esistente frammentazione rimediale, ricordando che

> *the effectiveness of remedies in the European algorithmic society firmly depends on the extent to which legislators can instil clear and efficient institutional collaboration, supported by the capacity of private actors, administrative authorities and courts to cooperate in the enforcement of EU law, above all, in a way that strengthens the protection of fundamental rights.*[20]

È in questa direzione che deve muoversi l'interprete. Oltre ad occuparsi delle singole disposizioni sostanziali, appare essenziale concentrarsi sull'effettività degli strumenti predisposti per tutelarle. Altrimenti, non si avrà nient'altro che l'astratta attribuzione di posizioni giuridiche soggettive, senza che, però, i vari diritti fondamentali che vengono in gioco siano, in realtà, sufficientemente protetti. Come già ricordato, ciò rappresenta molto più che un semplice problema di inefficienza amministrativa. Si tratta, invece, di un problema di mancata tutela di diritti fondamentali: un *enforcement* inefficiente «*represents a problem of far more than mere administrative underperformance. It is a problem of a deficit of protection of a fundamental right. It is a violation of a fundamental right by omission rather than by contravention*».[21]

20 De Gregorio e Demková, «The Constitutional Right to an Effective Remedy in the Digital Age» cit., p. 4.

21 Brito Bastos e Pałka, «Centralised GDPR Enforcement» cit., p. 511.

BIBLIOGRAFIA

Agenzia dell'Unione europea per i diritti fondamentali, Consiglio d'Europa, Corte europea dei diritti dell'uomo e Garante europeo della protezione dei dati, *Manuale sul diritto europeo in materia di protezione dei dati: edizione 2018*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo 2018, DOI: 10.2811/595922.

Angelopoulos, C., «Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape», *Journal of Intellectual Property Law & Practice*, 9, 10 (2014), p. 812-821, DOI: 10.1093/jiplp/jpu136.

Batlle, S. e A. van Waeyenberge, «EU–US Data Privacy Framework: A First Legal Assessment», *European Journal of Risk Regulation*, 15, 1 (2024), p. 191-200, DOI: 10.1017/err.2023.67.

Bertuzzi, L., «Commission announces first platforms to fall under EU digital rulebook's stricter regime», *Euractiv* (27 aprile 2023), https://www.euractiv.com/section/platforms/news/commission-announces-first-platforms-to-fall-under-eu-digital-rulebooks-stricter-regime/ (visitato il 17/02/2024).

– «Digital Services Act: il duello Francia-Irlanda sul principio del 'paese d'origine'», *Euractiv* (27 settembre 2021), https://euractiv.it/section/digitale/news/digital-services-act-duello-francia-irlanda-sul-principio-del-paese-origine/ (visitato il 03/02/2024).

Blume, P., «Article 61 Mutual assistance», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 973-985, DOI: 10.1093/oso/9780198826491.003.0104.

– «Article 62 Joint operations of supervisory authorities», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 986-994, DOI: 10.1093/oso/9780198826491.003.0105.

Bolognini, L., «Oggetto, obiettivi e ambito di applicazione del *Digital Services Act*», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 37-44.

Borgobello, M., «Digital Services Act, è il mercato interno il vero protagonista», *Agenda Digitale* (23 dicembre 2022), https://www.agendadigitale.eu/mercati-digitali/digital-service-act-mercato-interno/ (visitato il 20/12/2023).

Brati, O., «Dassonville and Cassis de Dijon – as the basic jurisprudence of the free movement of goods», *Academic Journal of Business, Administration, Law and Social Sciences*, 6, 1 (2020), p. 194-197, https://iipccl.org/wp-content/uploads/2021/08/Olsa-Brati-AJBALS.pdf.

Brito Bastos, F., «An Administrative Crack in the EU's Rule of Law: Composite Decision-making and Nonjusticiable National Law», *European Constitutional Law Review*, 16, 1 (2020), p. 63-90, doi: 10.1017/S1574019620000073.

– «Derivative illegality in European composite administrative procedures», *Common Market Law Review*, 55, 1 (2018), p. 101-134, doi: 10.54648/cola2018004.

Brito Bastos, F. e P. Pałka, «Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?», *European Constitutional Law Review*, 19, 3 (2023), p. 487-517, doi: 10.1017/S1574019623000202.

Brkan, M., «Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond», *International Journal of Law and Information Technology*, 27, 2 (2019), p. 91-121, doi: 10.1093/ijlit/eay017.

Buri, I., «A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer», in *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications*, a cura di J. Hoboken, I. Buri, J. Quintais, R. Fahy, N. Appelman e M. Straub, Verfassungsbooks, Berlin 2023, p. 77-89, https://intr2dok.vifa-recht.de/receive/mir_mods_00015033.

Buri, I. e J. van Hoboken, «The DSA supervision and enforcement architecture», *DSA Observatory* (24 giugno 2022), https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/ (visitato il 13/10/2023).

– «The General Approach of the Council on the Digital Services Act», *DSA Observatory* (7 dicembre 2021), https://dsa-observatory.eu/2021/12/07/the-general-approach-of-the-council-on-the-digital-services-act/ (visitato il 04/02/2024).

Busch, C., «The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'? Some observations on the pending case C-390/18 – Airbnb Ireland», *Journal of European Consumer and Market Law*, 4 (2018), p. 172-174.

Buttarelli, G., «La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche», *Giornale di diritto amministrativo*, 1 (2023), p. 116-127.

Bygrave, L. A., «Article 22 Automated individual decision-making, including profiling», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 522-542, doi: 10.1093/oso/9780198826491.003.0055.

– «Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», *Computer Law & Security Review*, 17, 1 (2001), p. 17-24, doi: 10.1016/S0267-3649(01)00104-2.

Caggiano, G., «La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea», *Annali AISDUE*, 3 (2021), https://www.aisdue.eu/en/giandonato-caggiano-la-proposta-di-digital-service-act-per-la-regolazione-dei-servizi-e-delle-piattaforme-online-nel-diritto-dellunione-europea/.

Castellucci, I. e F. Coppola, «Il sistema sanzionatorio decentrato del DSA: dinamica dell'apparato istituzionale», *Diritto di Internet*, 1 (2023), p. 49-55.

Chiti, E., «The Governance of Compliance», in *Compliance and the Enforcement of EU Law*, a cura di M. Cremona, Oxford University Press, Oxford 2012, p. 31-56, doi: 10.1093/acprof:oso/9780199644735.003.0002.

