Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

CINZIA PERARO*

PROTEZIONE EXTRATERRITORIALE DEI DIRITTI: IL TRASFERIMENTO DEI DATI PERSONALI DALL'UNIONE EUROPEA VERSO PAESI TERZI

SOMMARIO: 1. Introduzione: il caso *Schrems II* e l'estensione extraterritoriale del diritto dell'Unione. – 2. L'ambito di applicazione del RGPD. – 3. Il controllo della Corte di giustizia. – 4. La protezione dei diritti fondamentali. – 5. Il ruolo dei garanti nazionali. – 6. Considerazioni conclusive.

1. *Introduzione: il caso* Schrems II *e l'estensione extraterritoriale del diritto dell'Unione*

La sentenza *Schrems II*[1], con cui la Grande Sezione della Corte di giustizia ha dichiarato l'invalidità della decisione di adeguatezza 2016/1250, c.d. "scudo per la *privacy*"[2], offre lo

* Ricercatore a tempo determinato di tipo B in Diritto dell'Unione europea, Università degli Studi di Bergamo.

[1] Corte di giustizia (Grande Sezione), sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner* c. *Facebook Ireland Limited e Maximillian Schrems*, EU:C:2020:559 (nota come *Schrems II*). Per alcuni commenti, v. G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza* Schrems II *della Corte di giustizia*, in *St. integr. eur.*, 2020, p. 563 ss.; A. CHANDER, *Is Data Localization a Solution for Schrems II?*, in *Jour. Int. Econ. Law*, 2020, n. 23, p. 771 ss.; T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, in *Europeanlawblog.eu*, 21 July 2020; E FLETT, J. WILSON, J. CLOVER, *Schrems Strikes Again: EU-US Privacy Shield Suffers Same Fate as Its Predecessor*, in *Computer and Telecommunication Law Review*, 2020, n. 6, p. 161 ss.; G. FORMICI, *Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione europea a Stati terzi, le Conclusioni dell'Avvocato generale nel caso* Data Protection Commissioner *v.* Facebook Ireland Limited e Maximillian Schrems *e una storia che rischia di ripetersi*, in *Rivista di diritto dei media - MediaLaws*, 2020, n. 1, p. 310 ss.; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Dir. um. dir. int.*, 2020, p. 733 ss.; I. OLDANI, *The future of data transfer rules in the aftermath of Schrems II*, in *SIDIBlog*, 23 ottobre 2020; F. ROSSI DAL POZZO, *L'Accordo* Privacy Shield *non è un vero scudo per la* privacy: *scenari passati e futuri in merito a trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Riv. dir. int.*, 2020, p. 1112 ss.; D. SIMON, *Coup de tonnerre dans le monde du numérique*, in *Europe*, 2020, n. 8-9, p. 5 ss.; X. TRACOL, *"Schrems II": The return of the Privacy Shield*, in *Computer Law & Security Review*, 2020, n. 39, p. 1 ss.; W.G. VOSS, *Cross-Border Data Flows, the GDPR, and Data Governance*, in *Washington International Law Journal*, 2020, n. 3, p. 485 ss.; J.X. DHONT, *Schrems II. The EU adequacy regime in existential crisis?*, in *Maastricht Jour. Eur. Comp. Law*, 2019, n. 5, p. 597 ss. Si veda anche Comitato europeo per la protezione dei dati, *Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner* c. *Facebook Ireland Ltd* e *Maximillian Schrems*, 23 luglio 2020, reperibili al sito Internet https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_it.

[2] 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* [notificata con il numero C(2016) 4176], in *GUUE*, L 207 del 1° agosto 2016, p. 1 ss.

spunto per svolgere alcune riflessioni in tema di extraterritorialità[3] del diritto dell'Unione europea applicabile al caso specifico del trasferimento dei dati personali[4] di persone fisiche[5]

[3] Il termine "extraterritorialità" non deve essere riferito all'applicazione universale del diritto dell'Unione, ma va inteso come estensione territoriale, oltre i confini dell'Unione stessa, della sua portata e della sua efficacia, applicandosi a fattispecie che si verificano altrove, ma che con essa presentano un collegamento sufficiente. Ciò emerge, come verrà osservato nel presente lavoro, dai criteri di determinazione dell'ambito geografico del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in *GUUE*, L 119 del 4 maggio 2016, p. 1 ss., nonché nelle ipotesi di trasferimento transfrontaliero dei dati, dove, in base alla relativa disciplina, la Corte di giustizia può spingersi fino a valutare la normativa straniera applicabile alle (successive) operazioni di trattamento dei dati personali trasferiti dagli Stati membri, sebbene localizzate in Stati terzi e non rientranti quindi nell'ambito di applicazione territoriale del RGPD, al fine di garantire i diritti dei titolari dei dati stessi e permettere il loro trasferimento. Sull'espansione territoriale della normativa in materia di protezione dei dati personali, v. anche M. BRKAN, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?*, in *Maastricht Jour. Eur. Comp. Law*, 2016, n. 5, p. 812 ss., spec. p. 827 ss. In generale, sull'extraterritorialità, v. M. CREMONA, J. SCOTT (eds.), *EU Law Beyond Borders. The Extraterritorial Reach of EU Law*, Oxford, 2019. Inoltre, occorre tenere distinto l'ulteriore profilo, che non sarà oggetto della presente analisi, dell'esercizio della sovranità da parte di uno Stato rispetto ad attività che si verificano al di fuori dei confini del proprio territorio e dell'efficacia extraterritoriale dei provvedimenti adottati dalle sue autorità, qualora ciò sia previsto dalle norme nazionali sulla giurisdizione. A tal riguardo, si veda, con riferimento all'ingiunzione, adottata nei confronti di Facebook, di cessare la diffusione di informazioni personali, la sentenza della Corte di giustizia del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek* c. *Facebook Ireland Limited*, EU:C:2019:821, punto 48 ss., dove si afferma che la normativa europea, nella specie la direttiva 2000/31, non prevede «alcuna limitazione, segnatamente territoriale, alla portata dei provvedimenti che gli Stati membri hanno diritto di adottare conformemente alla direttiva in parola» e che «non osta a che detti provvedimenti ingiuntivi producano effetti a livello mondiale»; tuttavia «stante la dimensione mondiale dei servizi elettronici, il legislatore dell'Unione ha ritenuto necessario garantire la coerenza delle norme dell'Unione in tale ambito con le norme applicabili a livello internazionale» e pertanto « [s]petta agli Stati membri garantire che i provvedimenti da essi adottati e che producono effetti a livello mondiale tengano debitamente conto di queste ultime norme». Con riferimento al diritto all'oblio e alla portata territoriale dell'obbligo di deindicizzazione o rimozione dei dati, si vedano le sentenze della Corte di giustizia (Grande Sezione) del 24 settembre 2019, causa C-507/17, *Google LLC* c. *Commission nationale de l'informatique et des libertés (CNIL)*, EU:C:2019:772, e del 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc.* c. *Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, EU:C:2014:317. In dottrina, tra i molti, v. G. FROSIO, *Enforcement of European rights on a global scale*, in E. ROSATI (ed.), *Handbook of European Copyright Law*, London, 2021, reperibile al sito Internet https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3650521; R. CAFARI PANICO, *Riflessioni sul diritto all'oblio e la libertà di espressione nel caso Eva Glawschnig-Piesczek/Facebook*, in *Liber amicorum per Massimo Panebianco*, Napoli, 2020, p. 57 ss.; F. CALOPRISCO, *La Corte di giustizia si esprime sulla portata territoriale dell'obbligo di deindicizzare i dati personali* online. *Sul bilanciamento caso per caso tra* selfrestraint *ed espansionismo del diritto dell'Unione*, in *Annali AISDUE*, vol. I, Bari, 2020, p. 357 ss.; H. MUIR WATT, *La portée territoriale du droit au déréférencement: un exercice de proportionnalité dans l'espace*, in *Rev. cr. dr. int. privé*, 2020, n. 2, p. 334 ss.; C. RAUCHEGGER, A. KUCZERAWY, *Injunctions to remove illegal online content under the eCommerce Directive:* Glawischnig-Piesczek, in *Comm. M. Law Rev.*, 2020, n. 57, p. 1495 ss.; M.G. STANZIONE, *Libertà di espressione e diritto alla* privacy *nel dialogo delle Corti. Il caso del diritto all'oblio*, in *Eur. dir. priv.*, 2020, n. 3, p. 991 ss.; M. SZPUNAR, *Territoriality of Union law in the era of globalisation*, in D. PETRLIK, M. BOBEK, J.M. PASSER (cor.), *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux. Liber amicorum Jiří Malenovský*, Bruxelles, 2020, p. 149 ss.; G. BEVILACQUA, *La dimensione territoriale dell'oblio in uno spazio globale e universale*, in *Federalismi.it*, 2019, n. 23; B. HESS, *Protecting privacy by cross-border injunction*, in *Riv. dir. int. priv. proc.*, 2019, n. 2, p. 284 ss.; F. ZORZI GIUSTINIANI, *Il diritto all'oblio nella rete e i suoi limiti nell'attuale contesto europeo*, in AA.VV., *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, Bari, 2019, p. 919 ss.; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018, p. 82 ss.; O. LINSKEY, *The Europeanisation of Data Protection Law*, in *Camb. YB Eur. Legal Studies*, 2017, p. 252 ss.; G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015; C. KUNER, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, in *International Data Privacy Law*, 2015, n. 4, p. 235 ss.; ID., Google Spain *in the EU and International context*, in *Maastricht Jour.*

verso paesi terzi[6], disciplinato nel regolamento (UE) 2016/679 in materia di protezione dei dati personali (RGPD), che, come noto, sostituisce dal 25 maggio 2018 la direttiva 95/46[7].

Le questioni pregiudiziali sottoposte dalla *High Court* irlandese alla Corte di giustizia riguardavano l'applicabilità del RGPD ai trasferimenti di dati personali verso gli Stati Uniti fondati su clausole contrattuali tipo contenute nella decisione 2010/87 della Commissione europea[8]; il livello di protezione richiesto da tale regolamento nell'ambito di un siffatto

Eur. Comp. Law, 2015, n. 1, p. 158 ss.; A.L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione "digitale"*, in *St. integr. eur.*, 2015, n. 2, p. 347 ss.

[4] Sulla definizione di dati personali, v. art. 4, n. 1 del RGPD, e in dottrina, tra i molti, C. DEL FEDERICO, A.R. POPOLI, *Le definizioni*, in G. FINOCCHIARO (dir.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 63 ss., spec. p. 64 ss.; D. RÜCKER, *Scope of application of the GDPR*, in D. RÜCKER, T. KUGLER (eds.), *New European General Data Protection Regulation. A Practitioner's Guide*, Baden-Baden, 2018, p. 9 ss., spec. p. 12 ss.; A. PISAPIA, *La tutela*, cit., p. 29 s.

[5] Il regolamento ha come obiettivo la protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali: v. art. 10 e considerando 14 del RGPD.

[6] I trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali sono regolati dal capo V, artt. 44-50, del RGPD, su cui v. anche il considerando 101. Con riferimento alla disciplina contenuta nella precedente direttiva 95/46, la Corte di giustizia, con sentenza del 6 novembre 2003, causa C-101/01, *procedimento penale a carico di Bodil Lindqvist*, EU:C:2003:596, spec. punto 69, aveva escluso che si potesse ritenere sussistente «un "trasferimento verso un paese terzo di dati personali" ogni volta che dati personali vengono caricati su una pagina Internet», altrimenti si tratterebbe di «un trasferimento verso tutti i paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet». In quest'ultimo caso, la disciplina di cui al capo IV della direttiva 95/46 diverrebbe infatti «necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale» e che «non appena la Commissione constatasse, ai sensi dell'art. 25, n. 4, della direttiva 95/46, che un solo paese terzo non garantisce un livello di protezione adeguato, gli Stati membri sarebbero tenuti ad impedire qualsiasi immissione su Internet di dati personali». Per un commento alla sentenza, tra i molti, v. A. GIANNACCARI, *Il trasferimento di dati personali in Internet*, in *Danno e responsabilità*, 2004, n. 4, p. 382 ss.; nonché M.C. MENEGHETTI, *I trasferimenti di dati personali all'estero*, in G. FINOCCHIARO (dir.), *La protezione dei dati personali*, cit., p. 594 ss., spec. p. 607 ss.; P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza* Schrems *e nel nuovo regolamento generale sulla protezione dei dati*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, p. 169 ss., spec. p. 174. Per un inquadramento del tema del trasferimento transnazionale dei dati, v. G. CAGGIANO, *Sul trasferimento*, cit., p. 577 ss.; F. BALDUCCI ROMANO, *I trasferimenti di dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 949 ss.; M.C. MENEGHETTI, *I trasferimenti*, cit., p. 594 ss.; R. PANETTA, *Il trasferimento all'estero dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 357 ss.; E.A. ROSSI, Data protection *nei rapporti transnazionali tra imprese. Aspetti problematici della Convenzione n. 108 del Consiglio d'Europa e del regolamento (UE) 679/2016*, in *St. integr. eur.*, 2019, p. 209 ss., spec. p. 215 ss.; D. KELLEHER, K. MURRAY, *EU Data Protection Law*, London, 2018, p. 116 ss.; A. PISAPIA, *La tutela*, cit., p. 110 ss.; F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *Diritto Mercato Tecnologie*, numero speciale 2017, p. 129 ss.; L. VALLE, L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Il Diritto dell'informazione e dell'informatica*, 2017, n. 1, p. 169 ss.

[7] 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*, in *GUCE*, L 281 del 23 novembre 1995, p. 31 ss.

