IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

21 ottobre 2021

Il nuovo meccanismo dello sportello unico all'interno della caotica disciplina del trattamento transfrontaliero dei dati personali. La Corte di Giustizia si pronuncia sulla corretta interpretazione dell'Istituto

Angelo Napoli

Nuova
Editrice
Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

IL NUOVO MECCANISMO DELLO SPORTELLO UNICO ALL'INTERNO DELLA CAOTICA DISCIPLINA DEL TRATTAMENTO TRANSFRONTALIERO DEI DATI PERSONALI. LA CORTE DI GIUSTIZIA SI PRONUNCIA SULLA CORRETTA INTERPRETAZIONE DELL'ISTITUTO

Angelo Napoli
Università degli studi di Salerno

SOMMARIO*:* 1. La vicenda – 2. Il trattamento transfrontaliero di dati personali: gli aspetti conflittuali del rapporto tra Unione Europea e Stati Uniti – 3. La ripartizione dei poteri tra le autorità all'interno del nuovo quadro normativo europeo – 4. Rilievi conclusivi

ABSTRACT: La sentenza interpretativa della Corte di Giustizia emessa nella causa C-645/19 verte sul nuovo istituto dello sportello unico, recentemente introdotto dal GDPR, e sul ruolo ricoperto dalle autorità garanti in caso di trattamento transfrontaliero di dati personali. Più di precipuo, i giudici europei hanno evidenziato come, nella ripartizione dei poteri tra le diverse amministrazioni preposte alla tutela dei dati personali, sia sempre necessario assicurare il rispetto delle disposizioni del regolamento, il cui obiettivo è quello di garantire una cooperazione e collaborazione tra tutte le autorità che entrano in gioco in un determinato procedimento. Evidente è la finalità unificatrice della normativa di nuova specie, volta ad offrire una maggiore certezza del diritto e, conseguentemente, ad evitare che, in caso di illecito trattamento transfrontaliero di dati personali di internauti provenienti da più Stati, i garanti nazionali possano procedere ciascuno forte della propria autonomia. Invero, lasciando a questi ultimi la libertà di agire secondo le proprie regole, introducendo svariati procedimenti sulla medesima questione, con esiti presumibilmente differenti a causa delle diverse normative applicate dalle autorità giudiziarie chiamate a pronunciarsi, si alimenterebbe una caotica disorganizzazione processuale. Pertanto, l'intento è quello di creare uno

stretto dialogo tra le autorità, che assicuri una tutela uniforme e rispettosa dei principi europei.

Il provvedimento *de quo*, inoltre, concede lo spunto per una serie di riflessioni sulla circolazione dei dati personali al di là dei confini nazionali ed europei: in particolare, è qui utile ripercorrere l'evoluzione del rapporto tra Unione Europea e Stati Uniti volto a garantire una protezione sempre più stringente ai cittadini europei che forniscono dati alle imprese oltreoceano, nonché porre l'attenzione sulle problematiche ancora in atto su tale argomento.

ABSTRACT**:** *The interpretative judgment of the Court of Justice issued in case C-645/19 concerns the new one-stop shop, recently introduced by the GDPR, and the role played by the guarantor authorities in the case of cross-border processing of personal data. More specifically, the European judges have publicy remarked how being compliant with the provisions of the regulations, whose aim is to guarantee full cooperation between the authorities involved in a specific proceeding, is always necessary in the cooperation of powers in between administrations involved in data protection. The unifying purpose of the new type of legislation is evident, aimed at offering greater legal certainty and, consequently, to avoid that, in the event of illegal cross-border processing of personal data of Internet users from several States, the national guarantors can each proceed strongly of their autonomy. Indeed, leaving the latter to act according to their own rules, introducing various procedures on the same issue, with results applied by the differentiated freedoms due to the different judicial authorities called upon to pronounce, would feed a chaotic procedural disorganization. Therefore, the intent is to create a close dialogue between the authorities, which ensures uniform protection and respect for European principles.*

Furthermore, the above mentioned provision becomes the point of origin for further considerations on the circulation of personal data beyond national and European borders: in particular, it is useful here to retrace the evolution of the relationship between the European Union and the United States aimed at guaranteeing ever more stringent protection for European citizens than providing data to overseas companies, as well as holding attention on current issues concerning this topic.