Commissione Europea, *Shaping Europe's digital future.* Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo 2020, doi: 10.2759/091014.

Cortese, B., «La protezione dei dati a carattere personale nel diritto dell'Unione Europea dopo il Trattato di Lisbona», *Il Diritto dell'Unione Europea*, 2 (2013), p. 313-335.

– «Rinvio pregiudiziale e ricorso di annullamento: parallelismi, intersezioni e differenze», in *Il rinvio pregiudiziale*, a cura di F. Ferraro e C. Iannone, Giappichelli, Torino 2020, p. 241-270.

Costa-Cabral, F. e O. Lynskey, «Family ties: The intersection between data protection and competition in EU law», *Common Market Law Review*, 54, 1 (2017), p. 11-50.

Craig, P. P., *EU administrative law*, 3ª ed., Oxford University Press, Oxford 2018.

Custers, B. e G. Malgieri, «Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data», *Computer Law & Security Review*, 45 (2022), doi: 10.1016/j.clsr.2022.105683.

D'Ippolito, G., «Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale», *Il Diritto dell'Informazione e dell'Informatica*, 634, 3 (2020), p. 634-674.

Daniele, L., *Diritto dell'Unione europea: sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Settima edizione, Giuffrè, Milano 2020.

Davies, G., «The European Union Legislature as an Agent of the European Court of Justice», *Journal of Common Market Studies*, 54, 4 (2016), p. 846-861, doi: 10.1111/jcms.12353.

De Baere, G., «'Is This a Conflict Rule Which I See before Me?' Looking for a Hidden Conflict Rule in the Principle of Origin as Implemented in Primary European Community Law and in the 'Directive on Electronic Commerce'», *Maastricht Journal of European and Comparative Law*, 11, 3 (2004), p. 287-319, doi: 10.1177/1023263X0401100304.

De Gregorio, G. e S. Demková, «The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe», *CGSL Working Papers*, 3 (2024), https://catolicalaw.fd.lisboa.ucp.pt/asset/3761/file.

De Stefani, F., «Definizione di: "destinatario", "hosting", "piattaforma e "motori di ricerca"», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 97-130.

Defraigne, P. e A. De Streel, *What is the digital internal market and where the European Union should intervene?*, rapp. tecn. 2011/33, Florence School of Regulation, 2011, https://cadmus.eui.eu/handle/1814/17914.

De Hert, P. e V. Papakonstantinou, «The new General Data Protection Regulation: Still a sound system for the protection of individuals?», *Computer Law & Security Review*, 32, 2 (2016), p. 179-194, doi: 10.1016/j.clsr.2016.02.006.

Della Cananea, G., «The European Union's Mixed Administrative Proceedings», *Law and Contemporary Problems*, 68 (2004), p. 197-217.

Docksey, C., «Article 65. Dispute Resolution by the Board», in *The EU General Data Protection Regulation: A Commentary - 2021 Update*, a cura di C. Kuner, L. A. Bygrave e C. Docksey, Oxford University Press, New York 2021, p. 227-235, https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf.

Drechsler, L. C., «Op-Ed: "Walking the line between procedural autonomy and effective legal remedies in the General Data Protection Regulation (C-132/21, *Nemzeti Adatvédelmi és Információszabadság Hatóság*)"», *EU Law Live* (gennaio 2023), https://eulawlive.com/op-ed-walking-the-line-between-procedural-autonomy-and-effective-legal-remedies-in-the-gene

ral-data-protection-regulation-c-132-21-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag/.

Eckert, G., «L'indépendance des autorités de régulation économique à l'égard du pouvoir politique», *Revue française d'administration publique*, 143, 3 (2012), p. 629-643, doi: 10.3917/rfap.143.0629.

Eckes, C. e J. Mendes, «The Right to Be Heard in Composite Administrative Procedures: Lost in between Protection?», *European Law Review*, 36 (2011), p. 651-670.

Eliantonio, M., «Access to Justice in Composite Procedures for the Implementation of EU Law: the Story so Far», in *Questions choisies de droit européen des affaires / Selected Issues in European Business Law*, a cura di P. Van Creynenbreugel e J. Wildemeersch, Bruylant, Bruxelles 2023, p. 189-221.

– «Judicial Review in an Integrated Administration: the Case of 'Composite Procedures'», *Review of European Administrative Law*, 7, 2 (2015), p. 65-102, doi: 10.7590/187479814X14186465138022.

Eliantonio, M. e N. Vogiatzis, «Judicial and Extra-Judicial Challenges in the EU Multi- and Cross-Level Administrative Framework», *German Law Journal*, 22, 3 (2021), p. 315-324, doi: 10.1017/glj.2021.18.

Frosio, G. e C. Geiger, «Taking fundamental rights seriously in the Digital Services Act's platform liability regime», *European Law Journal*, 29, 1-2 (2023), p. 31-77, doi: 10.1111/eulj.12475.

Galetta, D.-U. e J. Ziller, «L'independance des juges et le droit de l'Union Européenne du point de vue l'autonomie istitutionnelle (et procedurale) des etats membres», in *Les valeurs de l'Union Européenne*, a cura di F. Péraldi Leneuf, Pedone, Paris 2020, p. 67-79.

Garabiol-Furet, M.-D., «Plaidoyer pour le principe du pays d'origine», *Revue du Marché commun et de l'Union européenne*, 495 (2006), p. 82-87.

Gentile, G. e O. Lynskey, «Deficient by Design? The Transnational Enforcement of the GDPR», *International & Comparative Law Quarterly*, 71, 4 (2022), p. 799-830, doi: 10.1017/S0020589322000355.

Georgieva, L., «Article 66 Urgency procedure», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 1027-1031, doi: 10.1093/oso/9780198826491.003.0110.

González Fuster, G., J. Ausloos, D. Bons, L. A. Bygrave, B. d. R. Lazarotto, L. Drechsler, O. Gkotsopoulou, C. Hristov, K. Irion, L. Jasmontaite, C. Kroese, O. Lynskey e M. S. Magierska, *The right to lodge a data protection complaint : ok, but then what? An empirical study of current practices under the*

GDPR, rapp. tecn., Data Protection Law Scholars Network (DPSN), Access Now, Fiesole 2022, https://cadmus.eui.eu/handle/1814/74899.