[8] Decisione 2010/87/UE della Commissione, del 5 febbraio 2010, *relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi* a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio [notificata con il numero C(2010) 593], in *GUUE*, L 39 del 12 febbraio 2010, p. 5 ss., come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione del 16 dicembre 2016 [notificata con il numero C(2016) 8471], in *GUUE*, L 344 del 17 dicembre 2016, p. 100 ss.. La decisione del 2010 è stata sostituita con la decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 *relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi* a norma del

trasferimento; gli obblighi che incombono alle autorità nazionali di controllo in tale contesto e, infine, la compatibilità dell'istituzione di un mediatore, avvenuta nella pendenza del giudizio sulla base della decisione "scudo per la *privacy*", con i diritti fondamentali, quali la tutela dei dati personali[9] e il rispetto della vita privata[10], garantiti rispettivamente dagli artt. 8 e 7 della Carta dei diritti fondamentali dell'Unione europea, nonché col diritto a un ricorso effettivo di cui all'art. 47 della Carta stessa. Seppur non direttamente richiesta dal giudice del rinvio, la Corte di giustizia ha valutato la legittimità della decisione del 2016, ritenendo di dover affrontare i dubbi sollevati in merito alla figura del mediatore e alla tutela che deve essere garantita in forza dei summenzionati artt. 7, 8 e 47 della Carta, nel contesto del trasferimento dei dati al paese terzo, alla luce del nuovo quadro normativo contenuto nella decisione in parola[11].

Sulla base delle argomentazioni sviluppate dalla Corte, nel presente lavoro si intende analizzare i profili di extraterritorialità che emergono con riferimento all'applicazione della normativa contenuta nel RGPD, tenendo conto delle disposizioni relative alla delimitazione del suo campo di applicazione, per poi esaminare l'estensione del controllo giurisdizionale dei giudici del Lussemburgo, in sede di verifica della validità dell'atto di esecuzione su cui si fonda il trasferimento dei dati, avendo, in specie, riguardo all'ordinamento degli Stati Uniti, e, infine, dare atto della protezione extraterritoriale dei diritti fondamentali propri dell'ordinamento europeo che vengono in gioco in questa ipotesi. A ciò si aggiunge, quale ulteriore profilo, l'ambito di competenza delle autorità di controllo nazionali, che sarà qui analizzato con riferimento alla loro valutazione in concreto della conformità del trasferimento dei dati all'estero al diritto dell'Unione.

---

regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, C/2021/3972, in *GUUE*, L 199 del 7 giugno 2021, p. 31 ss.

[9] Sul diritto fondamentale alla protezione dei dati personali, v. considerando 1 del RGPD. In argomento, cfr. F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *Annali AISDUE*, 2020, vol. I, p. 63 ss., spec. p. 66 ss. e 71 ss.; M.C. MENEGHETTI, *The different shapes of extraterritoriality in EU data protection law and its international justifications*, in *Dir. comm. int.*, 2019, n. 4, p. 695 ss., spec. p. 697; C. PERARO, *Legittimazione ad agire di un'associazione a tutela dei consumatori e diritto alla protezione dei dati personali a margine della sentenza Fashion ID*, in *Riv. dir. int. priv. proc.*, 2019, n. 4, p. 982 ss., spec. p. 990 ss.; D. KELLEHER, K. MURRAY, *EU Data Protection Law*, cit., p. 3 ss.; B. NASCIMBENE, I. ANRÒ, *La tutela dei diritti fondamentali nella giurisprudenza della Corte di giustizia: nuove sfide, nuove prospettive*, in *Riv. it. dir. pub. com.*, 2017, n. 2, p. 323 ss., spec. p. 342 ss.; G.F. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale disomogeneo alla luce della nuova proposta di General Data Protection Regulation*, in *Osservatorio del diritto civile e commerciale*, 2015, n. 2, p. 421 ss.; G. GONZALEZ FUSTER, R. GELLERT, *The fundamental right of data protection in the European Union: in search of an uncharted right*, in *International Review of Law, Computers & Technology*, 2012, n. 1, p. 73 ss.

[10] Sulla distinzione tra tutela della *privacy* e dei dati personali, v. C. FARALLI, *La privacy dalle origini a oggi. Profili storico-filosofici*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati*, cit., p. 1 ss., spec. p. 6 s.; G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (dir.), *La protezione dei dati personali*, cit., p. 1 ss., spec. p. 10 ss.; EAD., *La giurisprudenza della Corte di giustizia in materia di dati personali da* Google Spain *a* Schrems, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali*, cit., p. 113 ss.; M. BRKAN, *The Essence of the Fundamental Rights to Privacy and Data protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, in *Germ. Law Jour.*, 2019, n. 20, p. 864 ss.; V.M. PFISTERER, *The Right to privacy – A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *Germ. Law Jour.*, 2019, n. 20, p. 722 ss., spec. p. 726 ss.; A. FORDE, *The Conceptual Relationship Between Privacy and Data protection*, in *Cam. Law Rev.*, 2016, p. 135 ss.; J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, n. 4, p. 222 ss.

[11] Sentenza *Schrems II*, punto 151; e Avvocato generale Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, causa C-311/18, *Schrems II*, EU:C:2019:1145, punto 160 ss.

Occorre tuttavia premettere alcune considerazioni più generali sull'extraterritorialità del diritto dell'Unione in tema di protezione dei dati personali, trovando essa una prima giustificazione nel suo particolare contesto di riferimento. Il mondo digitale non presenta infatti delimitazioni spaziali e, di conseguenza, i concetti di sovranità e territorio nazionale diventano flessibili e seguono l'oggetto della tutela, vale a dire i dati e i diritti dei titolari. Come si vedrà, il diritto dell'Unione protegge i dati delle persone fisiche che si trovano sul suo territorio e assicura una tutela alle stesse nel caso del loro trasferimento all'estero a fronte di attività di trattamento dei dati che ivi vengono effettuate. Si verifica, in tal modo, un superamento del principio della sovranità territoriale per l'assenza di veri e propri confini del "cyberspazio"[12], dove l'ubiquità di Internet annulla le stesse nozioni di territorio e giurisdizione[13] e richiede un adattamento (o un'estensione) delle norme a tutela dei diritti delle persone. L'Unione, pertanto, adeguandosi alle esigenze dettate dal contesto digitale, ha predisposto, sul piano interno così come su quello esterno, le garanzie necessarie a tutelare i dati e i diritti dei soggetti titolari, ogniqualvolta il diritto UE, e quindi anche la Carta, trovi applicazione[14], al fine di assicurarne una protezione effettiva.

È stato osservato che già con la sentenza *Schrems I*[15], pronunciata in seguito allo scandalo "Datagate" sulla raccolta di dati attraverso programmi di sorveglianza americani[16] e

[12] Sulla definizione del "cyberspazio", v. anche M.B. FORNACIARI, *Sistema delle fonti e definizione dello spazio giuridico europeo*, in *Federalismi.it*, 2021, n. 9, p. 118 ss., spec. p. 121 ss.; D. MARRANI, *Sovranità territoriale e sicurezza internazionale nel* cyberspace, in *Liber amicorum per Massimo Panebianco*, Napoli, 2020, p. 357 ss.

[13] In tal senso, v. Y. PADOVA, *Is the right to be forgotten a universal, regional, or 'glocal' right?*, in *International Data Privacy Law*, 2019, vol. 9, n. 1, p. 15 ss., spec. p. 23.

[14] In generale, sull'ambito di applicazione della Carta, v., per tutti, N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Milano, 2018, p. 133 ss. e 183 ss.

[15] Corte di giustizia (Grande Sezione), sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems* c. *Data Protection Commissioner*, EU:C:2015:650 (nota come *Schrems I*). Per alcuni commenti, v. M.C. MENEGHETTI, *I trasferimenti*, cit., p. 626 ss.; G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizio di comunicazione*, in *Rivista di diritto dei media - MediaLaws*, 2018, n. 2, p. 64 ss., spec. p. 72 ss.; F. BORGIA, *Profili critici*, cit., p. 131 ss.; C. DE TERWANGNE, C. GAYREL, *Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse: les impacts de l'arrêt Schrems*, in *Cah. dr. eur.*, 2017, n. 1, p. 35 ss.; R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost.*, 2016, n. 1, p. 289 ss.; S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la* privacy, in *Dir. pub. comp. eur.*, 2016, n. 3, p. 687 ss.; A. GIATTINI, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso* Schrems *e l'invalidità del sistema di 'approdo sicuro*, in *Dir. um. dir. int.*, 2016, p. 247 ss.; M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione* Schrems *della Corte di giustizia UE*, in *Dir. Un. eur.*, 2016, n. 4, p. 755 ss.; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Riv. dir. int.*, 2016, n. 3, p. 690 ss.; G. SCARCHILLO, *Dal Safe Harbour al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*, in *Dir. comm. int.*, 2016, n. 4, p. 901 ss.; A. MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati fra EU e USA. Quali scenari per cittadini e imprese?*, in *Contr. Impr./Eur.*, 2015, n. 2, p. 719 ss.; V. SALVATORE, *La Corte di giustizia restituisce (temporaneamente) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti*, in *St. integr. eur.*, 2015, p. 623 ss.; V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il Diritto dell'informatica e dell'informazione*, 2015, n. 4-5, p. 683 ss. Si veda anche la Comunicazione della Commissione al Parlamento europeo e al Consiglio relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14 (*Schrems*), COM(2015)566 final del 6 novembre 2015.

[16] Sulla vicenda, tra i molti, v. M. ROTENBERG, Schrems II, *from Snowden to China: Toward a new alignment on transnatlantic data protection*, in *Eur. Law Jour.,* 2020, n. 26, p. 141 ss.; F. BORGIA, *Profili critici*, cit., p. 131 ss.; M. NINO, *Il caso "Datagate": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla*

riguardante l'invalidità della decisione di adeguatezza 2000/520, c.d. "approdo sicuro"[17], che regolava il trasferimento dei dati dall'Unione agli Stati Uniti, la Corte di giustizia aveva rivendicato «la necessità di poter difendere la sovranità digitale della stessa Unione europea, riconoscendo alle istituzioni europee la piena giurisdizione sul trattamento dei dati personali dei cittadini europei»[18]. Essa aveva quindi ammesso che l'ambito spaziale di Internet in realtà ha dei suoi confini, che sono determinati dalla presenza delle persone titolari dei dati nel territorio degli Stati membri.

La rivendicazione dell'Unione del potere normativo nello spazio digitale mira a stabilire un equilibrio tra la tutela dei diritti fondamentali alla protezione dei dati e alla vita privata, così come garantiti dalla Carta e dalla Corte, da una parte, e gli interessi nazionali legati alla sicurezza pubblica, dall'altra, anche qualora siano le autorità pubbliche del paese terzo ad invocarla come giustificazione delle loro attività di accesso o utilizzo dei dati. Tali operazioni vanno infatti valutate a prescindere dal motivo posto a loro fondamento e alla luce dei principi di necessità e proporzionalità, che, pur essendo parametri propri dell'ordinamento dell'Unione, devono essere rispettati da tutti gli operatori che si trovano nello spazio giuridico europeo. È in tale prospettiva che deve essere esaminata la valutazione effettuata dalla Corte di giustizia nel caso *Schrems II* in merito all'ordinamento degli Stati Uniti, in quanto luogo di destinazione dei dati trasferiti dall'Unione. Al paese terzo vengono così applicati i suddetti requisiti, vuoi indirettamente, perché oggetto d'esame è in realtà la decisione impugnata, tramite la quale viene dato atto delle normative straniere che predispongono mezzi di tutela a favore dei soggetti titolari dei dati personali, vuoi direttamente, perché, in pratica, il sistema di protezione dei diritti fondamentali dell'Unione funge da parametro per valutare l'adeguatezza dello Stato di destinazione.

Si perviene così ad una prima conclusione circa l'espansione degli standard europei "nella rete globale senza frontiere"[19]: le soluzioni legislative e giurisprudenziali si fondano

---

protezione dei dati personali e della privacy, in *Dir. um. dir. int.*, 2013, n. 3, p. 727 ss.; F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *Federalismi.it*, 2013, n. 13.

17 Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti [notificata con il numero C(2000) 2441], in *GUCE*, L 215 del 25 agosto 2000, p. 7 ss.

18 C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *Federalismi.it*, 2019, n. 13, p. 11. Sull'espressione "sovranità digitale", in dottrina, v. G. CAGGIANO, *Sul trasferimento*, cit., p. 564 ss.; nonché V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso* Schrems: *la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali*, cit., p. 7 ss. V. anche le Comunicazioni della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, datate 19 febbraio 2020, *Plasmare il futuro digitale dell'Europa*, COM(2020)67 final, spec. p. 2, e, in relazione alla creazione di uno spazio unico europeo dei dati, *Una strategia europea per i dati*, COM(2020)66 final, spec. a p. 1, dove viene fatto riferimento alla possibilità per l'Unione di "conquistarsi un ruolo guida nell'economia dei dati"; e la precedente Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Scambio e protezione dei dati personali in un mondo globalizzato*, COM(2017)7 final del 10 gennaio 2017, p. 2 s.

19 La Corte di giustizia (Grande Sezione), nella sentenza del 24 settembre 2019, *Google CNIL*, cit., ha affermato che Internet è «una rete globale senza frontiere e i motori di ricerca conferiscono ubiquità alle informazioni e ai link contenuti in un elenco di risultati visualizzato a seguito di una ricerca effettuata a partire dal nome di una persona fisica» (punto 56). Come osservato, « [l]a liquidità dello spazio di Internet comporta necessariamente l'assenza di confini», non trattandosi «di spazi fisici, ma di spazi immateriali delimitati da frontiere prive di forme visibili ma non per questo inesistenti, che il fine di tutelare i dati personali, per loro natura non connessi ad un determinato territorio, consente di superare, ma solo in circostanze eccezionali, come lo sono tutte le

sulla necessità di tutelare, nel contesto digitale, i diritti fondamentali, come garantiti nell'ordinamento europeo, dove la Carta diventa il (solo) criterio di legittimità delle azioni politiche e commerciali. Ne deriverebbe perciò un "effetto Bruxelles"[20] degli standard di tutela dei dati personali propri dell'Unione europea[21], tale da divenire modello globale di protezione[22] e influenzare positivamente le normative degli Stati terzi, finanche a richiedere un loro adeguamento, per poter dialogare con l'Unione stessa[23].