1. LA VICENDA

Il 25 giugno 2021 la Corte di Giustizia si è pronunciata sulla questione pregiudiziale proposta dalla Corte di appello di Bruxelles[1] avente ad oggetto l'interpretazione delle disposizioni del regolamento 2016/679 che hanno introdotto il meccanismo dello sportello unico, con lo scopo di chiarire la sfera di potere che spetta alle autorità garanti di agire in giudizio nell'ipotesi di illecito trattamento transfrontaliero di dati personali.

Il caso sottoposto al vaglio della Corte trae origine dalla richiesta di inibitoria formulata dal Presidente della Commissione belga per la tutela della vita privata[2] nei confronti delle società Facebook Ireland, Facebook Inc. e Facebook Belgium, al fine di interrompere l'illecita raccolta di dati degli utenti da parte di queste ultime. Nello specifico, la parte attrice chiedeva al giudice di prime cure che fosse ingiunto alle convenute la cessazione della raccolta di dati degli internauti belgi, in assenza del loro consenso e tramite i cookie e i social plugin che consentono alle imprese di ottenere svariate tipologie di dati, nonché la distruzione di tutti i dati raccolti attraverso tali modalità illecite; l'autorità belga, di conseguenza, eccepiva la violazione degli artt. 7, 8 e 47 della Carta dei diritti fondamentali[3].

In seguito a tale decisione, le società *de quibus* interponevano appello, al termine del quale il giudice di secondo grado stravolgeva completamente la sentenza emessa in primo grado dichiarandosi competente a statuire esclusivamente sulle azioni intentate nei confronti di Facebook Belgium. Nelle more del giudizio, quest'ultima società eccepiva l'incompetenza dell'Autorità per la protezione dei dati belga[4], in qualità di successore della CPVP[5], a ri-

[1] Corte di Giustizia UE, sentenza 25 giugno 2021, causa C-645/2019, *Facebook Ireland*
[2] *Commissie ter bescherming van de persoonlijke levenssfeer* (nel prosieguo "CPVP").
[3] I tre articoli citati tutelano, rispettivamente, il "rispetto della vita privata e della vita familiare" (art. 7), la "protezione dei dati di carattere personale" (art. 8) e il "diritto ad un ricorso effettivo e a un giudice imparziale" (art. 47).
[4] *Gegevensbeschermingsautoriteit* (in seguito "APD").
[5] La legge 8 dicembre 1992, che ha recepito nell'ordinamento belga la direttiva 95/46, ha istituito la CPVP quale garante dei dati personali belga. A tal proposito, l'art. 32, paragrafo 3, seconda parte, della normativa in esame sanciva il potere del presidente della CPVP di "sottoporre al giudice di primo grado qualsiasi controversia relativa all'applicazione della presente legge e delle sue misure di esecuzione". In seguito

chiedere un provvedimento di siffatta portata, in quanto, in seguito all'entrata in vigore del Regolamento 2016/679, e, nello specifico, del già citato meccanismo dello sportello unico, l'APD avrebbe perso il potere di azione per gli illeciti trattamenti di dati all'estero per i fatti successivi all'entrata in vigore del regolamento stesso, che spetterebbe esclusivamente all'autorità capofila. Pertanto, sarebbe spettato unicamente all'*Irish data Protection Commission*, ovvero alla Commissione irlandese per la protezione dei dati, la competenza a proseguire il procedimento principale.

Sulla base di quanto premesso, la Corte di appello belga decideva di sospendere il procedimento e di chiedere alla Corte di Giustizia un chiarimento interpretativo sulla portata di tale istituto[6].

---

all'entrata in vigore del GDPR, l'ordinamento belga ha istituito, con la legge 3 dicembre 2017, una nuova autorità per la protezione dei dati, l'ADP, che gode degli stessi poteri che competevano alla CPVP (art. 3) e si qualifica quale successore legale della medesima per i processi già iniziati da quest'ultima (art. 6).