Gottschalk, T., «The EU-US Data Privacy Framework (DPF) – A Blueprint for International Data Transfers?», *European Data Protection Law Review*, 9, 4 (2023), p. 448-453, doi: 10.21552/edpl/2023/4/11.

Graef, I., «Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment», *Maastricht Journal of European and Comparative Law*, 30, 3 (2023), p. 325-334, doi: 10.1177/1023263X231205836.

Graziani, C., «PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali», *DPCE Online*, 33, 4 (2017), p. 959-966.

Hacker, P., «UberPop, UberBlack, and the Regulation of Digital Platforms after the Asociación Profesional Elite Taxi Judgment of the CJEU», *European Review of Contract Law*, 14, 1 (2018), p. 80-96, doi: 10.1515/ercl-2018-1005.

Hatzopoulos, V., «General Principles for the Collaborative Economy», in *General principles of EU law and the EU digital order*, a cura di U. Bernitz, X. Groussot, J. Paju e S. A. De Vries, Kluwer Law International B.V., Alphen aan den Rijn 2020, p. 131-150.

Hijmans, H., «Article 1 Subject-matter and objectives», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 48-59, doi: 10.1093/oso/9780198826491.003.0003.

– «Article 55 Competence», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 902-912, doi: 10.1093/oso/9780198826491.003.0097.

– «Article 56 Competence of the lead supervisory authority», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 913-926, doi: 10.1093/oso/9780198826491.003.0098.

– «Article 57 Tasks», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 927-938, doi: 10.1093/oso/9780198826491.003.0099.

– «Article 65 Dispute resolution by the Board», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 1014-1026, doi: 10.1093/oso/9780198826491.003.0109.

– «Understanding the Role of Independent, Effective and Accountable DPAs: New Branches of Government in Between the Union and the Member States», in *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, a cura di H. Hijmans, Springer International Publishing, Cham 2016, p. 325-387, DOI: 10.1007/978-3-319-34090-6_7.

HILDEBRANDT, M., «The Dawn of a Critical Transparency Right for the Profiling Era», in *Digital Enlightenment Yearbook 2012*, a cura di J. Bus, M. Crompton, M. Hildebrandt e G. Metakides, IOS Press, Amsterdam 2012, p. 41-56, DOI: 10.3233/978-1-61499-057-4-41.

HILTUNEN, M., «Social Media Platforms within Internal Market Construction: Patterns of Reproduction in EU Platform Law», *German Law Journal*, 23, 9 (2022), p. 1226-1245, DOI: 10.1017/glj.2022.80.

HOFMANN, H. C., «Multi-Jurisdictional Composite Procedures - The Backbone to the EU's Single Regulatory Space», *University of Luxembourg Law Working Paper*, 3 (2019), DOI: 10.2139/ssrn.3399042.

HOFMANN, H. C. e L. MUSTERT, «Data protection», in *Research Handbook on the Enforcement of EU Law*, a cura di M. Scholten, Edward Elgar, Cheltenham 2023, p. 461-475, DOI: 10.4337/9781802208030.00039.

– «Procedures Matter – What to Address in GDPR Reform and a new GDPR Procedural Regulation», *University of Luxembourg Law Research Paper*, 2 (2023), DOI: 10.2139/ssrn.4492662.

HOLZNAGEL, D., «Platform Liability for Hate Speech & the Country of Origin Principle: Too Much Internal Market?: How hate speech liability rules for social media platforms are testing the boundaries of the E-Commerce-Directive's country of origin principle», *Computer Law Review International*, 21, 4 (2020), p. 103-109, DOI: 10.9785/cri-2020-210403.

HUSTINX, P., «EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation», in *New Technologies and EU Law*, a cura di M. Cremona, Oxford University Press, Oxford 2017, p. 123-173, DOI: 10.1093/acprof:oso/9780198807216.003.0005.

HÜTTL, T., «The content of 'complete independence' contained in the Data Protection Directive», *International Data Privacy Law*, 2, 3 (2012), p. 137-148, DOI: 10.1093/idpl/ips011.

INGLESE, M., «Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland», *Eurojus*, 1 (2020), p. 37-52, https://rivista.eurojus.it/wp-content/uploads/pdf/Sentenze-Elite-Taxi-e-Airbnb-Ireland-Marco-Inglese-.pdf.

Izyumenko, E., «European Court of Human Rights rules that collateral website blocking violates freedom of expression», *Journal of Intellectual Property Law & Practice*, 15, 10 (2020), p. 774-775, DOI: 10.1093/jiplp/jpaa135.

Jaursch, J., «Platform Oversight: Here is what a Strong Digital Services Coordinator Should Look», in *Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications*, a cura di J. Hoboken, I. Buri, J. Quintais, R. Fahy, N. Appelman e M. Straub, Verfassungsbooks, Berlin 2023, p. 91-105, https://intr2dok.vifa-recht.de/receive/mir_mods_00015033.

Kaschny, L. e S. Lavrijssen, «The Independence of National Regulatory Authorities and the European Union Energy Transition», *International and Comparative Law Quarterly*, 72, 3 (2023), p. 715-736, DOI: 10.1017/S0020589323000271.

Kellerbauer, M., «Article 114 TFEU», in *The EU Treaties and the Charter of Fundamental Rights*, a cura di M. Kellerbauer, M. Klamert e J. Tomkin, Oxford University Press, New York 2019, p. 1235-1255, DOI: 10.1093/oso/9780198759393.003.212.

Kerber, W., «Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law», *The Antitrust Bulletin*, 67, 2 (2022), p. 280-301, DOI: 10.1177/0003603X221084145.

Killeen, M., «Zalando files suit against Commission over very large platform designation», *Euractiv* (27 giugno 2023), https://www.euractiv.com/section/platforms/news/zalando-files-suit-against-commission-over-very-large-platform-designation/ (visitato il 17/02/2024).

Klamert, M., «Article 4 TEU», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer, M. Klamert e J. Tomkin, Oxford University Press, New York 2019, p. 35-60, DOI: 10.1093/oso/9780198759393.003.7.

Kotschy, W., «Article 78 Right to an effective judicial remedy against a supervisory authority», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 1125-1132, DOI: 10.1093/oso/9780198826491.003.0124.

Krzysztofek, M., *GDPR: General Data Protection Regulation (EU) 2016/679: post-reform personal data protection in the European Union*, Wolters Kluwer, Alphen aan den Rijn 2019.