Sta di fatto che, alla luce della giurisprudenza in materia di dati personali e, da ultimo, della sentenza in parola, l'effetto espansivo del diritto dell'Unione non riguarda solo modelli o standard di protezione europei, ma attiene ai diritti fondamentali dello stesso ordinamento, così come vengono garantiti al suo interno, sia sotto il profilo sostanziale e contenutistico sia

---

circostanze nelle quali l'esercizio della 'sovranità', dell'Unione, come degli Stati, esorbita i propri confini» (R. CAFARI PANICO, *Riflessioni*, cit., p. 68).

[20] L'espressione "Brussels Effect" è stata introdotta con riferimento al contesto commerciale, richiamando le modalità con cui il diritto dell'Unione si radicava negli ordinamenti giuridici extraeuropei con l'effetto di "europeizzare" certi aspetti del commercio globale: così A. BRADFORD, *The Brussels Effect*, in *Northwestern University Law Review*, 2012, n. 1, p. 1 ss., dove l'A. definisce il «Europe's unilateral power to regulate global markets» (p. 3) o «process of unilateral regulatory globalization» (p. 10) come un «unprecedented and deeply underestimated global power that the EU is exercising through its legal institutions and standards" e che "successfully exports that influence to the rest of the world» (p. 1); nonché EAD., *The Brussels Effect. How the European Union Rules the World*, Oxford, 2020. In merito, v. anche R. CAFARI PANICO, *Riflessioni*, cit., p. 72; G. COMPARATO, *La sovranità economica fra diritto interno e diritto transnazionale dell'economia. Considerazioni alla luce dell'esperienza britannica*, in *DPCE online*, 2020, n. 1, p. 263 ss., spec. p. 279 s.; C. KUNER, *The Internet and the Global Reach of EU Law*, in M. CREMONA, J. SCOTT (eds.), *EU Law Beyond Borders*, cit., p. 112 ss.; J. SCOTT, *The Global Reach of EU Law*, *ivi*, p. 21 ss., spec. p. 31 ss.

[21] In tal senso, v. R.A. COSTELLO, Schrems II: *Everything is illuminated?*, in *European Papers, European Forum*, 15 October 2020, p. 1 ss., spec. p. 12 s.

[22] È stato osservato che il sistema creato con il RGPD dall'Unione può influenzare gli ordinamenti degli Stati terzi come "global source of inspiration" (C. RYNGAERT, M. TAYLOR, *The GDPR*, cit., p. 9). Non è comunque escluso che altri ordinamenti adottino proprie normative, respingendo l'idea di una forza extraterritoriale del diritto dell'Unione, in un bilanciamento di interessi volti a garantire non solo gli interessi economici, ma anche la tutela delle persone: cfr. G. ROSSOLILLO, *Diritti fondamentali, norme unilaterali e norme imperative alla luce del regolamento 2016/679 sul trattamento e la libra circolazione dei dati personali*, in *Liber Amicorum Angelo Davì. La vita giuridica internazionale nell'età della globalizzazione*, vol. I, Napoli, 2019, p. 597 ss., spec. p. 616 s.; nonché i contributi del *Symposium on the GDPR and international law*, in *Am. Jour. Int. Law, AJIL Unbound*, 2020, n. 114; e X. TRACOL, *"Schrems II"*, cit., p. 7, per il quale, dalle valutazioni della Corte di giustizia in merito al sistema giuridico americano, emerge l'inadeguatezza dei mezzi di protezione a favore dei titolari dei dati trasferiti negli Stati Uniti e la differenza di impostazione di quel sistema, basato su meccanismi di sorveglianza, a differenza dell'Unione, che fonda il suo processo di integrazione attorno alla protezione dei valori e quindi alla tutela dei diritti fondamentali sia sul piano normativo sia su quello giurisdizionale.

[23] Così D. SIMON, *Coup de tonnerre*, cit., p. 10, dove, richiamando il "Brussels Effect", ha auspicato che «cette décision aura une influence positive en proviquant une exportation effective et un contagion salutaire du modèle européen de protection des données personnelles dans le droit des États tiers». Per alcuni commenti in merito al RGPD come modello globale di protezione della *privacy* e dei dati personali, v. i contributi del *Symposium on the GDPR and international law*, cit.; nonché A. BRADFORD, *The Brussels Effect. How the European Union Rules the World*, cit., p. 147 ss.; C. KUNER, *The Internet*, cit., p. 126 s. e 144 s. Il modello europeo di protezione dei diritti fondamentali può quindi fungere da «punto di riferimento a livello mondiale per la regolamentazione dell'economia digitale»: così la Comunicazione della Commissione al Parlamento europeo e al Consiglio, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, COM(2020)264 final del 24 giugno 2020, p. 3. Sull'europeizzazione della *governance* della Rete, quale finalità politica perseguita dalla portata extraterritoriale dell'applicazione del RGPD, v. F. RAGNO, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del* private enforcement *del GDPR*, in *Ordine internazionale e diritti umani*, 2020, n. 4, p. 818 ss., spec. p. 822 e i riferimenti ivi citati.

sotto quello procedurale, per i rimedi richiesti ai fini della loro protezione effettiva[24], quali parte integrante la fattispecie tutelata. Ciò si pone, inoltre, come ulteriore affermazione del processo di costituzionalizzazione del diritto fondamentale alla tutela dei dati personali, con cui la Corte di giustizia sembra così rivendicare il suo ruolo di "scudo per l'Europa"[25] e per i diritti degli individui.

2. *L'ambito di applicazione del RGPD*

La questione dell'applicabilità del RGPD, posta dal giudice del rinvio nella causa *Schrems II*, riguardava l'interpretazione dell'art. 2, par. 1 e par. 2, lett. a) e b) del RGPD in combinato disposto con l'art. 4, par. 2 TUE relativo alla competenza degli Stati membri in materia di sicurezza pubblica nazionale[26]. In merito a tale ultimo aspetto, la Corte di giustizia ha precisato che l'art. 4 TUE trova applicazione solo all'interno dell'Unione e che la sicurezza nazionale rientra nelle competenze esclusive degli Stati membri, non potendo quindi la norma in questione assumere rilevanza nel caso di specie, ove il motivo di giustificazione del trattamento è stato invocato con riferimento alle attività delle autorità del paese terzo[27].

Si trattava pertanto di verificare la disciplina applicabile al trasferimento transfrontaliero dei dati. Il regolamento copre qualsiasi operazione, non necessariamente automatizzata, che riguarda i dati personali, inclusa «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione»[28]. In tali definizioni, osserva la

---

[24] In merito, v. O. LYNSKEY, *Extraterritorial Impact in Data Protection Law through an EU Law Lens*, Working Paper n. 08-2020, Brexit Institute, p. 5; nonché R.A. COSTELLO, *Schrems II*, cit., p. 13, secondo la quale «the evolution of the Brussels Effect from a regulatory trend to a means of exporting a prescriptive formula for adherence to democratic features of government and the ordering and substantive content of another jurisdiction's legal regime is of questionable value in either asserting the legitimacy of the Union's own legal ordering or in fostering sustainable models for bilateral agreement and relationships in digital context».

[25] L'espressione si rinviene nella versione italiana della sentenza *Schrems II*, al punto 190, come risultato della traduzione della locuzione "*privacy shield*" in luogo di "scudo per la *privacy*". Pur errato, il termine "scudo" assume un particolare significato, ai fini del presente lavoro, in quanto evocativo del ruolo della Corte di giustizia volto a garantire la protezione dei diritti dei soggetti titolari dei dati personali. L'idea di una Europa protettiva era già stata sostenuta in relazione al caso *Schrems I*: cfr. L. AZOULAI, M. VAN DER SLUIS, *Institutionalizing personal data protection in times of global institutional distrust:* Schrems, in *Comm. M. Law Rev.*, 2016, vol. 53, p. 1343 ss., spec. p. 1356 e 1362 s., i quali hanno osservato che la sentenza rappresentava «a further declaration of indipendence of protective Europe» nel mondo digitale; nonché, in generale, v. G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *St. integr. eur.*, 2018, n. 1, p. 9 ss.

[26] Sentenza *Schrems II*, punto 80.

[27] *Ivi*, punto 81.

[28] Cfr. artt. 2, par. 1 e 4, punto 2 del RGPD. In merito, l'Avvocato generale Saugmandsgaard Øe (conclusioni del 19 dicembre 2019, *Schrems II*, cit., punto 217 ss.) ha osservato che, a prescindere da un obbligo di conservazione dei dati derivante dalla normativa nazionale, «la messa a disposizione di dati da parte del titolare del trattamento a favore di un'autorità pubblica risponde alla definizione di "trattamento" di cui all'articolo 4, punto 2, del RGPD» e ciò vale anche «per il filtraggio preliminare dei dati mediante criteri di ricerca al fine di isolare quelli relativamente ai quali le autorità pubbliche hanno richiesto l'accesso» (punto 222). La conclusione è che, in base a quanto sostenuto dalla Corte nei casi *Tele2 Sverige* (Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, EU:C:2016:970) e *Ministerio Fiscal* (Grande Sezione, 2 ottobre 2018, causa C-207/16, EU:C:2018:788), «il RGPD e, di conseguenza, la Carta si applicano a una normativa nazionale che impone a un fornitore di servizi di comunicazioni elettroniche di offrire il proprio contributo alle autorità responsabili della sicurezza nazionale, mettendo loro a disposizione i dati, eventualmente dopo averli filtrati, anche indipendentemente da qualsiasi obbligo giuridico di conservazione di tali dati» (punto 223). Sulle attività

Corte, non viene fatto alcun riferimento alla distinzione tra operazioni che siano «realizzate all'interno dell'Unione o presentino un collegamento con un paese terzo»[29]. Nella determinazione dell'ambito di applicazione materiale del RGPD si riscontra così un'apertura a situazioni extraeuropee. Il trasferimento va ricondotto nella nozione di trattamento ai sensi dell'art. 4, punto 2 del RGPD[30], al quale è poi dedicato il capo V, su cui si tornerà in seguito.

Al trasferimento di dati personali, oggetto della causa *Schrems II*, tra due operatori economici (da Facebook Ireland verso Facebook Inc.), a fini commerciali, non trovano in ogni caso applicazione le eccezioni di cui all'art. 2, par. 2 del RGPD, posto che le situazioni ivi escluse riguardano attività che non rientrano nell'ambito di applicazione del diritto dell'Unione (lett. a)[31], che effettuano gli Stati membri nell'ambito della politica estera e di sicurezza comune (lett. b), che consistono in un trattamento di dati compiuto da una persona fisica nell'ambito di un'attività strettamente personale o domestica (lett. c), oppure che sono realizzate dalle autorità competenti per la prevenzione e il perseguimento di reati o l'esecuzione di sanzioni penali, inclusa la salvaguardia della sicurezza pubblica (lett. d)[32].

In base alle disposizioni del regolamento, la Grande Sezione è quindi giunta a ritenere applicabile il RGPD quando i dati, durante o dopo il loro trasferimento, vengono trattati dalle autorità del paese terzo, anche se per scopi connessi alla sua sicurezza nazionale[33]. Tale conclusione, secondo la Corte, è avallata dalla formulazione dell'art. 45, par. 2, lett. a) del RGPD, che impone espressamente alla Commissione di tenere in considerazione, in sede di valutazione dell'adeguatezza del livello di protezione offerto da un paese terzo, «la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione»[34].

La definizione dell'ambito materiale del regolamento va letta alla luce della sua portata territoriale, individuata dall'art. 3[35], che fa riferimento ai criteri dello stabilimento (par. 1) e

---

oggetto del RGPD, tra i molti, v. A. SPANGARO, *L'ambito di applicazione materiale della disciplina del regolamento europeo 679/2016*, in G. FINOCCHIARO (dir.), *La protezione dei dati personali*, cit., p. 27 ss.; A. PISAPIA, *La tutela*, cit., p. 31 ss.; D. KELLEHER, K. MURRAY, *EU Data Protection Law*, cit., p. 61 ss.; D. RÜCKER, *Scope of application of the GDPR*, cit., p. 9 ss.; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, n. 22, spec. p. 10 ss.

[29] Sentenza *Schrems II*, punto 82. Cfr. anche Avvocato generale Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, *Schrems II*, cit., punto 104.

[30] Sentenza *Schrems II*, punto 83.

[31] La formulazione evoca la distinzione tra situazioni puramente interne agli Stati membri e situazioni in cui trova attuazione il diritto dell'Unione: v. F. ROSSI DAL POZZO, *La giurisprudenza*, cit., p. 69 s.

[32] Sentenza *Schrems II*, punti 84-85.

[33] *Ivi*, punto 87.

[34] *Ibidem*; su cui v. anche *infra*, par. 3.