[6] Nello specifico, il giudice belga chiedeva:

"1) Se gli articoli [55, paragrafo 1], da 56 a 58 e da 60 a 66 del [regolamento 2016/679], in combinato disposto con gli articoli 7, 8 e 47, della [Carta], debbano essere interpretati nel senso che un'autorità di controllo, che, in forza della normativa nazionale adottata in esecuzione dell'articolo [58, paragrafo 5], di tale regolamento, abbia il potere di agire in sede giudiziale dinanzi a un giudice del suo Stato membro contro le violazioni di detto regolamento, non può esercitare tale potere con riguardo a un trattamento transfrontaliero se essa non è l'autorità di controllo capofila per il trattamento transfrontaliero di cui trattasi.

2) Se, a tal riguardo, assuma rilevanza la circostanza che il titolare di detto trattamento transfrontaliero non abbia in tale Stato membro lo stabilimento principale, ma solo un altro stabilimento.

3) Se, a tal riguardo, assuma rilevanza la circostanza che l'autorità nazionale di controllo intenti l'azione nei confronti dello stabilimento principale del titolare del trattamento o nei confronti dello stabilimento nel proprio Stato membro.

4) Se, a tal riguardo, assuma rilevanza la circostanza che l'autorità nazionale di controllo abbia già intentato l'azione prima della data di entrata in vigore (il 25 maggio 2018) del regolamento [2016/679].

5) In caso di risposta affermativa alla prima questione, se l'articolo [58, paragrafo 5], del regolamento 2016/679 abbia effetto diretto, cosicché un'autorità nazionale di controllo può invocare detto articolo per intentare o proseguire un'azione nei confronti di privati, anche se l'articolo [58, paragrafo 5], del regolamento 2016/679 non sia stato specificamente trasposto nella normativa degli Stati membri, pur essendo la trasposizione obbligatoria.

6) In caso di risposta affermativa alle questioni che precedono, se l'esito di siffatti procedimenti possa ostare ad una conclusione opposta dell'autorità di controllo capofila nel caso in cui tale autorità capofila esamini le medesime attività di trattamento transfronta-

Una volta esposta la vicenda, occorre ricostruire il contesto all'interno del quale si pone la decisione in esame, ripercorrendo le tappe fondamentali sul trattamento transfrontaliero dei dati personali e soffermandosi sulla decisione della Corte europea, al fine di comprendere la corretta ripartizione dei poteri tra più autorità garanti in seguito all'introduzione del meccanismo dello sportello unico.

2. Il trattamento transfrontaliero di dati personali: gli aspetti conflittuali del rapporto tra unione europea e stati uniti

La gestione di dati personali da parte di imprese non situate nel territorio nazionale della persona fisica che ne consente il trattamento, in particolare nel caso in cui la circolazione avvenga al di fuori dell'UE[7], rappresenta una

liero o attività analoghe, conformemente al meccanismo previsto agli articoli 56 e 60 del regolamento 2016/679».

[7] Per un'attenta analisi del trattamento transfrontaliero di dati personali, si veda, *ex multis*, G.M. RICCIO - F. PEZZA, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali,* in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, 2019, p. 585 ss.; G. RESTA - V. ZENO-ZENCOVICH (a cura di), *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE,* in *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma TrE-Press, 2016; F. BIGNAMI - G. RESTA, *Transatlantic Privacy Regulation: Conflict and Cooperation,* in *Law and Contemporary Problems*, 2015, 78, p. 231 ss.; D. PITTELLA, *Trasferimento verso paesi terzi,* in *La nuova disciplina europea della privacy,* Padova, 2016, p. 259 ss.; G.M. RICCIO, *Capo V – Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, in GDPR e Normativa Privacy. Commentario,* p. 394 ss.; L. ZAGATO, *Il trasferimento di dati personali verso stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE,* in *Diritto del Commercio internazionale,* 2008, n. 2, p. 297 ss.; S. KIRSCHEN, *Il trasferimento all'estero dei dati personali verso paesi terzi o organizzazioni internazionali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018,* Bologna, 2019, p. 261 ss..

Sul concetto di trattamento transfrontaliero di dati personali, si veda Corte di Giustizia CE, sentenza 06 novembre 2003, causa C-101/2001, *Göta Hovrätt c. Bodil Lindqvist*, con nota a sentenza di G. CASSANO - I.P. CIMINO, *Qui, là, in nessun luogo… come le frontiere dell'Europa si aprirono ad Internet: cronistoria di una crisi annunciata per le regole giuridiche fondate sul principio di territorialità,* in Giur. It., 2004, 10, dove gli autori spiegano come la Corte di Giustizia, nel caso Lindqvist, abbia rielaborato la definizione di trattamen-

prassi in continua espansione, quale conseguenza dell'incessabile sviluppo tecnologico e del persistente abbattimento delle frontiere.