Kuenzler, A., «What competition law can do for data privacy (and vice versa)», *Computer Law & Security Review*, 47 (2022), DOI: 10.1016/j.clsr.2022.105757.

Kuner, C., F. H. Cate, C. Millard, D. J. B. Svantesson e O. Lynskey, «When two worlds collide: the interface between competition law and data protection»,

International Data Privacy Law, 4, 4 (2014), p. 247-248, DOI: 10.1093/idpl/ipu025.

KUSCHEWSKY, M. e D. GERADIN, «Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges», *World Competition*, 37, 1 (2014), p. 69-102, DOI: 10.54648/WOCO2014005.

LANDI, A., «I fornitori di servizi di intermediazione molto grandi», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 63-96.

– «L'*exchange commerce*. La Direttiva (UE) 2019/770», in *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, a cura di L. Bolognini, Giuffrè Francis Lefebvre, Milano 2021, p. 139-159.

LEMOINE, L. e M. VERMUELEN, «The extraterritorial implications of the Digital Services Act», *DSA Observatory* (1 novembre 2023), https://dsa-observatory.eu/2023/11/01/the-extraterritorial-implications-of-the-digital-services-act/ (visitato il 18/02/2024).

LIONELLO, L., «La creazione del mercato europeo dei dati: sfide e prospettive», *Diritto del Commercio Internazionale*, 3 (2021), p. 675-706.

LOCK, T., «Article 41 CFR Right to good administration», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer, M. Klamert e J. Tomkin, Oxford University Press, New York 2019, p. 2204-2207, DOI: 10.1093/oso/9780198759393.003.564.

– «Article 8 CFR», in *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, a cura di M. Kellerbauer, M. Klamert e J. Tomkin, Oxford University Press, New York 2019, p. 2121-2127, DOI: 10.1093/oso/9780198759393.003.528.

LUTZI, T., «Internet Cases in EU Private International Law — Developing a Coherent Approach», *The International and Comparative Law Quarterly*, 66, 3 (2017), p. 687-721, http://www.jstor.org/stable/26348302.

LYPALO, D., «Can Competition Protect Privacy? An Analysis Based on the German Facebook Case», *World Competition*, 44, 2 (2021), p. 169-198, DOI: 10.54648/WOCO2021011.

MAFFEO, A., «Misure restrittive contro la Russia: il Tribunale rigetta la richiesta di sospensione di *RT France*», *Eurojus*, 2 (2022), p. 300-311, https://rivista.eurojus.it/wp-content/uploads/pdf/Maffeo-Misure-restrittive-contro-la-Russia-1.pdf.

MAGIERSKA, M., «No, the Data Protection Complaint is Not a Petition», *European Law Blog* (25 gennaio 2024), https://europeanlawblog.eu/2024/01/25

/no-the-data-protection-complaint-is-not-a-petition/ (visitato il 03/03/2024).

Malgieri, G. e G. Comandé, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», *International Data Privacy Law*, 7, 4 (2017), p. 243-265, doi: 10.1093/idpl/ipx019.

Marasà, E. e O. Pollicino, «EU Court of Justice rules that Uber provides a transport service and is not a mere electronic intermediary: regulatory implications and "digital" judicial insulation», *MediaLaws* (8 febbraio 2018), https://www.medialaws.eu/eu-court-of-justice-rules-that-uber-provides-a-transport-service-and-is-not-a-mere-electronic-intermediary-regulatory-implications-and-digital-judicial-insulation/ (visitato il 15/02/2024).

Mendoza, I. e L. A. Bygrave, «The Right Not to be Subject to Automated Decisions Based on Profiling», in *EU Internet Law: Regulation and Enforcement*, a cura di T.-E. Synodinou, P. Jougleux, C. Markou e T. Prastitou, Springer International Publishing, Cham 2017, p. 77-98, doi: 10.1007/978-3-319-64955-9_4.

Meta, F., «AI Act, tensione Governo-Garante Privacy. Stanzione: "Autorità di controllo sia indipendente"», *Corriere Comunicazioni* (25 marzo 2024), https://www.corrierecomunicazioni.it/digital-economy/ai-act-tensione-governo-garante-privacy-stanzione-autorita-di-controllo-sia-indipendente/ (visitato il 01/04/2024).

Michinelli, A., «I servizi intermediari della società dell'informazione», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 45-61.

Monti, G., «Independence, Interdependence and Legitimacy: The EU Commission, National Competition Authorities, and the European Competition Network», *EUI working papers LAW*, 01 (2014), https://cadmus.eui.eu/bitstream/handle/1814/29218/LAW_2014_01.pdf?sequence=1&isAllowed=y.

Morgese, G., «Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE», *Federalismi.it*, 1 (2022), p. 80-126.

Murone, F. G., «Il Digital Service Act e il contrasto ai contenuti illeciti (pt. II)», *Ius in Itinere* (28 febbraio 2022), https://www.iusinitinere.it/il-digital-service-act-e-il-contrasto-ai-contenuti-illeciti-pt-ii-41577.

Mustert, L., «EDPB Decision 1/2023: The Schrems Saga Back on the GDPR's Enforcement Rails», *European Data Protection Law Review*, 9, 2 (2023), p. 194-199, doi: 10.21552/edpl/2023/2/14.

– «The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?», *European Data Protection Law Review*, 9, 4 (2023), p. 454-464, DOI: 10.21552/edpl/2023/4/12.
– «The EDPB's second Article 65 Decision – Is the Board Stepping up its Game?», *European Data Protection Law Review*, 7, 3 (2021), p. 416-422, DOI: 10.21552/edpl/2021/3/10.
– «The First Article 65 Decision – Correct and Consistent Application of the GDPR Ensured?», *European Data Protection Law Review*, 7, 1 (2021), p. 94-100, DOI: 10.21552/edpl/2021/1/12.

Neergaard, U., «The Approach of the CJEU in the Era of Digitalization: Free Movement in Relation to the Internet as Its 25th Anniversary», in *General principles of EU law and the EU digital order*, a cura di U. Bernitz, X. Groussot, J. Paju e S. A. De Vries, Kluwer Law International B.V., Alphen aan den Rijn 2020, p. 83-105.

Neergaard, U. e S. A. De Vries, «The Interaction between Free Movement Law and Fundamental Rights in the (Digital) Internal Market», *SSRN Electronic Journal* (2023), DOI: 10.2139/ssrn.4561901.