[35] Si vedano al riguardo le *Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3)*, adottate il 12 novembre 2019 dal Comitato europeo per la protezione dei dati, reperibili al sito Internet https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_it. Su tale norma, tra i molti, v. F. RAGNO, *Il diritto fondamentale*, cit., p. 821 s.; A. NERVI, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 161 ss., spec. p. 169 ss.; M.C. MENEGHETTI, *The different shapes of extraterritoriality*, cit., p. 704 ss.; G. ROSSOLILLO, *Diritti fondamentali*, cit., p. 603 ss.; C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., spec. p. 13 ss.; A. SPANGARO, *L'ambito di applicazione materiale*, cit., p. 44 ss.; A. AZZI, *The Challanges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, p. 126 ss.; C. COLAPIETRO, *I principi*, cit., p. 7 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, 2018, n. 3, p. 1098 ss., spec. p. 1113 s.; D. KELLEHER, K. MURRAY, *EU Data Protection Law*, cit., p. 113 ss.; P. SCHUMACHER, *Scope of application of the GDPR*,

dell'indirizzamento o *targeting* (par. 2). In particolare, in base al primo, il RGPD si applica al «trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento»[36] da parte di un titolare o di un responsabile[37] di tali operazioni che si trovi nell'Unione, «indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione». In linea con l'approccio estensivo dei giudici del Lussemburgo in merito alla nozione di stabilimento, adottato già in relazione alla precedente direttiva 95/46, secondo cui essa comprende qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile[38], l'uso del criterio in parola persegue l'obiettivo di assicurare una tutela efficace, in quanto il requisito territoriale viene considerato in modo più affievolito.

Analogamente, il criterio dell'indirizzamento di cui al par. 2 concorre a garantire la tutela delle persone e dei loro dati, basandosi su elementi di collegamento territoriale più flessibili. Il RGPD trova infatti applicazione quando «il trattamento dei dati personali di interessati che si trovano nell'Unione», operato da un titolare o da un responsabile del trattamento ubicato in uno Stato terzo, riguardi l'offerta di beni o la prestazione di servizi ai suddetti interessati nel territorio dell'Unione oppure il monitoraggio del loro comportamento quando questo ha luogo all'interno dell'Unione stessa. In questi casi, il legislatore europeo ha definito l'ambito geografico del RGPD basandosi solo sulla mera presenza, nell'Unione, del titolare dei dati personali, a prescindere dalla sua nazionalità o dal luogo della sua residenza[39].

---

in D. RÜCKER, T. KUGLER (eds.), *New European General Data Protection Regulation*, cit., p. 37 ss., spec. p. 37 ss.; M. GÖMANN, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, in *Comm. M. Law Rev.*, 2017, vol. 54, p. 567 ss.; L. VALLE, L. GRECO, *Transnazionalità*, cit., p. 200 ss.; D. RÜCKER, *Scope of application*, cit., p. 37 ss.

[36] Sulla nozione di "stabilimento", v. considerando 22, che riprende la giurisprudenza della Corte di giustizia relativa alla precedente direttiva 95/46: cfr. (Grande Sezione), sentenza del 13 maggio 2014, *Google Spain*, cit.; nello stesso senso, (Grande Sezione), sentenza del 5 giugno 2018, causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* c. *Wirtschaftsakademie Schleswig-Holstein GmbH*, EU:C:2018:388, punto 57. Sulla formula "contesto delle attività di uno stabilimento", v. G. CAGGIANO, *Sul trasferimento*, cit., p. 568 ss.; ID., *L'interpretazione del criterio di collegamento del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio*, cit., p. 43 ss.; nonché L. VALLE, L. GRECO, *Transnazionalità*, cit., p. 178 ss.; G. ROSSOLILLO, *Diritti fondamentali*, cit., p. 600 ss.; C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., p. 13 ss.; W.G. VOSS, *Cross-Border Data Flows*, cit., p. 495 s.; D. RÜCKER, *Scope of application*, cit., p. 37 s.; A. PISAPIA, *La tutela*, cit., p. 32 ss.; G. CASSANO, I.P. CIMINO, *Qui, là, in nessun luogo… Come le frontiere dell'Europa si aprirono a Internet: cronistoria di una crisi annunciata per le regole giuridiche fondate sul principio di territorialità*, in *Giur. it.*, 2004, n. 10, p. 1805 ss.

[37] Per le definizioni di titolare e responsabile del trattamento, v. art. 4, punti 7 e 8 del RGPD. In generale sui soggetti del trattamento, v. D. FARACE, *Il titolare e il responsabile del trattamento*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 731 ss.; L. GRECO, *L'organigramma privacy: I soggetti del trattamento*, in G. FINOCCHIARO (dir.), *La protezione dei dati personali*, cit., p. 321 ss.; D. RÜCKER, *Scope of application*, cit., p. 23 ss. Cfr. altresì *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, adottato il 16 febbraio 2010 dal Gruppo di lavoro Articolo 29 per la protezione dei dati, reperibile al sito Internet https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_it.pdf.; sostituito dalle *Linee guida 7/2020* adottate il 2 settembre 2020 dal Comitato europeo per la protezione dei dati, reperibili al sito Internet https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[38] Cfr. *Linee guida 3/2018*, cit., p. 7, dove viene chiarito che, al fine di determinare uno stabilimento, «la soglia può essere piuttosto bassa quando le attività di un titolare del trattamento si focalizzano sulla prestazione di servizi online», bastando «la presenza nell'Unione di un solo dipendente o agente di un soggetto extra UE» qualora la sua attività sia «sufficientemente stabile».

[39] Sul punto, v. *Linee guida 3/2018*, cit., p. 15 ss., dove viene precisato che la definizione di interessati nell'Unione non si basa su criteri quali la cittadinanza, la residenza o altri elementi della condizione giuridica dei soggetti i cui dati sono oggetto di trattamento, e che ciò si pone in linea con la formulazione generica del soggetto titolare del diritto alla protezione dei dati personali di cui all'art. 8 della Carta che si riferisce a "ogni individuo"; nonché

La disposizione è infatti caratterizzata da «un capovolgimento dei soggetti attori»[40], in applicazione del principio della personalità passiva[41], poiché viene fatto riferimento ai titolari dei dati per individuare le attività che rientrano nel campo di applicazione del regolamento. Questa norma è anche espressione della "dottrina degli effetti"[42], in base alla quale vengono prese in considerazione le conseguenze, che si verificano nell'Unione, di operazioni localizzate altrove. Ciò che rileva, quindi, è l'intenzione dell'autore (titolare o responsabile) del trattamento di offrire beni o servizi[43] a persone fisiche che si trovano nell'Unione oppure di monitorare il comportamento di suddette persone[44].

Alla luce delle disposizioni analizzate, si può dunque parlare di estensione extraterritoriale dell'ambito del RGPD a fattispecie che si collocano al di fuori dei confini dell'Unione, ma che presentano in ogni caso un collegamento con il suo territorio, prevedendo come criteri per determinare la sua operatività, lo stabilimento del titolare o del responsabile del trattamento nel territorio dell'Unione o l'ubicazione, sempre nell'Unione, delle persone a cui sono destinati i servizi, ma non anche delle attività di trattamento dei loro dati che potrebbero perciò avvenire all'estero[45]. Con l'impiego di un concetto affievolito di stabilimento e con il riferimento ai soggetti beneficiari della tutela si assiste a un'apertura dei confini territoriali del diritto dell'Unione, quale risultato della volontà dell'Unione stessa di tutelare su scala globale i dati personali e i diritti dei titolari.

Queste soluzioni sono dettate dall'evoluzione e dallo sviluppo delle relazioni commerciali internazionali nel contesto digitale, tanto che nel RGPD viene prevista una disciplina specifica per il trasferimento transfrontaliero dei dati e il loro successivo trattamento nel paese terzo o trasferimento da questo verso un altro paese o un'altra organizzazione internazionale, al fine di «assicurare che il livello di protezione delle persone

---

G. ROSSOLILLO, *Diritti fondamentali*, cit., spec. p. 604 e 610, secondo la quale il criterio in parola evoca l'impostazione già seguita da altri strumenti a tutela dei diritti fondamentali, nei quali non è richiesto un vincolo più intenso, quale la nazionalità o la residenza.

[40] Così C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., a p. 17, dove rileva che l'Unione «ha stabilito che a determinare l'applicabilità della legge europea non sia più il luogo in cui è stabilito il titolare del trattamento, ma il luogo in cui risiede, vive e opera l'interessato persona fisica, se fissato sul territorio dell'Unione europea».

[41] Per M.C. MENEGHETTI, «the passive personality principle (…) allows EU to regulate situations that occur beyond its borders for the purpose of protecting its nationals» (*The different shapes of extraterritoriality*, cit., p. 709 ss.).

[42] Secondo tale dottrina, l'applicazione del diritto dell'Unione si fonda sulla presenza, nel territorio dell'Unione, degli effetti che produce una determinata condotta avente luogo altrove: v. G. ROSSOLILLO, *Diritti fondamentali*, cit., p. 606 e 609; nonché M.C. MENEGHETTI, *The different shapes of extraterritoriality*, cit., p. 712 s.; D. RÜCKER, *Scope of application*, cit., p. 37; J. SCOTT, *The new EU "extraterritoriality"*, in *Comm. M. Law Rev.*, 2014, n. 5, p. 1343 ss., spec. p. 1355. Sullo sviluppo della teoria degli effetti nel settore della concorrenza, v. per tutti P. DE PASQUALE, *L'applicazione extraterritoriale dei divieti* antitrust, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*[2], Milano, 2020, p. 201 ss. In tema di protezione dei marchi, la Corte di giustizia (Grande Sezione), nella sentenza del 12 luglio 2011, causa C-324/09, *L'Oréal SA e altri* c. *eBay International AG e altri*, EU:C:2011:474, con riferimento alla direttiva 89/104 e al regolamento n. 40/94, aveva affermato che «sarebbe pregiudicata l'efficacia di tali norme qualora l'uso, in un'offerta in vendita o in una pubblicità su Internet destinata a consumatori che si trovano nell'Unione, di un segno identico o simile a un marchio registrato nell'Unione fosse sottratto all'applicazione di tali norme per il solo fatto che il terzo all'origine di detta offerta o pubblicità sia stabilito in uno Stato terzo, che il server del sito Internet da lui utilizzato si trovi in tale Stato o ancora che il prodotto oggetto di detta offerta o pubblicità si trovi in uno Stato terzo» (punto 63).

[43] Cfr. considerando 23 e *Linee guida 3/2018*, cit., p. 17.

[44] Cfr. considerando 24 e *Linee guida 3/2018*, cit., p. 21.

[45] In merito, v. anche C. SARTORETTI, *Il regolamento europeo sulla privacy*, cit., p. 15; con riferimento alla direttiva 95/46, v. G. CAGGIANO, *La Corte di giustizia*, cit., p. 25.

fisiche garantito dal presente regolamento non sia pregiudicato»[46]. A tale riguardo è intervenuta la Corte di giustizia, nella causa *Schrems II*, per rispondere alle domande poste dal giudice del rinvio in merito alla legittimità e alla conformità alla normativa europea del trasferimento dei dati dall'Unione agli Stati Uniti, basato su accordi che integrano le clausole contrattuali tipo di cui alla decisione 2010/87, e del meccanismo di mediazione, introdotto con la decisione del 2016.

3. *Il controllo della Corte di giustizia*

Il trasferimento dei dati all'estero era stato oggetto, in relazione alla direttiva 95/46 e agli atti di esecuzione fondati su di essa, della sentenza *Schrems I* del 2015, della quale la decisione *Schrems II* del 2020 rappresenta una evoluzione per una duplice considerazione: da una parte, la normativa di riferimento è cambiata, avendo ad oggetto la decisione 2016/1250 che ha sostituito la decisione 2000/520, dichiarata invalida, ed essendo entrato in vigore il RGPD; dall'altra, dalle argomentazioni della Grande Sezione emerge un controllo più effettivo e protettivo rispetto a quello svolto in *Schrems I*, per essersi, la Corte stessa, spinta fino a considerare le disposizioni materiali dell'ordinamento dello Stato terzo coinvolto.

Nella causa *Schrems II*, i dubbi sollevati dal giudice irlandese hanno riguardato il significato da attribuire al livello di protezione richiesto dall'art. 46 del RGPD, che disciplina il trasferimento di dati personali verso paesi terzi effettuato sulla base di clausole contrattuali tipo di protezione dei dati, nella specie contenute nella decisione 2010/87, nonché l'individuazione degli elementi che devono essere valutati per stabilire che il livello di protezione sia garantito[47]. Un simile trasferimento può infatti fondarsi, in base al sistema normativo delineato nel regolamento, su una decisione adottata dalla Commissione ai sensi dell'art. 45, con cui viene dichiarato che il paese terzo garantisce un livello di protezione adeguato[48], oppure, in assenza di una siffatta decisione di adeguatezza, sulla presenza, nell'ordinamento dello Stato di destinazione, di garanzie adeguate fornite dal titolare o dal responsabile del trattamento e del riconoscimento, in capo agli interessati, di diritti azionabili e mezzi di ricorso effettivi, come richiesto dall'art. 46.

In particolare, con riferimento alla constatazione di adeguatezza, i giudici del Lussemburgo hanno ripreso quanto già espresso nel caso *Schrems I*[49], laddove era stato chiarito che il livello di protezione predisposto dal paese terzo non deve essere

---

[46] Art. 44 del RGPD, cit. Il regime di cui al capo V mira, infatti, a garantire la continuità del livello elevato di tale protezione: cfr. considerando 6; sentenza *Schrems II*, punti 92-93; e Avvocato generale Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, *Schrems II*, cit., punto 117. A tal riguardo, v. anche Corte di giustizia (Grande Sezione), parere 1/15 del 26 luglio 2017, *Accordo PNR UE-Canada*, EU:C:2017:592, punto 134, dove viene chiarito che il «diritto alla protezione dei dati di carattere personale richiede, in particolare, che la continuità del livello elevato di protezione delle libertà e dei diritti fondamentali riconosciuti dal diritto dell'Unione sia garantita in caso di trasferimento di dati personali dall'Unione a un paese terzo. Anche se le misure dirette ad assicurare un siffatto livello di protezione possono essere diverse da quelle attuate all'interno dell'Unione al fine di garantire il rispetto degli obblighi risultanti dal diritto dell'Unione, tali misure devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione».