Nugent, N. e M. Rhinard, «The 'political' roles of the European Commission», *Journal of European Integration*, 41, 2 (2019), p. 203-220, DOI: 10.1080/07036337.2019.1572135.

Occhiena, M. e N. Posteraro, «Pareri e attività consultiva della pubblica amministrazione: dalla decisione migliore alla decisione tempestiva», *Il diritto dell'economia*, 100, 3 (2019), p. 27-62, https://www.ildirittodelleconomia.it/wp-content/uploads/2020/03/02Occhiena_Posteraro.pdf.

Ortega Giménez, A., «¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU.» *Cuadernos de Derecho Transnacional*, 16, 1 (2024), p. 483-513, DOI: 10.20318/cdt.2024.8432.

Pavese, V. M., «Comitato: nozione, disciplina applicabile», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 199-202.

Pelino, E., «L'interazione tra DSA e GDPR», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 9-14.

Pocar, F., M. C. Baruffi e A. Adinolfi, *Commentario breve ai trattati dell'Unione europea*, 2ª ed., CEDAM, Padova 2014.

Polański, P. P., «Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union», *Computer Law & Security Review*, 34, 3 (2018), p. 562-581, DOI: 10.1016/j.clsr.2017.11.001.

Priolo, E., «Coordinatori dei servizi digitali, Commissione e sanzioni», in *Digital services act e Digital markets act: definizioni e prime applicazioni dei nuovi regolamenti europei*, a cura di L. Bolognini, M. Scialdone e E. Pelino, Giuffrè, Milano 2023, p. 203-227.

Quintais, J. P., N. Appelman e R. Ó Fathaigh, «Using Terms and Conditions to apply Fundamental Rights to Content Moderation», *German Law Journal*, 24, 5 (2023), p. 881-911, doi: 10.1017/glj.2023.53.

Rauh, C., «EU politicization and policy initiatives of the European Commission: the case of consumer policy», *Journal of European Public Policy*, 26, 3 (2019), p. 344-365, doi: 10.1080/13501763.2018.1453528.

Reinhardt, J., «Realizing the Fundamental Right to Data Protection in a Digitized Society», in *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*, a cura di M. Albers e I. W. Sarlet, Springer, Cham 2022, p. 55-68, doi: 10.1007/978-3-030-90331-2_4.

Sabia, R., «L'enforcement pubblico del Digital Services Act tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni», *MediaLaws*, 2 (2023), p. 88-113, https://www.medialaws.eu/wp-content/uploads/2023/10/2-23-Sabia.pdf.

Sarra, C., *Il mondo-dato: saggi su datificazione e diritto*, 2. ed, CLEUP, Padova 2022.

Scaffidi Runchella, L., «Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero», *Cuadernos de derecho transnacional*, 15, 2 (2023), p. 898-919, doi: 10.20318/cdt.2023.8083.

Schreiber, A., «Feeling fine! Harmonisation and inconsistency in EU supervisory authority administrative fines», *Journal of Data Protection & Privacy*, 2, 4 (2019), p. 375-388.

Sieradzka, M., «Asociación Profesional Elite Taxi vs Uber Systems Spain SL: Differences between the Internet Platform and the Transport Service», *Journal of European Competition Law & Practice*, 11, 5-6 (2020), p. 263-266, doi: 10.1093/jeclap/lpaa031.

Spindler, G. e L. Förster, «Privacy-compliant design of Cookie Banners according to the GDPR», *JIPITEC*, 14, 1 (2023), p. 2-33.

Tar, J., «Amazon joins Zalando in challenging very large online platform designation», *Euractiv* (12 luglio 2023), https://www.euractiv.com/section/platforms/news/amazon-joins-zalando-in-challenging-very-large-online-platform-designation/ (visitato il 17/02/2024).

Temple Lang, J., «The Principle of Sincere Cooperation, the Charter and Digitalisation», in *General principles of EU law and the EU digital order*, a cura di

U. Bernitz, X. Groussot, J. Paju e S. A. De Vries, Kluwer Law International, Alphen aan den Rijn 2020, p. 31-64.

Tosoni, L., «Article 4(22). Supervisory authority concerned», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 272-278, DOI: 10.1093/oso/9780198826491.003.0028.

– «Article 4(23) Cross-border processing», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 279-287, DOI: 10.1093/oso/9780198826491.003.0029.

– «Article 4(24) Relevant and reasoned objection», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 288-291, DOI: 10.1093/oso/9780198826491.003.0030.

– «Article 60 Cooperation between the lead supervisory authority and the other supervisory authorities concerned», in *The EU General Data Protection Regulation (GDPR): A Commentary*, a cura di C. Kuner, L. A. Bygrave, C. Docksey e L. Drechsler, Oxford University Press, New York 2020, p. 953-972, DOI: 10.1093/oso/9780198826491.003.0103.

– «The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation», *International Data Privacy Law*, 11, 2 (2021), p. 145-162, DOI: 10.1093/idpl/ipaa024.

Turillazzi, A., M. Taddeo, L. Floridi e F. Casolari, «The digital services act: an analysis of its ethical, legal, and social implications», *Law, Innovation and Technology*, 15, 1 (2023), p. 83-106, DOI: 10.1080/17579961.2023.2184136.

Van Cleynenbreugel, P., «The Commission's digital services and markets act proposals: First step towards tougher and more directly enforced EU rules?», *Maastricht Journal of European and Comparative Law*, 28, 5 (2021), p. 667-686, DOI: 10.1177/1023263X211030434.

Van den Poel, M., *Taking GDPR enforcement really seriously: What to expect from the GDPR Procedural Regulation?*, Workshop Summary, Brussels Privacy Hub Working Paper, gennaio 2024, https://brusselsprivacyhub.com/wp-content/uploads/2024/01/Event-Report-Taking-GDPR-enforcement-really-seriously.pdf.

Van de Waerdt, P. J., «Meta v Bundeskartellamt: Something Old, Something New», *European Papers*, 8, 3 (2023), p. 1077-1103, DOI: 10.15166/2499-8249/703.

Van Drunen, M. Z., N. Helberger e R. Ó Fathaigh, «The beginning of EU political advertising law: unifying democratic visions through the internal

market», *International Journal of Law and Information Technology*, 30, 2 (2022), p. 181-199, DOI: 10.1093/ijlit/eaac017.

VOGIATZOGLOU, P. e P. VALCKE, «Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law», in *Research Handbook on EU Data Protection Law*, Edward Elgar Publishing, Cheltenham 2022, p. 11-49, DOI: 10.4337/9781800371682.00010.

WACHTER, S., B. MITTELSTADT e L. FLORIDI, «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», *International Data Privacy Law*, 7, 2 (2017), p. 76-99, DOI: 10.1093/idpl/ipx005.

WAGNER, B. e H. JANSSEN, «A first impression of regulatory powers in the Digital Services Act», *Verfassungsblog* (4 gennaio 2021), DOI: 10.17176/20210104-182911-0, (visitato il 11/12/2023).

WIDDERSHOVEN, R., «National Procedural Autonomy and General EU Law Limits», *Review of European Administrative Law*, 12, 2 (2019), p. 5-34, DOI: 10.7590/187479819X15840066091222.

WIEDEMANN, K., «Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary», *IIC - International Review of Intellectual Property and Competition Law*, 52, 7 (2021), p. 915-933, DOI: 10.1007/s40319-021-01090-6.

WILLE, A., «The politicization of the EU Commission: democratic control and the dynamics of executive selection», *International Review of Administrative Sciences*, 78, 3 (2012), p. 383-402, DOI: 10.1177/0020852312447061.

WILMAN, F., «The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act», *JIPITEC*, 12, 3 (2021), p. 317-341, https://www.jipitec.eu/issues/jipitec-12-3-2021/5343.

WILS, W. P. J., «Independence of Competition Authorities: The Example of the EU and Its Member States», *World Competition*, 42, 2 (2019), p. 149-169, DOI: 10.54648/WOCO2019012.

ELENCO DEGLI ATTI CITATI

Atti dell'Unione europea

Diritto primario

Trattato sull'Unione europea (Versione consolidata), GU C 202, 07/06/2016.

Trattato sul funzionamento dell'Unione europea (Versione consolidata), GU C 202, 07/06/2016.

Carta dei diritti fondamentali dell'Unione europea, GU C 202, 07/06/2016.

Atti giuridici dell'Unione europea

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, GU L 281, 23/11/1995.

Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, GU L 204, 21/07/1998.

Direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998 relativa ad una modifica della direttiva 98/34/CE che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, GU L 217, 5/08/1998.

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, GU L 178, 17/07/2000.

Decisione della Commissione 2000/520/CE del 26 luglio 2000 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande

più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, GU L 215, 25/08/2000.

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, GU L 201, 31/01/2002.

Regolamento (CE) n. 773/2004 della Commissione, del 7 aprile 2004, relativo ai procedimenti svolti dalla Commissione a norma degli articoli 81 e 82 del trattato CE, GU L 123, 27/04/2004.

Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e 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, GU L 149, 11/06/2005.

Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105, 13/04/2006.

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 (codificazione), GU L 241, 17/09/2015.

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, GU L 119, 04/05/2016.

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 116, 04/05/2016.

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, GU L 207, 01/08/2016.

Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, GU L 88, 31/03/2017.

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, GU L 295, 21/11/2018.

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, GU L 303, 14/11/2018.

Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, GU L 136, 22/05/2019.

Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online, GU L 172, 17/05/2021.

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, GU L 265, 12/10/2022.

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, GU L 277, 27/10/2022.

Decisione di esecuzione (UE) 2023/1795 della Commissione del 10 luglio 2023 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

sul livello di protezione adeguato dei dati personali nell'ambito del quadro UE-USA per la protezione dei dati personali, GU L 231, 20/09/2023.

Altri atti di istituzioni, organi od organismi dell'Unione europea

Gruppo di lavoro articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017, versione emendata e adottata in data 6 febbraio 2018 (wp251rev.01), disponibili al link https://ec.europa.eu/newsroom/article29/items/612053/en.

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

Comitato europeo per la protezione dei dati, Decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, adottata il 9 novembre 2020, https://edpb.europa.eu/system/files/2021-04/edpb_bindingdecision01_2020_it.pdf.

Garante europeo della protezione dei dati, *Opinion 1/2021 on the Proposal for a Digital Services Act*, 10 febbraio 2021.

Linee guida 9/2020 sull'obiezione pertinente e motivata ai sensi del regolamento (UE) 2016/679, versione 2.0, adottate il 9 marzo 2021, https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202009_rro_final_it.pdf.

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

Comitato europeo per la protezione dei dati, Decisione vincolante 1/2021 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente WhatsApp Ireland ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, adottata il 28 luglio 2021, https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_it.pdf.

Comitato europeo per la protezione dei dati, Regolamento interno, versione 8, adottato il 25 maggio 2018, modificato da ultimo e adottato il 6 aprile 2022, https://www.edpb.europa.eu/system/files/2022-08/edpb_rules_of_procedure_version_8_adopted_20220406_it.pdf.

Comitato europeo per la protezione dei dati, Decisione vincolante 1/2023 in merito alla controversia presentata dall'autorità di controllo irlandese sui trasferimenti di dati da parte di Meta Platforms Ireland Limited per il servizio offerto da Facebook (articolo 65 GDPR), adottata il 13 aprile 2023, https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_it.pdf.

Comitato europeo per la protezione dei dati, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, versione 2.0, adottate in data 14 febbraio 2023, disponibili al seguente link: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

Comitato europeo per la protezione dei dati, Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR, versione 2.1, adottate il 24 maggio 2023, https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_it_0.pdf.

Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679 (COM(2023) 348 final).

Atti degli Stati membri

Decreto legislativo 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali», recante «disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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)» (GU n. 174 del 29/07/2003).

Bundeskartellamt, decisione B6-22/16 del 6 febbraio 2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con Deliberazione del 4 aprile 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9107633.

Decreto-legge 15 settembre 2023, n. 123, recante «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale» (GU n. 216 del 15/09/2023), convertito con modificazioni dalla L. 13 novembre 2023, n. 159 (GU 14/11/2023, n. 266).

ELENCO DEI CASI CITATI

Giurisprudenza della Corte di giustizia dell'Unione Europea

Corte di giustizia (sentenze ed ordinanze)

Corte giust., 13 giugno 1958, causa 9-56, *Meroni & Co., Industrie Metallurgiche S.p.A. c. Alta Autorità della Comunità europea del Carbone e dell'Acciaio*, ECLI:EU:C:1958:7.

Corte giust., 15 luglio 1963 (Grande Sezione), causa 25-62, *Plaumann & Co. c. Commissione della Comunità economica europea*, ECLI:EU:C:1963:17.