[47] Sentenza *Schrems II*, punto 90.

[48] Le decisioni di esecuzione sono state definite atti esecutivi di terzo livello dell'ordinamento dell'Unione: cfr. G. CAGGIANO, *Il bilanciamento tra diritti*, cit., p. 10.

[49] Sentenza *Schrems I*, punti 72-74.

necessariamente identico a quello garantito dall'Unione, ma, per risultare adeguato, deve essere «sostanzialmente equivalente a quello assicurato all'interno dell'Unione», ora contenuto nel RGPD, letto alla luce della Carta[50]. I diritti della Carta devono infatti essere presi in considerazione per determinare il livello di protezione[51], così come richiede lo stesso regolamento e, in particolare, come emerge dal considerando 10, che indica come obiettivo quello di protezione delle libertà e dei diritti fondamentali delle persone fisiche all'interno dell'Unione con riguardo al trattamento dei dati personali[52]. La Carta si pone quindi, al tempo stesso, come parametro di legittimità e strumento integrativo delle previsioni del RGPD.

Con il passaggio dalla necessaria adeguatezza alla sostanziale equivalenza, ma non all'identicità, dei livelli di protezione europeo e straniero si assiste all'estensione extraterritoriale degli standard europei, che diventano i criteri per accertare l'adeguatezza dell'ordinamento del paese di destinazione dei dati[53]. Una simile valutazione, tuttavia, non imporrebbe, di per sé, di condurre un'analisi comparata tra il sistema dell'Unione e quello dello Stato terzo, dovendosi avere riguardo solo agli elementi rilevanti di quest'ultimo. Diversamente, la determinazione della sostanziale equivalenza richiede di considerare i due sistemi e confrontarli per poter riconoscere il secondo simile al primo[54]. Nel regolamento non si rinviene, in effetti, la necessità di fare un confronto tra i due sistemi, venendo indicati, pur non in modo esaustivo, unicamente i fattori[55] dell'ordinamento terzo che la Commissione deve prendere in considerazione per attestare il livello di protezione al fine di stabilirne l'adeguatezza e permettere così il trasferimento dei dati. Ciononostante, come si evince dalla giurisprudenza della Corte, il risultato è che l'esame del livello di protezione viene effettuato in una prospettiva europea, alla stregua dei criteri propri dell'ordinamento dell'Unione, rendendo, in definitiva, imprescindibile la comparazione tra quest'ultimo e quello straniero.

---

[50] Sentenza *Schrems II*, punto 94, e considerando 104 del RGPD. V. anche Avvocato generale Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, *Schrems II*, cit., punto 248: «tale criterio non significa che il livello di protezione deve essere "identico" a quello richiesto nell'Unione. Pur se i mezzi ai quali ricorre un paese terzo per proteggere i diritti delle persone interessate possono differire da quelli prescritti dal RGPD, letto alla luce della Carta, "tali strumenti devono (...) rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione"».

[51] Sentenza *Schrems II*, punto 99.

[52] *Ivi*, punto 101.

[53] A tal riguardo, è stato osservato che la Corte di giustizia, con tale passaggio, ha rivendicato «il ruolo di Corte costituzionale pan europea, andando a rimarcare la necessità di un check and balance tra il potere, squisitamente politico e discrezionale della Commissione, e la sofisticata tutela dei diritti fondamentali garantita dall'Unione»: A. CRISTOFANO, *La Sentenza Schrems II e il judicial activism della Corte di Giustizia dell'Unione Europea. Verso un GDPR a vocazione universale?*, 15 febbraio 2021, reperibile al sito Internet www.medialaws.eu.

[54] La sussistenza della protezione sostanzialmente equivalente deve infatti essere valutata «non tanto alla luce di una corrispondenza formale tra i dettati normativi, quanto sulla base di un'analisi sostanziale del complesso di disposizioni adottate nell'ordinamento giuridico sottoposto a scrutinio»: così M.C. MENEGHETTI, *I trasferimenti*, cit., p. 619.

[55] Cfr. considerando 104 e art. 45 del RGPD, ai sensi dei quali, gli elementi che devono essere oggetto di valutazione da parte della Commissione per stabilire l'adeguatezza di un ordinamento extraeuropeo a divenire destinatario di dati personali, i quali devono essere «[i]n linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo», come «il modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale», nonché «criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo», a cui si aggiunge l'esistenza di un «effettivo controllo indipendente della protezione dei dati», «meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri», il riconoscimento agli interessati di «diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale».

Con la sentenza *Schrems II*, la Grande Sezione ha ritenuto quindi di dover procedere ad analizzare il sistema giuridico dello Stato terzo e determinare il suo livello di adeguatezza per poterlo considerare una destinazione sicura con garanzie adeguate. Il controllo giurisdizionale consiste in realtà in un esame indiretto dell'ordinamento statunitense, effettuato in via mediata poiché avente ad oggetto la legittimità di un atto dell'Unione, che lo richiama. Operando in tal modo, la Corte assicura in concreto, nel contesto dei rapporti internazionali, la protezione effettiva dei dati personali delle persone che si trovano nell'Unione. Diversamente, in *Schrems I*, il ragionamento della Corte era apparso più "tecnico", in quanto essa aveva dichiarato l'invalidità della decisione "approdo sicuro" basandosi essenzialmente sul dato testuale. L'attenzione era stata posta, in particolare, sulla formulazione dell'art. 1 di tale decisione, dove non veniva affermato in modo esplicito che «gli Stati Uniti "garantiscono" effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali»[56], violando così i requisiti dell'art. 25, par. 6 della direttiva 95/46[57]. In tale occasione, la Corte aveva considerato il sistema istituito con la decisione del 2000, rilevando che l'adesione ai principi ivi contenuti non era imposta alle autorità pubbliche straniere[58], permetteva la prevalenza della legge statunitense sui principi stessi[59] e consentiva così un accesso generalizzato ai dati trasferiti di fronte ad esigenze di tutela della sicurezza pubblica[60]. Per tali ragioni, la decisione in parola rendeva possibili ingerenze nei diritti fondamentali delle persone titolari dei dati[61]. Non essendovi poi «constatazioni sufficienti quanto alle misure di protezione offerte dagli Stati Uniti»[62], la Grande Sezione era giunta a dichiarare l'invalidità di tutta la decisione. In sostanza, la Commissione avrebbe dovuto verificare in concreto il rispetto dei diritti e non procedere ad un esame in astratto dello schema di "approdo sicuro"[63]. La Corte, dal canto suo, non aveva approfondito l'esame del sistema normativo americano e dei programmi di sorveglianza ivi impiegati[64], e non si era quindi espressa sull'adeguatezza del livello di protezione dallo stesso offerto[65].

Ciò è avvenuto, invece, nel caso *Schrems II*, dove alla Corte di giustizia era stato domandato se le clausole tipo di protezione contenute nella decisione del 2010 fossero idonee, da sole, a garantire un livello adeguato di protezione[66], tenuto conto che le autorità

---

56 Sentenza *Schrems I*, punto 97.
57 *Ivi*, punto 98.
58 *Ivi*, punti 80-82. Su cui v., tra i molti, B. CAROTTI, *Il caso* Schrems*, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giorn. dir. amm.*, 2016, n. 3, p. 333 ss., spec. p. 338 s.; A. PISAPIA, *La tutela*, cit., p. 111 ss.; T. KUGLER, *Practical examples*, in D. RÜCKER, T. KUGLER (eds.), *New European General Data Protection Regulation*, cit., p. 199; F. BORGIA, *Profili critici*, cit., p. 141 ss.; P. PIRODDI, *I trasferimenti di dati personali*, cit., p. 190 ss.
59 Sentenza *Schrems I*, punti 84-86.
60 *Ivi*, punti 88-89; su cui v. L. AZOULAI, M. VAN DER SLUIS, *Institutionalizing personal data protection*, cit., p. 1365; B. CAROTTI, *Il caso* Schrems, cit., p. 338 ss.; V. SALVATORE, *La Corte di giustizia*, cit., p. 633 ss.
61 Sentenza *Schrems I*, punto 87.
62 *Ivi*, punto 83.
63 *Ivi*, punto 98 ss.
64 A tal riguardo, si veda S. CRESPI, *Il trasferimento dei dati personali*, cit., a p. 713, dove, con riferimento al caso *Schrems I*, l'A., anticipando in un certo senso quanto accaduto con *Schrems II*, ha osservato che, qualora la Corte si fosse spinta «fino a sindacare il contenuto del diritto straniero, valutando se il diritto USA garantisca sufficienti garanzie alla luce dei criteri UE di proporzionalità e necessità», tale metodo interpretativo l'avrebbe esposta «a critiche di "espansione extraterritoriale"»; da ciò derivando che l'approccio adottato in *Schrems I* fosse quindi rispettoso dell'ordinamento dello Stato terzo.
65 Così X. TRACOL, *"Schrems II"*, cit., p. 7.
66 Sentenza *Schrems II*, punto 90.

pubbliche del paese di destinazione non sono da esse vincolate, in quanto le clausole sono convenute solo tra il titolare o il responsabile del trattamento, ubicato in uno Stato membro, e il destinatario del trasferimento, situato negli Stati Uniti.

Ai sensi del regolamento, in mancanza di una decisione di adeguatezza, il trasferimento transfrontaliero di dati è possibile anche quando vengono offerte "garanzie adeguate" dallo Stato di destinazione[67], che possono consistere in norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo, oppure clausole contrattuali autorizzate da una tale autorità. Tali garanzie, come enunciato nel considerando 108 del RGPD, devono «compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato» e hanno lo scopo di «assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo»[68]. Al fine di determinare il livello di protezione, occorre pertanto valutare una serie di elementi per accertare se lo Stato terzo riconosca agli interessati garanzie adeguate, diritti azionabili e mezzi di ricorso effettivi. In tale contesto, rilevano appunto le clausole contrattuali convenute tra il titolare o il responsabile del trattamento stabilito nell'Unione e il destinatario del trasferimento ubicato nel paese terzo, nonché «gli elementi rilevanti del sistema giuridico di quest'ultimo»[69], quali quelli enunciati nell'art. 45, par. 2 del RGPD in merito alla valutazione di adeguatezza.

Sebbene le clausole siano contenute in una decisione della Commissione, non è scontato che la protezione garantita tramite esse costituisca, da sola, un mezzo idoneo per assicurare la tutela effettiva dei dati trasferiti. Diversamente dalla decisione di adeguatezza, nel caso dell'adozione di clausole tipo di protezione, la Commissione non è infatti obbligata a procedere all'accertamento del livello di protezione offerto dal sistema normativo dello Stato terzo, tenuto conto che spetta alle parti contrattuali prevedere garanzie adeguate[70]. Come osservato dalla Grande Sezione, il ricorso a siffatte clausole può dunque non bastare per tutelare gli interessati da ingerenze da parte delle autorità pubbliche del paese di destinazione dei dati e, di conseguenza, tali disposizioni dovrebbero essere accompagnate da «altre clausole o garanzie supplementari»[71]. In mancanza di simili garanzie, l'autorità di controllo dello Stato membro competente è legittimata ad intervenire per sospendere o cessare il trasferimento nel caso in cui ritenga che le clausole non siano rispettate dal paese terzo e che la protezione dei dati non possa essere garantita[72]. Il potere dei garanti nazionali non è poi inficiato dalla decisione di adeguatezza della Commissione, che, pur vincolante, non ne impedisce l'esercizio[73], come del resto avvenuto nel caso di specie. Alla luce

---

67 Cfr. art. 46 del RGPD.
68 Sentenza *Schrems II*, punto 95.
69 *Ivi*, punto 104.
70 *Ivi*, punto 129 ss.; in merito v. anche i considerando 108 e 114 del RGPD.
71 Sentenza *Schrems II*, punto 125 ss. e punto 132; nonché considerando 109. In merito alle garanzie supplementari, v. Comitato europeo per la protezione dei dati, *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*, adottate il 18 giugno 2021, reperibili al sito Internet https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_it.
72 Sentenza *Schrems II*, punti 106 ss.
73 *Ivi*, punti 114 ss., 150 e 157.

dell'analisi delle clausole contenute nella decisione del 2010[74], la Corte ha precisato, infine, che non è in dubbio la sua validità, essendo in essa previsti meccanismi idonei di protezione[75].

Rimaneva pertanto da verificare l'adeguatezza della disciplina degli Stati Uniti, come paese di destinazione dei dati provenienti dall'Unione, ai sensi della decisione "scudo per la *privacy*" del 2016[76]. La questione della conformità di tale decisione al RGPD, letto alla luce della Carta[77], emergeva, in modo implicito, dalla domanda posta dal giudice del rinvio relativa al mediatore, che era stato infatti istituito in base ad essa[78]. È in tale contesto che la Grande Sezione ha esaminato la legittimità dell'atto secondario in parola, prendendo in considerazione gli elementi su cui esso si fonda, dal sistema normativo ai mezzi di tutela esistenti nello Stato terzo.