Corte giust., 5 maggio 1970, causa 77/69, *Commissione delle Comunità europee c. Regno del Belgio*, ECLI:EU:C:1970:34.

Corte giust., 16 dicembre 1976, 33/76, *Rewe-Zentralfinanz eG e Rewe-Zentral AG contro Landwirtschaftskammer für das Saarland*, ECLI:EU:C:1976:188.

Corte giust., 20 febbraio 1979, causa 120/78, *Rewe-Zentral AG c. Bundesmonopolverwaltung für Branntwein*, ECLI:EU:C:1979:42.

Corte giust., 17 novembre 1983, causa 292/82, *Firma E. Merck c. Hauptzollamt Hamburg-Jonas*, ECLI:EU:C:1983:335.

Corte giust., 28 gennaio 1986, causa 169/84, *Compagnie française de l'azote (Cofaz) SA ed altri c. Commissione delle Comunità europee*, ECLI:EU:C:1986:42.

Corte giust., 23 aprile 1986, causa 294/83, *Parti écologiste "Les Verts" c. Parlamento europeo*, ECLI:EU:C:1986:166.

Corte giust., 23 settembre 1986, causa 5/85, *AKZO Chemie BV e AKZO Chemie UK Ltd c. Commissione delle Comunità europee*, ECLI:EU:C:1986:328.

Corte giust., 22 ottobre 1987, causa 314/85, *Foto-Frost c. Hauptzollamt Lübeck-Ost*, ECLI:EU:C:1987:452.

Corte giust., 26 aprile 1988, causa 352/85, *Bond van Adverteerders e altri c. Stato dei Paesi Bassi*, ECLI:EU:C:1988:196.

Corte giust., 14 febbraio 1989, causa 247/87, *Star Fruit Company SA c. Commissione delle Comunità europee*, ECLI:EU:C:1989:58.

Corte giust., 22 giugno 1989, causa 103/88, *Fratelli Costanzo SpA c. Comune di Milano*, ECLI:EU:C:1989:256.

Corte giust., 22 maggio 1990, causa C-70/88, *Parlamento europeo c. Consiglio delle Comunità europee*, ECLI:EU:C:1990:217.

Corte giust., 21 settembre 1989, causa 68/88, *Commissione delle Comunità europee c. Repubblica ellenica*, ECLI:EU:C:1989:339.

Corte giust., 19 marzo 1991, causa C-202/88, *Repubblica francese c. Commissione delle Comunità europee*, ECLI:EU:C:1991:120.

Corte giust., 23 aprile 1991, causa C-41/90, *Klaus Höfner e Fritz Elser c. Macrotron GmbH*, ECLI:EU:C:1991:161.

Corte giust., 16 giugno 1993, causa C-325/91, *Repubblica francese c. Commissione delle Comunità europee*, ECLI:EU:C:1993:245.

Corte giust., 27 ottobre 1993, causa C-69/91, *Procedimento penale contro Francine Decoster, in Gillon*, ECLI:EU:C:1993:853.

Corte giust., 9 marzo 1994, causa C-188/92, *TWD Textilwerke Deggendorf GmbH c. Repubblica Federale di Germania*, ECLI:EU:C:1994:90.

Corte giust., 10 maggio 1995, causa C-384/93, *Alpine Investments BV c. Minister van Financiën*, ECLI:EU:C:1995:126.

Corte giust., 30 novembre 1995, causa C-55/94, *Reinhard Gebhard c. Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, ECLI:EU:C:1995:411.

Corte giust., 24 ottobre 1996, causa C-32/95 P, *Commissione delle Comunità europee contro Lisrestal - Organização Gestão de Restaurantes Colectivos Ld^{a}, Gabinete Técnico de Informática Ld^{a} (GTI), Lisnico - Serviço Marítimo Internacional Ld^{a}, Rebocalis - Rebocagem e Assistência Marítima Ld^{a} e Gaslimpo - Sociedade de Desgasificação de Navios SA*, ECLI:EU:C:1996:402.

Corte giust., 13 maggio 1997, causa C-233/94, *Repubblica federale di Germania c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:1997:231.

Corte giust., 3 ottobre 2013 (Grande Sezione), causa C-583/11 P, *Inuit Tapiriit Kanatami e altri c. Parlamento europeo e Consiglio dell'Unione europea*, ECLI:EU:C:2013:625.

Corte giust., 7 novembre 2013, causa C-518/11, *UPC Nederland BV c. Gemeente Hilversum*, ECLI:EU:C:2013:709.

Corte giust., 16 gennaio 2014, causa C-45/13, *Andreas Kainz c. Pantherwerke AG*, ECLI:EU:C:2014:7.

Corte giust., 14 marzo 2013, causa C-32/11, *Allianz Hungária Biztosító Zrt. e a. c. Gazdasági Versenyhivatal*, ECLI:EU:C:2013:160.

Corte giust., 27 marzo 2014, causa C-314/12, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192.

Corte giust., 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, ECLI:EU:C:2014:238.

Corte giust., 8 aprile 2014 (Grande Sezione), causa C-288/12, *Commissione europea c. Ungheria*, ECLI:EU:C:2014:237.

Corte giust., 8 maggio 2014, causa C-604/12, *H.N. c. Minister for Justice, Equality and Law Reform e a.*, ECLI:EU:C:2014:302.

Corte giust., 13 maggio 2014 (Grande Sezione), causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, ECLI:EU:C:2014:317.

Corte giust., 17 luglio 2014, cause riunite C-141/12 e C-372/12, *YS c. Minister voor Immigratie, Integratie en Asiel e Minister voor Immigratie, Integratie en Asiel c. M e S*, ECLI:EU:C:2014:2081.

Corte giust., 11 settembre 2014, causa C-291/13, *Sotiris Papasavvas c. O Fileleftheros Dimosia Etaireia Ltd e a.*, ECLI:EU:C:2014:2209.

Corte giust., 5 novembre 2014, causa C-166/13, *Sophie Mukarubega c. Préfet de police e Préfet de la Seine-Saint-Denis*, ECLI:EU:C:2014:2336.

Corte giust., 11 dicembre 2014, causa C-249/13, *Khaled Boudjlida c. Préfet des Pyrénées-Atlantiques*, ECLI:EU:C:2014:2431.

Corte giust., ordinanza del 28 gennaio 2015, causa C-411/14 P, *Romano Pisciotti c. Commissione europea*, ECLI:EU:C:2015:48

Corte giust., 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, ECLI: ECLI:EU:C:2015:650.