L'art. 1 della decisione 2016/1250 contiene la constatazione che gli Stati Uniti assicurano un livello adeguato di protezione dei dati trasferiti, basato sull'applicazione di principi che, contenuti nell'allegato II[79], costituiscono lo "scudo per la *privacy*". Il punto I.5 di tale allegato prevede una deroga nelle ipotesi in cui sia necessario «soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia»[80]. Ad avviso della Corte, il carattere generale di tale deroga permette però ingerenze nei diritti fondamentali dei titolari dei dati trasferiti da parte delle autorità pubbliche dello Stato terzo, che possono accedervi e, in particolare, utilizzare tali dati nell'ambito dei programmi di intelligence statunitensi[81]. In merito, viene rilevato che la stessa Commissione aveva, in effetti, valutato i suddetti sistemi di sorveglianza e, tuttavia, aveva dichiarato che le ingerenze si limitavano allo stretto necessario[82]. I giudici del Lussemburgo hanno comunque proceduto all'esame della normativa statunitense per valutare l'effettività delle garanzie offerte dai programmi in questione e per determinare se gli stessi fossero compatibili con la tutela dei diritti fondamentali determinata dal RGPD in combinato disposto con la Carta. Basti qui rilevare che le osservazioni dei giudici europei hanno riguardato la mancanza di limitazioni, in capo alle autorità straniere, all'accesso ai dati tramite i suddetti programmi, di garanzie per i cittadini stranieri titolari dei dati, di diritti azionabili dinanzi ai giudici e, infine, di rimedi esperibili per assicurare una loro tutela[83].

L'estensione del sindacato giurisdizionale della Corte del Lussemburgo ha quindi come obiettivo, su un piano pratico, quello di verificare il livello di protezione offerto dalla normativa americana, integrata nel sistema dell'Unione tramite l'atto di esecuzione adottato per garantire il trasferimento transfrontaliero dei dati. Tale controllo viene effettuato a prescindere dal fatto che le operazioni (successive al trasferimento) di trattamento, accesso o utilizzo dei dati, ritenute nel caso di specie ingerenze nei diritti delle persone, si verifichino

---

[74] *Ivi*, punto 122 ss.
[75] *Ivi*, punti 136-149. La decisione del 2010 è stata sostituita con la decisione di esecuzione (UE) 2021/914, cit., al fine di adeguarla al nuovo contesto normativo (cfr. considerando 6), con cui la Commissione ha altresì preso atto della pronuncia della Corte di giustizia in *Schrems II*, in particolare laddove specifica la portata delle clausole stesse (cfr. considerando 3) e la responsabilità dei soggetti del trattamento e del trasferimento transfrontaliero dei dati nella verifica della sussistenza di adeguate garanzie e nell'adozione di ulteriori garanzie supplementari (cfr. considerando 11 e 18 ss.).
[76] Sentenza *Schrems II*, punto 162.
[77] *Ivi*, punto 161.
[78] *Ivi*, punti 150-153.
[79] *Ivi*, punto 163.
[80] *Ivi*, punto 164.
[81] *Ivi*, punto 165.
[82] *Ivi*, punti 166-167.
[83] *Ivi*, punti 178-185.

all'estero. È il trasferimento transfrontaliero dei dati europei che rappresenta il collegamento sufficiente per permettere alla Corte di applicare allo Stato terzo i principi propri dell'ordinamento dell'Unione in tema di diritti fondamentali, perseguendo lo scopo di promozione dei propri valori e di protezione dei propri interessi, finendo per condizionare il trattamento dei dati trasferiti (nel paese terzo) all'applicazione degli standard europei[84]. La decisione di addentrarsi nel sistema americano ha tuttavia suscitato osservazioni critiche[85], vuoi per essersi la Corte sostituita alla Commissione nella verifica degli elementi indicati nel RGPD per determinare il livello di protezione, vuoi per avere essa espresso un'opinione sull'ordinamento terzo. Queste considerazioni non sono comunque condivisibili, in quanto l'approccio della Corte si rivela, in concreto, del tutto idoneo ad assicurare una tutela efficace ed effettiva dei diritti sui dati personali.

4. *La protezione dei diritti fondamentali*

L'ordinamento statunitense è stato oggetto di analisi nella sentenza *Schrems II* per determinare, da una parte, la legittimità delle interferenze da parte delle sue autorità pubbliche nei diritti delle persone titolari dei dati trasferiti e per stabilire, dall'altra, la sussistenza al suo interno di rimedi di tutela a fronte di eventuali ingerenze illegittime. Una simile analisi è stata dettata dalla necessità di verificare che anche oltreoceano, nel caso del trasferimento dei dati personali, venisse offerta una protezione dei diritti fondamentali sostanzialmente equivalente a quella dell'Unione.

Ai fini di tale valutazione, è stato osservato che il livello adeguato di protezione richiesto allo Stato terzo non va inteso nel senso che sia necessario garantire la protezione del (solo) contenuto essenziale del diritto fondamentale alla protezione dei dati personali[86]. Infatti, lo standard di protezione equivalente consisterebbe in un concetto più ampio, che comprende, oltre al contenuto dei diritti fondamentali, anche i rimedi previsti per la loro tutela. È a tal riguardo che si riscontra un'estensione del diritto dell'Unione al di fuori dei suoi confini, poiché ai diritti fondamentali viene implicitamente riconosciuto un effetto extraterritoriale[87], quale conseguenza dell'apertura del RGPD ad attività condotte al di fuori dei confini dell'Unione, che divengono oggetto del sindacato della Corte di giustizia chiamata ad interpretare la validità dell'atto europeo posto a fondamento del trasferimento transfrontaliero dei dati.

---

84 C. KUNER, *The Internet*, cit., p. 125.

85 In realtà, la Corte, invalidando la decisione "scudo per la *privacy*", chiude definitivamente il dibattito che era sorto già all'epoca dell'adozione della decisione in parola: v. Gruppo di lavoro Articolo 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, WP 238, 13 aprile 2016; *Annual Joint Review* del 28 novembre 2017 e del 22 gennaio 2019; Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la *privacy* (2018/2645(RSP)); nonché Comitato europeo per la protezione dei dati, *Dichiarazione in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland e Maximillian Schrems*, adottata il 17 luglio 2020. Sul punto, v. G. FORMICI, *Schrems*, cit., p. 322 ss.; S. SICA, V. D'ANTONIO, *Verso il* Privacy Shield: *il tramonto dei* Safe Harbour Privacy Principles, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali*, cit., p. 137ss.

86 In tal senso, v. M. BRKAN, *The Essence*, cit., p. 882.

87 In merito all'efficacia extraterritoriale della Carta, v. N. LAZZERINI, *La Carta*, cit., p. 174 ss., dove l'A. fa riferimento all'applicazione extraterritoriale della Carta «nei casi in cui la regola di diritto dell'Unione applicabile alla fattispecie produce effetti al di fuori del territorio degli Stati membri» (p. 175).

Con riguardo alle attività effettuate da parte delle autorità pubbliche americane aventi ad oggetto i dati di provenienza europea, a cui già si è fatto riferimento, nella sentenza *Schrems II* è stato accertato che la deroga contenuta nell'allegato II rende possibili eccezioni ai principi dello "scudo per la *privacy*" e che i programmi di sorveglianza statunitensi permettono quindi l'accesso e l'utilizzo dei dati e delle informazioni trasferite dall'Unione. Tenuto conto che tali trattamenti, «indipendentemente dall'uso ulteriore delle informazioni» e dal fatto se «gli interessati abbiano o meno subito eventuali inconvenienti»[88], interferiscono nei diritti fondamentali delle persone al rispetto della loro vita privata e dei loro dati personali, ne consegue che le attività delle autorità dello Stato terzo devono essere vagliate alla luce degli artt. 7 e 8 della Carta[89].

La Corte di giustizia ha perciò fatto riferimento all'art. 52 della Carta per determinare se le suddette ingerenze violassero o meno i principi di necessità e proporzionalità[90], senza ritenere necessario verificare anche il rispetto delle «condizioni sostanzialmente equivalenti a quelle previste dall'art. 52, par. 1, prima frase», vale a dire del contenuto essenziale dei diritti fondamentali[91]. Sotto quest'ultimo profilo, la sentenza *Schrems II* si differenzia dalla precedente *Schrems I*, dove la Grande Sezione aveva dichiarato la violazione del contenuto essenziale[92] del diritto alla vita privata di cui all'art. 7 della Carta, in quanto, in base alla normativa americana di attuazione dell'accordo sull'"approdo sicuro", le autorità pubbliche potevano accedere in maniera generalizzata alle informazioni e ai dati personali trasferiti[93]. In tal caso, la Corte non aveva dovuto effettuare il test della proporzionalità, ponendo a confronto il diritto alla *privacy* con un interesse non appartenente all'Unione, quale era la sicurezza pubblica degli Stati Uniti[94], trattandosi di un accesso generalizzato, di per sé lesivo dell'essenza dei diritti fondamentali in gioco[95]. Di conseguenza, non si era reso neppure

---

88 Sentenza *Schrems II*, punto 171.

89 *Ivi*, punto 170.

90 *Ivi*, punti 174 e 179 ss.

91 *Ivi*, punto 178.

92 «L'essenza dei diritti fondamentali è compromessa quando le eventuali restrizioni «rimettono in discussione quei diritti in quanto tali» (nella versione inglese «That limitation does not call into question the principle as such»): si vedano, a titolo esemplificativo, le sentenze della Corte di giustizia del 29 aprile 2015, causa C-528/13, *Geoffrey Léger* c. *Ministre des Affaires sociales, de la Santé et des Droits des femmes et Établissement français du sang*, EU:C:2015:288, punto 54; e del 5 luglio 2017, causa C-190/16, *Werner Fries* c. *Lufthansa CityLine GmbH*, EU:C:2017:513, punto 38. Sulla nozione di "essenza dei diritti", v., per tutti, G. CAGGIANO, *Sul trasferimento*, cit., p. 574 s.

93 Sentenza *Schrems I*, punto 94.

94 Così M. BRKAN, *The Essence*, cit., p. 875.

95 Sulla salvaguardia della sicurezza nazionale, invocata come motivo di deroga nell'ambito della 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 (in *GUCE*, L 201 del 31 luglio 2002, p. 37 ss.), si vedano, in tema di trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence, Corte di giustizia (Grande Sezione), sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International* c. *Secretary of State for Foreign and Commonwealth Affairs e a.*, EU:C:2020:790, punto 50 ss.; in tema di conservazione preventiva dei dati relativi al traffico e dei dati relativi all'ubicazione, Corte di giustizia (Grande Sezione), sentenza del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.* c. *Premier ministre e a.*, EU:C:2020:791, spec. punto 134 ss.; nonché, sulla conservazione generalizzata e indifferenziata dei dati per finalità di indagine e lotta alla criminalità in generale, Corte di giustizia (Grande Sezione), sentenza del 2 marzo 2021, causa C-746/18, *procedimento penale a carico di H.K.*, EU:C:2021:152. Sull'invalidità della 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, per l'ingerenza "di vasta portata e di particolare gravità"

necessario esaminare i principi dell'"approdo sicuro"[96]. Nella sentenza *Schrems II*, invece, i programmi di sorveglianza statunitensi sono stati valutati alla luce del rispetto del principio di proporzionalità. A tal riguardo, la Corte ha riconosciuto la mancanza del rispetto dei requisiti minimi imposti dall'art. 52, par. 1, seconda frase, della Carta, in quanto i suddetti programmi non limitavano gli accessi ai dati allo stretto necessario, né li sottoponevano a un qualsivoglia controllo giudiziario[97].

Quanto all'altra questione sollevata dal giudice irlandese relativa ai rimedi di tutela offerti, dallo Stato terzo, ai soggetti interessati e, nello specifico, all'istituzione del mediatore, la Grande Sezione ha ricordato che la sussistenza di strumenti efficaci di protezione dei diritti, e quindi di un controllo giurisdizionale indipendente, costituisce una condizione essenziale per garantire lo Stato di diritto[98]. Ciò comporta che non è giustificabile alcuna misura che interferisca con l'essenza dei diritti fondamentali, nemmeno quando essa sia basata su motivi di sicurezza pubblica[99]. Diverso sarebbe il caso in cui, come in *Schrems II*, le attività non compromettano il contenuto essenziale dei diritti, ma, non incontrando limiti, possano comunque interferire nell'esercizio dei diritti fondamentali violando il principio di proporzionalità[100].

Nell'esame del sistema di ricorsi previsto dall'ordinamento statunitense, la Corte di giustizia ha applicato i criteri propri dell'Unione in tema di tutela giurisdizionale effettiva, ai sensi dell'art. 47 della Carta, per verificarne la compatibilità con il diritto dell'Unione stessa. Ne deriva che il diritto di cui all'art. 47 deve, in sostanza, trovare applicazione anche al di fuori del territorio dell'Unione, con riferimento, in generale, all'esistenza di mezzi di protezione e, in particolare, ai requisiti di effettività ed efficacia che tali rimedi devono possedere. Sotto quest'ultimo aspetto, il giudice del rinvio interrogava la Corte di giustizia in merito alla effettività del meccanismo di mediazione, istituito dalle autorità americane e indicato dalla Commissione nella decisione "scudo per la *privacy*" come elemento atto a determinare l'adeguatezza del livello di protezione degli Stati Uniti[101]. Dalla pronuncia della Corte emerge invece che non risulta assicurata l'indipendenza del mediatore, data la

---

nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, non essendo limitata allo stretto necessario, v. Corte di giustizia (Grande Sezione), sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, EU:C:2014:238. Per alcuni commenti sulla sicurezza nazionale come giustificazione dell'ingerenza nei diritti fondamentali, v. G. CAGGIANO, *La Corte di giustizia*, cit., p. 16 ss.; S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *Eur. Law Rev.*, 2018, n. 5, p. 669 ss.; C. KUNER, *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15*, EU-Canada PNR, in *Comm. M. Law Rev.*, 2018, n. 55, p. 857 ss.; O. TAMBOU, *Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights*, in *Eur. For. Aff. Rev.*, 2018, n. 2, p. 187 ss.

[96] Sentenza *Schrems I*, punto 98; su cui v. L. AZOULAI, M. VAN DER SLUIS, *Institutionalizing personal data protection*, cit., p. 1366.

[97] Sentenza *Schrems II*, punto 178 ss.

[98] *Ivi*, punti 186-189, spec. punto 187; e sentenza *Schrems I*, punto 95. In merito, v. G. CAGGIANO, *La Corte di giustizia*, cit., p. 20 s.; ID., *Il bilanciamento tra diritti*, cit., p. 10; nonché K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *Germ. Law Jour.*, 2019, n. 20, p. 779 ss., spec. p. 782 ss.; M. BRKAN, *The Essence*, cit., p. 864 ss.; T. OJANEN, *Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter*, in *Eur. Const. Law Rev.*, 2016, n. 12, p. 318 ss., spec. p. 327.

[99] Su cui, v. K. LENAERTS, *Limits on Limitations*, cit., p. 783 ss.

[100] *Ivi*, a p. 784, dove l'A. suggerisce, al fine di determinare la violazione di un diritto, di verificare "the intensity" e "the extent of the limitation", e p. 786 ss. sul rapporto tra essenza dei diritti e test di proporzionalità; nonché v. G. CAGGIANO, *La Corte di giustizia*, cit., p. 16 ss.

[101] Sentenza *Schrems II*, punto 190 ss.

mancanza di qualsiasi indicazione circa le garanzie previste nelle ipotesi della sua revoca e dell'annullamento della sua nomina, nonché per il fatto che allo stesso non sarebbe riconosciuto il potere di adottare decisioni vincolanti nei confronti dei servizi dell'intelligence[102]. Pertanto, la mediazione «non fornisce mezzi di ricorso dinanzi a un organo che offra alle persone i cui dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'art. 47 della Carta»[103]. Ne consegue che gli strumenti processuali dello Stato terzo, integrati nel sistema dell'Unione tramite la decisione di adeguatezza, devono anch'essi rispettare i criteri di cui all'art. 47. In altri termini, ai paesi terzi viene imposto, implicitamente, un obbligo di disporre di mezzi di tutela giurisdizionale effettiva per poter sviluppare interessi commerciali con l'Unione tramite la circolazione dei dati personali. Ciò riflette, sul piano esterno, il medesimo obbligo stabilito dal diritto primario dell'Unione in capo agli Stati membri, pur godendo essi di un'autonomia procedurale[104].

Alla luce delle considerazioni esposte, la Grande Sezione ha concluso che la Commissione, nel constatare che gli Stati Uniti assicurano un livello adeguato di protezione, ha disatteso quanto previsto dal RGPD, in particolare dall'art. 45 in combinato disposto con gli artt. 7, 8 e 47 della Carta[105]. L'art. 1 della decisione "scudo per la *privacy*" è dunque incompatibile con il diritto dell'Unione e, stante la sua inscindibilità con gli altri articoli della decisione stessa, «la sua invalidità ha l'effetto di inficiare la validità di tale decisione nel suo complesso»[106].

5. *Il ruolo dei garanti nazionali*

A seguito della pronuncia della Grande Sezione nella causa *Schrems II*, il *Data Protection Commissioner* irlandese ha adottato nei confronti di Facebook una decisione provvisoria (*preliminary draft decision*)[107] con cui ha annunciato l'avvio di ulteriori indagini, nonché espresso l'intenzione (*preliminary view*) di sospendere il trasferimento dei dati dall'Unione agli Stati Uniti[108], prendendo atto delle conclusioni cui sono pervenuti i giudici europei in merito all'inadeguatezza del sistema giuridico del paese di destinazione per la mancanza di mezzi effettivi di tutela. Da parte sua, Facebook ha presentato una richiesta di *judicial review* della

---

[102] *Ivi*, punti 194-196.
[103] *Ivi*, punto 197.
[104] In tal senso, v. anche P. PIRODDI, *I trasferimenti di dati personali*, cit., a p. 191, dove l'A., in relazione alla sentenza *Schrems I*, afferma che una protezione effettiva ed equivalente a quella assicurata dall'Unione europea corrisponde a «una protezione sostanzialmente identica a quella esistente nell'Unione europea» e che l'espressione ricorda «l'endiadi "effettività ed equivalenza di tutela"» usata dalla Corte «per limitare l'autonomia procedurale degli Stati membri nella predisposizione della tutela di diritti spettanti ai singoli in forza del diritto dell'Unione»; nella sentenza *Schrems I*, «questi principi sono applicati dalla Corte nei confronti di Stati terzi rispetto all'Unione». In generale sull'autonomia procedurale degli Stati membri, v., per tutti, C. PERARO, *Diritti fondamentali sociali e tutela collettiva nell'Unione europea*, Napoli, 2020, p. 223 ss. e 233 ss.
[105] Sentenza *Schrems II*, punto 198.
[106] *Ivi*, punto 199 s.
[107] La notizia è comparsa sul Wall Street Journal il 9 settembre 2020 (www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980). Cfr. anche The High Court, Judicial review, judgment of Mr. Justice David Barniville delivered on the 14th day of May, 2021, *Facebook Ireland Limited* v *Data Protection Commission* (in seguito "decisione della *High Court*"), spec. punti 2 e 39 ss., reperibile al sito Internet www.courts.ie/judgments.
[108] Su cui v. decisione della *High Court*, punto 52 ss e spec. punto 69.

suddetta decisione davanti all'Alta Corte irlandese[109], che ha però respinto i motivi di impugnazione sostenendo la legittimità dell'azione del *Data Protection Commissioner*[110].

Per quanto qui rileva, il garante irlandese, promuovendo una procedura investigativa in merito al trasferimento dei dati da parte di Facebook, dall'Unione verso gli Stati Uniti, ha esercitato i suoi poteri e agito in linea con le argomentazioni della Corte di giustizia, laddove essa ha osservato che il trasferimento dei dati verso un paese terzo, fondato su clausole contrattuali o su una decisione di adeguatezza, può essere oggetto di reclamo e quindi di indagine da parte dell'autorità di controllo competente, la quale può anche proporre un ricorso davanti ai giudici nazionali affinché procedano ad un rinvio pregiudiziale di validità dell'atto alla base del trasferimento stesso[111]. Infatti, come ha chiarito la Corte, sebbene la decisione di adeguatezza sia un atto vincolante[112], alle autorità di controllo non può essere impedito l'esercizio delle competenze e dei poteri previsti dal regolamento[113], vale a dire di esaminare eventuali reclami sollevati da individui circa il trasferimento dei loro dati all'estero e di agire in via giudiziale qualora ritengano fondate le doglianze[114]. Rimane invece irrisolta la questione se l'autorità irlandese potesse adottare un simile ordine di sospensione del trasferimento transfrontaliero dei dati anche nel caso in cui la decisione di adeguatezza non fosse stata dichiarata invalida[115]. La risposta all'interrogativo è negativa, in quanto tale provvedimento non troverebbe un'idonea base giuridica, dovendo piuttosto, come ha fatto l'autorità irlandese nella causa *Schrems II*, essere intrapresa un'azione giudiziale volta a far valere i dubbi di conformità del trasferimento extraeuropeo dei dati alla normativa dell'Unione davanti al giudice nazionale, che, a sua volta, potrebbe rimettere le eventuali questioni pregiudiziali alla Corte di giustizia.

Nel caso di specie, la competenza e i poteri del garante irlandese, con riguardo al trasferimento transfrontaliero dei dati, derivano dal fatto che esso è l'autorità di controllo

---

109 Si veda la notizia sul sito Internet www.irishtimes.com/business/media-and-marketing/high-court-to-decide-on-facebook-s-data-commissioner-challenge-as-soon-as-possible-1.4457397; nonché la decisione della *High Court*, punti 4 e 87 ss.

110 Decisione della *High Court* (v. punto 430 ss. per un sommario delle conclusioni).

111 Sentenza *Schrems II*, punti 106 ss. e 156. Si tratta quindi di un "sistema decentrato di verifica dell'adeguatezza": M. NINO, *La sentenza Schrems II*, cit., p. 748. Analogamente, già nella sentenza *Schrems I*, la Corte di giustizia aveva rilevato che la Commissione, nell'esercizio delle sue prerogative, non può limitare i poteri delle autorità nazionali, previsti dalla direttiva 95/46, qualora vi siano elementi idonei a rimettere in discussione la decisione di adeguatezza: per un commento, v. A. BARLETTA, *La tutela effettiva della* privacy *nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di* Internet, in *Eur. dir. priv.*, 2017, n. 4, p. 1179 ss., spec. p. 1204 ss.

112 Sentenza *Schrems II*, punto 155.

113 *Ivi*, punto 119; e cfr. artt. 57 e 58 del RGPD.

114 Sentenza *Schrems II*, punti 157 ss.

115 La questione è stata sollevata davanti all'Alta Corte irlandese nell'ambito del procedimento promosso da Facebook avverso l'ordine di sospensione, come emerge dalla lettera datata 9 febbraio 2021 trasmessa dall'autorità di controllo irlandese al presidente della Commissione LIBE del Parlamento europeo, parte di uno scambio di corrispondenza avviato dallo stesso garante irlandese a seguito della pubblicazione di due proposte di risoluzione concernenti l'attuazione del RGPD [Risoluzione del Parlamento europeo sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP), adottata il 25 marzo 2021, P9_TA(2021)0111, reperibile al sito Internet www.europarl.europa.eu/doceo/document/TA-9-2021-0111_IT.html] e la sentenza *Schrems II* [Risoluzione del Parlamento europeo sulla sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020 – Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems ("Schrems II") – Causa C-311/18 (2020/2789(RSP), adottata il 20 maggio 2021, P9_TA(2021)0256, reperibile al sito Internet www.europarl.europa.eu/doceo/document/TA-9-2021-0256_IT.html]. La corrispondenza è stata pubblicata dal *Data Protection Commissioner* sul sito Internet www.dataprotection.ie/en/news-media/latest-news/dpc-correspondence-libe-committee.

capofila ai sensi dell'art. 56, par. 1, del RGPD, posto che in Irlanda si trova lo stabilimento principale della succursale europea di Facebook. Nelle situazioni che implicano la circolazione extraeuropea dei dati, il regolamento prevede infatti una distribuzione di competenze e di poteri tra le autorità degli Stati membri, con una conseguente responsabilizzazione dell'autorità capofila, e specifiche procedure di coordinamento, ritenute idonee al perseguimento degli obiettivi di tutela dei diritti delle persone. In particolare, la stessa autorità capofila deve coordinarsi con le altre autorità di controllo nazionali[116], avvalendosi, come disposto dall'art. 60 ss. del RGPD, dei meccanismi di cooperazione (c.d. sportello unico[117]) o di coerenza, in cui sono coinvolti anche la Commissione e il Comitato europeo per la protezione dei dati, al fine di assicurare un'applicazione uniforme del regolamento stesso. Nelle ipotesi in cui un eventuale reclamo riguardi più Stati membri, spetterà all'autorità capofila adottare un progetto di decisione, che diventerà vincolante per tutti i garanti nazionali, qualora essi non sollevino obiezioni[118], ferma restando la possibilità per gli stessi di adottare provvedimenti d'urgenza provvisori in presenza di circostanze eccezionali[119], nonché di gestire i reclami quando l'oggetto riguardi unicamente uno stabilimento sito nel rispettivo Stato membro o incida in modo sostanziale sugli interessati che si trovano in tale Stato e la capofila decida di non trattare il caso[120].

Il coordinamento delle competenze e dei poteri delle autorità nazionali interessate e dell'autorità capofila è stato oggetto del rinvio pregiudiziale nella causa *Facebook Ireland e a.*[121], presentato nell'ambito di un procedimento avviato dall'autorità belga per la protezione dei dati, che si era rivolta al tribunale nazionale chiedendo un'ingiunzione nei confronti di Facebook Belgium per far cessare le attività di raccolta e utilizzazione illecita di informazioni sul comportamento di navigazione privata degli utenti di Internet in Belgio. La decisione del giudice di primo grado di accoglimento dell'istanza era stata impugnata dalla società resistente davanti alla Corte d'appello di Bruxelles, la quale aveva sospeso il procedimento, tenendo conto, in particolare, delle eccezioni sollevate in merito alla competenza del garante belga a proseguire il giudizio, non essendo questa, bensì quella irlandese, l'autorità di controllo capofila, trovandosi, come già osservato, in Irlanda lo stabilimento principale del titolare del trattamento (Facebook Ireland).

La Grande Sezione della Corte di giustizia, con la sentenza del 15 giugno 2021, ha confermato che le autorità di controllo, diverse dalla capofila, possono intentare un'azione davanti al giudice nazionale nei casi di trattamento transfrontaliero dei dati, purché siano rispettate le disposizioni del RGPD sull'attribuzione delle competenze e sulle procedure di cooperazione e di coerenza. Nello specifico, i giudici del Lussemburgo, così come l'Avvocato generale Bobek nelle sue conclusioni[122], hanno riconosciuto, alla luce delle norme del

---

116 In merito, v., per tutti, A. BARLETTA, *La tutela*, cit., p. 1200 ss. Con riferimento alla direttiva 95/46, sulla delimitazione territoriale dei poteri delle autorità nazionali di controllo, esercitabili solo contro le violazioni avvenute all'interno del proprio territorio, dovendo in tutti gli altri casi chiedere l'intervento delle autorità degli altri Stati membri, v. Corte di giustizia, sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo s.r.o.* c. *Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639, punto 42 ss.

117 Considerando 127 del RGPD.

118 Art. 60 del RGPD.

119 Art. 66 del RGPD.

120 Cfr. art. 56, parr. 2-3 e 5, del RGPD.

121 Corte di giustizia (Grande Sezione), sentenza del 15 giugno 2021, causa C-645/19, *Facebook Ireland Ltd., Facebook Inc., Facebook Belgium BVBA* c. *Gegevensbeschermingsautoriteit*, EU:C:2021:483.