Corte giust., 15 settembre 2016, causa C-484/14, *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, ECLI:EU:C:2016:689.

Corte giust., 20 dicembre 2017 (Grande Sezione), causa C-434/15, *Asociación Profesional Elite Taxi c. Uber Systems Spain SL*, ECLI:EU:C:2017:981.

Corte giust., 20 febbraio 2018 (Grande Sezione), causa C-16/16 P, *Regno del Belgio c. Commissione europea*, ECLI:EU:C:2018:79.

Corte giust., 5 giugno 2018 (Grande Sezione), causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

Corte giust., 25 luglio 2018 (Grande Sezione), causa C-135/16, *Georgsmarienhütte GmbH e a. c. Bundesrepublik Deutschland*, ECLI:EU:C:2018:582.

Corte giust., 4 ottobre 2018, causa C-416/17, *Commissione europea c. Repubblica francese (anticipo d'imposta)*, ECLI:EU:C:2018:811.

Corte giust., 6 novembre 2018 (Grande Sezione), cause riunite da C-622/16 P a C-624/16 P, *Scuola Elementare Maria Montessori Srl c. Commissione europea, Commissione europea c. Scuola Elementare Maria Montessori Srl e Commissione europea c. Pietro Ferracci*, ECLI:EU:C:2018:873.

Corte giust., 19 dicembre 2018 (Grande Sezione), causa C-219/17, *Silvio Berlusconi e Finanziaria d'investimento Fininvest SpA (Fininvest) c. Banca d'Italia e Istituto per la Vigilanza Sulle Assicurazioni (IVASS)*, ECLI:EU:C:2018:1023.

Corte giust., 14 marzo 2019, causa C-724/17, *Vantaan kaupunki c. Skanska Industrial Solutions Oy e a.*, ECLI:EU:C:2019:204.

Corte giust., 8 maggio 2019, causa C-230/18, *PI contro Landespolizeidirektion Tirol*, ECLI:EU:C:2019:383.

Corte giust., 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, ECLI:EU:C:2019:821.

Corte giust., 19 dicembre 2019 (Grande Sezione), causa C-390/18, *Airbnb Ireland*, ECLI:EU:C:2019:1112.

Corte giust., ordinanza del 27 marzo 2024, causa C-639/23 P(R), *Commissione c. Amazon Services Europe*, ECLI:EU:C:2024:277.

Corte giust., causa C-97/23 P, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati*, pendente.

Corte di giustizia (pareri)

Parere della Corte (Grande Sezione) del 26 luglio 2017, 1/15, ECLI:EU:C:2017:592.

Pareri dell'Avvocato Generale

Conclusioni dell'AG Geelhoed presentate il 29 aprile 2004, causa C-304/02, *Commissione delle Comunità europee c. Repubblica francese*, ECLI:EU:C:2004:274.

Conclusioni dell'AG Szpunar presentate l'11 maggio 2017, causa C-434/15, *Asociación Profesional Elite Taxi c. Uber Systems Spain SL*, ECLI:EU:C:2017:981.

Conclusioni dell'AG Bobek presentate il 13 gennaio 2021, causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2021:5.

Tribunale

Trib. UE, sentenza del 18 settembre 1992, causa T-24/90, *Automec Srl c. Commissione delle Comunità europee*, ECLI:EU:T:1992:97.

Trib. UE, sentenza del 27 febbraio 2014, causa T-256/11, *Ahmed Abdelaziz Ezz e a. c. Consiglio dell'Unione europea*, ECLI:EU:T:2014:93.

Trib. UE, sentenza del 4 marzo 2015, causa T-496/11, *Regno Unito di Gran Bretagna e Irlanda del Nord c. Banca centrale europea (BCE)*, ECLI:EU:T:2015:133.

Trib. UE, sentenza del 4 dicembre 2015, causa T-273/13, *Mohammad Sarafraz c. Consiglio dell'Unione europea*, ECLI:EU:T:2015:939.

Trib. UE, sentenza dell'8 maggio 2018, causa T-283/15, *Esso Raffinage c. Agenzia europea per le sostanze chimiche*, ECLI:EU:T:2018:263.

Trib. UE, sentenza del 27 luglio 2022 (Grande Sezione), causa T-125/22, *RT France c. Consiglio dell'Unione europea*, ECLI:EU:T:2022:483.

Trib. UE, ordinanza del 7 dicembre 2022, causa T-709/21, *WhatsApp Ireland c. Comitato europeo per la protezione dei dati*, ECLI:EU:T:2022:783.

Trib. UE, ordinanza del 27 settembre 2023, causa T-367/23R, *Amazon Services Europe c. Commissione*, ECLI:EU:T:2023:589.

Trib. UE, ordinanza del 16 ottobre 2023, causa T-348/23, *Zalando c. Commissione*

Trib. UE, causa T-348/23, *Zalando c. Commissione*, pendente

Trib. UE, causa T-367/23, *Amazon Services Europe c. Commissione*, pendente.

Giurisprudenza della Corte europea dei diritti dell'uomo

Corte EDU, sentenza del 13 febbraio 2003, *Çetin e a. c. Turchia*, ECHR:2003:0213JUD004015398.

Corte EDU, sentenza del 10 marzo 2009, *Times Newspapers Ltd c. Regno Unito*, ECHR:2009:0310JUD000300203.

Corte EDU, sentenza del 18 dicembre 2012, *Ahmet Yıldırım c. Turchia*, ECHR:2012:1218JUD000311110.

Corte EDU, sentenza del 1 dicembre 2015, *Cengiz e a. c. Turchia*, ECHR:2015:1201JUD004822610.

Corte EDU, sentenza del 23 giugno 2020, *Vladimir Kharitonov c. Russia*, ECHR:2020:0623JUD001079514.

Giurisprudenza degli Stati membri

TAR Lazio, sez. I, 10 gennaio 2020, n. 261.

Rechtbank Den Haag, sentenza del 5 febbraio 2020, ECLI:NL:RBDHA:2020:865.

Conseil constitutionnel, sentenza del 18 giugno 2020, https://www.legifrance.gouv.fr/cons/id/CONSTEXT000042053930/.

Tribunal Supremo, sentenza del 19 luglio 2022, n. 1039/2022, ECLI:ES:TS:2022:3207.

Cass. civ., sez. I, ordinanza 11 ottobre 2023, n. 28417.