122 Avvocato generale Bobek, conclusioni del 13 gennaio 2021, causa C-645/19, *Facebook Ireland e a.*, EU:C:2021:5, spec. punto 129 ss.

regolamento relative al meccanismo dello "sportello unico", la competenza decisionale dell'autorità capofila, quale "unico interlocutore"[123] del titolare o del responsabile del trattamento il cui stabilimento principale è ubicato nel rispettivo Stato membro, nei casi riguardanti il trattamento transfrontaliero dei dati[124]. Non è comunque esclusa, qualora ricorrano i presupposti di cui all'art. 56 del RGPD, la possibilità per gli altri garanti nazionali di gestire reclami e di adottare una decisione d'urgenza o misure provvisorie[125], nonché, ai sensi dell'art. 58, par. 5, del RGPD, di adire un giudice nel proprio Stato in caso di presunta violazione del regolamento stesso[126].

Ad avviso della Corte, poi, tale potere delle autorità di controllo di intentare un'azione giudiziale esercitabile «solo nel rispetto delle norme sulla ripartizione delle competenze decisionali» di cui agli artt. 55 e 56, in combinato disposto con l'art. 60, del RGPD, è conforme ai diritti fondamentali di cui agli artt. 7, 8 e 47 della Carta, in quanto rimane in capo a ciascuna di esse la responsabilità di «contribuire ad un livello elevato di protezione di detti diritti»[127], divenendo così essenziale lo strumento del ricorso in giudizio per dare seguito alle eventuali violazioni lamentate[128]. In tal modo verrebbe assicurato, in ogni Stato membro, un uguale livello di attuazione del regolamento e di conseguente protezione dei diritti, impedendo «una pratica di *forum shopping*, in particolare da parte dei titolari del trattamento»[129], i quali sarebbero altrimenti indotti a compiere attività potenzialmente lesive dei diritti in quelle giurisdizioni in cui alle autorità non è permesso ricorrere in giudizio.

L'esercizio delle competenze di cui all'art. 58, par. 5, non è inoltre subordinato alla condizione che sia presente, nel territorio dell'autorità di controllo, uno stabilimento del titolare o del responsabile del trattamento, poiché la norma è «formulata in termini generali»[130]. È infatti solo necessario che il trattamento rientri nell'ambito di applicazione territoriale del regolamento ai sensi dell'art. 3[131]. Alla stessa stregua, l'azione giudiziaria può essere promossa nei confronti di qualsiasi stabilimento, diverso da quello principale, che si trovi nello Stato membro di appartenenza del garante nazionale interessato, qualora tale azione riguardi un trattamento dei dati effettuato «nell'ambito delle attività di detto stabilimento» ai sensi dell'art. 3, par. 1, del RGPD[132]. Sul punto, l'Avvocato generale aveva sostenuto che l'azione giudiziale di un garante locale può essere promossa anche nei confronti di titolari o responsabili del trattamento situati altrove nell'Unione europea. L'indicazione "territorio del rispettivo Stato membro", contenuta nell'art. 55 del RGPD, che, letto in combinato disposto con le norme sull'ambito di applicazione territoriale, delimita la competenza delle autorità nazionali, va infatti intesa come riferita agli "effetti del trattamento dei dati nel territorio di uno Stato membro", non fungendo quindi da limite alle azioni dei garanti stessi[133].

Le autorità degli Stati membri possono poi fondare le loro azioni sulla stessa disposizione di cui all'art. 58, par. 5, del RGPD, tenuto conto che, come chiarito dalla Corte,

123 Sentenza *Facebook Ireland e a.*, punto 63; e cfr. art. 56, par. 6, del RGPD.
124 Sentenza *Facebook Ireland e a.*, punto 56.
125 *Ivi*, punto 57 ss.
126 *Ivi*, punto 65.
127 *Ivi*, punto 66 ss.
128 *Ivi*, punto 71.
129 *Ivi*, punto 68.
130 *Ivi*, punto 88; nonché Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 150.
131 Sentenza *Facebook Ireland e a.*, punto 76 ss.
132 *Ivi*, punto 85 ss.; v. anche Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 141 ss.
133 Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 152.

la norma possiede efficacia diretta, in quanto è inclusa in un regolamento e contiene un precetto specifico e immediatamente applicabile, in base alla quale alle autorità di controllo è riconosciuta la legittimazione ad agire nei confronti di privati davanti ai giudici nazionali, non essendo pertanto necessaria una normativa statale di attuazione[134].

Era stata sollevata, infine, una questione relativa al coordinamento tra diversi procedimenti promossi da varie autorità di controllo in merito ad analoghe attività di trattamento transfrontaliero e all'efficacia del provvedimento giurisdizionale, adottato all'esito di uno di questi giudizi, nei confronti dell'autorità capofila[135]. La Grande Sezione ha ritenuto che tale questione non fosse ricevibile perché non connessa al procedimento principale, non essendo state presentate circostanze che dimostrassero la sussistenza di procedimenti paralleli, e riguardante quindi un problema ipotetico[136]. L'Avvocato generale, da parte sua, aveva osservato che non occorreva fornire una risposta[137], sostenendo che la necessità di operare secondo il RGPD, vale a dire in base ai meccanismi obbligatori ivi previsti, quale lo sportello unico, eviterebbe, di fatto, il verificarsi di conflitti di giurisdizione e di problemi di coordinamento. Infatti, qualora si ammettesse la possibilità per qualsiasi autorità di controllo di ottenere una sentenza definitiva nella propria giurisdizione, che vincolerebbe tutte le autorità garanti degli Stati membri, si rischierebbe di permettere una "corsa alla prima sentenza"[138] in violazione delle disposizioni del regolamento.

In sostanza, dalla sentenza della Grande Sezione emerge che le autorità nazionali e la capofila devono esercitare le loro competenze secondo le disposizioni del RGPD e nel rispetto di una "leale ed efficace cooperazione"[139]. Risulta quindi una funzione essenziale delle autorità di controllo nel garantire una piena e coerente applicazione del regolamento, avendo esse il compito di svolgere la valutazione in concreto delle attività di trattamento dei dati e, di conseguenza, di assicurare la protezione effettiva dei diritti delle persone, non solo quando tali attività si verificano nel rispettivo Stato membro, ma soprattutto nel contesto del trasferimento transfrontaliero dei dati. Spetta in ogni caso al giudice nazionale accertare il rispetto, da parte del garante nell'esercizio dei suoi poteri, delle disposizioni del RGPD relative alle competenze delle autorità di controllo e alle procedure[140]. Nel caso *Facebook Ireland e a.*, all'autorità belga potrà quindi essere riconosciuta la possibilità di proseguire il giudizio, e ottenere così una inibitoria, solo qualora venga accertato che la stessa abbia intrapreso le azioni necessarie previste nell'ambito del meccanismo dello "sportello unico".

Va rilevato che criticità in relazione all'attuazione del regolamento da parte delle autorità nazionali e alla durata delle indagini condotte da alcune di esse, specialmente da quella irlandese, sono state evidenziate dal Parlamento europeo nella risoluzione relativa alla

134 Sentenza *Facebook Ireland e a.*, punto 106 ss.; Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 163 ss.
135 Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 169 ss.
136 Sentenza *Facebook Ireland e a.*, punto 114 ss.
137 Avvocato generale Bobek, conclusioni del 13 gennaio 2021, cit., punto 170.
138 *Ivi*, punto 171.
139 Sentenza *Facebook Ireland e a.*, punti 53, 60, 63 e 72.
140 *Ivi*, punto 73.

sentenza *Schrems II*[141] e nella risoluzione sull'attuazione del RGPD[142], con cui ha invitato tutti i soggetti coinvolti a una maggiore uniformità nell'applicazione della normativa in linea con le pronunce della Corte di giustizia e le indicazioni del Comitato europeo per la protezione dei dati[143]. Sta di fatto che i meccanismi obbligatori di *public enforcement*, combinando azioni decentralizzate con il ruolo centrale della capofila, rispondono alle esigenze e agli obiettivi delineati nel regolamento stesso, fermo restando il potere dei garanti, nel rispetto delle disposizioni del RGPD, di instaurare azioni giudiziali, negli Stati membri interessati, in presenza di dubbi di conformità. Lo strumento più efficace per la tutela effettiva dei diritti delle persone con riguardo ai dati personali è quindi affidato ai giudici nazionali e, in definitiva, alla Corte di giustizia, che assume così il ruolo di vero "scudo per l'Europa".

6. *Considerazioni conclusive*

La disciplina del trasferimento dei dati dall'Unione verso Stati terzi risulta significativa sotto un duplice profilo: da una parte, per la dimostrazione dell'evoluzione normativa europea, introducendo elementi che permettono una apertura extraterritoriale del suo ambito di applicazione, adeguandosi in tal modo il diritto dell'Unione al contesto digitale di riferimento; e, dall'altra, per la conseguente applicazione dei principi propri dell'ordinamento europeo allo Stato terzo di destinazione dei dati quando si tratta di accertare il rispetto dei diritti fondamentali coinvolti, che assumono dunque essi stessi una valenza extraterritoriale, richiedendo che tale Stato si adegui adottando standard essenzialmente equivalenti.

Spetta in ogni caso ai garanti per la protezione dei dati degli Stati membri, nell'esercizio dei poteri loro conferiti, operare in concreto le valutazioni in merito alla legittimità dei trattamenti dei dati, ivi compreso il loro trasferimento e trattamento transfrontaliero, e, in tale ipotesi, collaborare con l'autorità di controllo capofila. Rimane salva la possibilità, per gli stessi garanti, di sollevare i dubbi di legittimità davanti, prima, ai giudici nazionali e, poi, alla Corte di giustizia. Si assiste così a un modello di protezione, nel caso specifico del trasferimento dei dati all'estero, che, governato dai principi di leale cooperazione e assistenza reciproca, si basa in realtà su un doppio sistema decentrato, uno tra le autorità nazionali e l'autorità capofila e l'altro tra i giudici nazionali e i giudici del Lussemburgo.

In conclusione, a tre anni dall'applicazione del regolamento e alla luce della giurisprudenza dei giudici del Lussemburgo, pur emergendo la necessità di assicurare un'attuazione uniforme in tutti gli Stati membri del RGPD[144], i rimedi in esso delineati

[141] Risoluzione 2020/2789(RSP), cit., punti 4-5. Il Parlamento europeo ha anche invitato la Commissione ad avviare una procedura d'infrazione contro l'Irlanda «per non aver applicato correttamente il RGPD» (spec. punto 4). La gestione dei reclami da parte del garante irlandese è poi oggetto di una interrogazione parlamentare del 14 maggio 2021, E-002629/2021 (reperibile al sito Internet www.europarl.europa.eu/doceo/document/E-9-2021-002629_IT.html).

[142] Risoluzione 2020/2717(RSP), cit., punti 12 ss. e 20.

[143] *Ivi*, punto 28 ss.

[144] In merito, si veda anche la Comunicazione COM(2020)264 final, cit., p. 6 ss.

rispondono alle esigenze di protezione dei diritti delle persone nel contesto della circolazione internazionale dei dati[145].

[145] Il quadro così descritto, tuttavia, deve coordinarsi anche con la normativa dedicata alla tutela del consumatore, restando ferma, in merito, la competenza delle autorità nazionali antitrust. Si potrebbero così verificare possibili sovrapposizioni con i garanti della *privacy* quando l'intervento delle autorità antitrust ha ad oggetto i dati personali. La questione è stata sollevata dalle società Facebook Inc e Facebook Ireland Ltd in sede di ricorso avverso il provvedimento del 29 novembre 2018 dell'Autorità garante della concorrenza e del mercato italiana (AGCM) che le condannava per pratiche commerciali scorrette per non aver fornito informazioni adeguate agli utenti della piattaforma sull'attività di raccolta e utilizzo, a fini commerciali, dei loro dati (procedimento istruttorio PS/11112). Le ricorrenti avevano chiesto l'annullamento di tale provvedimento basandosi, tra l'altro, sulla mancanza di competenza in capo all'AGCM, poiché, a loro avviso, la questione riguardava il diritto fondamentale al rispetto dei dati personali e trovavano pertanto applicazione la normativa speciale contenuta nel RGPD, nonché, in particolare, l'art. 56 sulla competenza esclusiva, in materia di trattamento transfrontaliero dei dati, dell'autorità capofila irlandese, essendo ubicato in Irlanda lo stabilimento principale di Facebook. Sia il TAR del Lazio, con sentenza del 10 gennaio 2020, n. 261, sia il Consiglio di Stato, con sentenza del 29 marzo 2021, n. 2631, non hanno affrontato nello specifico tale profilo, essendo stato assorbito dalla determinazione del tema della commerciabilità dei dati personali e, di conseguenza, della possibile coesistenza delle due discipline, che, secondo i giudici, presentano ambiti operativi differenti e non contrastanti. Il tema è oggetto anche di un rinvio pregiudiziale alla Corte di giustizia (causa C-252/21, *Facebook e a.*) presentato dal Tribunale regionale superiore di Düsseldorf nell'ambito di una controversia tra il *Bundeskartellamt* (l'autorità antitrust tedesca) e Facebook, relativa all'abuso di posizione dominante sul mercato per raccogliere i dati delle persone. Su tale notizia, v. i siti Internet www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20210324_-PM_Facebook2/index.php e http://competitionlawblog.kluwercompetitionlaw.com/2021/04/02/of-pricing-guns-social-networks-and-gdpr-the-dusseldorf-higher-regional-courts-submits-facebook-case-to-the-cjeu/. Sulla vicenda, in generale, v. A. DAVOLA, *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in *Diritto di Internet*, 2021, n. 1, p. 61 ss. Per alcune considerazioni in merito a tutela della *privacy* e concorrenza, v. R. CAFARI PANICO, *L'identità digitale quale diritto del cittadino dell'Unione, fra tutela della* privacy *e concorrenza*, in *Papers di diritto europeo*, 2019, n. 2, p. 7 ss., spec. p. 15 ss.