Questo fenomeno in perenne crescita riscontra problematiche di non poco rilievo, laddove diviene fondamentale conciliare l'esigenza sociale di trasferire i dati in paesi extraeuropei con la necessità di rendere il più efficace possibile la protezione dei dati che transitano al di là dei predetti confini. In tale contesto, è d'uopo porre l'attenzione sul conflitto, tutt'ora *in fieri*, tra UE e USA; ciò in quanto, mentre l'Unione ha sempre garantito un'adeguata salvaguardia della sfera personale dei propri cittadini, attraverso disposizioni[8] adibite a tale finalità, negli Stati Uniti manca un'apposita regolamentazione volta alla protezione dei dati che gli utenti europei cedono ad imprese straniere.

Ciò posto, come si concilia questa incompatibilità con la necessità di rispettare le garanzie apprestate dall'UE con riferimento alla circolazione di dati sensibili oltre i confini comunitari?

Per rispondere a tale interrogativo, assume un certo rilievo il passaggio dalla direttiva al GDPR, che ha intensificato il sistema di tutela, e soprattutto la saga *Schrems*, che ha condotto ad un risvolto fondamentale (seppur non decisivo) all'interno del conflitto USA-UE.

Il quadro normativo nel quale prende vita la succitata vicenda è dato dagli articoli 25 e 26 della direttiva del '95, quali disposizioni regolatrici del trattamento transfrontaliero di dati personali. In particolare, il primo detta la regola generale secondo cui il trasferimento di dati di cittadini europei verso paesi stranieri è ammesso solo se questi ultimi garantiscono un livello di protezione dei dati adeguato alle garanzie offerte dall'Unione[9]. A tal fine, UE e

---

to transfrontaliero di dati personali, quale concetto che risente pienamente dello sviluppo tecnologico e del sempre maggiore distaccamento dal "principio della territorialità".

[8] Alla materia del trasferimento di dati personali verso paesi terzi è stato dapprima dedicato il Capo IV, artt. 25-26, della direttiva 95/46/CE, e successivamente il Capo V, artt. 44-50 del GDPR n. 2016/679.

[9] L'art. 26 della direttiva 95/45/CE contiene una deroga alla disposizione che lo precede, poiché consente il trasferimento di dati personali anche verso un paese terzo che non garantisca una protezione adeguata, purché sussista almeno una delle seguenti condizioni:
a) La persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto;
b) Il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa;

USA hanno stipulato un accordo, definito *Safe Harbour Principles*, eseguito per mezzo della decisione 2000/520 della Commissione (nominata "approdo sicuro"), attraverso il quale regolare i flussi di dati di utenti europei che vengono trasferiti a imprese situate negli Stati Uniti[10]. Il patto *de quo* darebbe vita ad una "presunzione di adeguatezza"[11] del sistema americano di protezione dei dati a quello europeo.

In questo scenario si inserisce la nota sentenza "*Schrems I*"[12], attraverso la quale la Corte di Giustizia ha dichiarato l'invalidità dell'"approdo sicuro",

---

c) Il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo;

d) Il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria;

e) Il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata;

f) Il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.

[10] Decisione del 26 luglio 2000 della Commissione Europea, a norma della direttiva 95/45/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, in GUCE, L. 215 DEL 25 AGOSTO 2000, P- 7 SS. Per un approfondimento sul tema, si veda S. SICA - V. D'ANTONIO, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità,* in *Diritto dell'informazione e dell'informatica*, 2015, p. 801 ss.; G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale*, in *Diritto dell'informazione e dell'informatica*, op. cit., p. 887 ss.; V. D'ANTONIO, *Il trasferimento dei dati all'estero, comm. Sub artt. 42 – 45,* in P. STANZIONE – S. SICA (a cura di), *La nuova disciplina della privacy*, Milano, 2004, p. 155 ss.; R. MIRANDA, *Trasferimento dei dati all'estero*, in C.M. BIANCA – F.D. BUSNELLI, *La protezione dei dati personali,* Padova, 2007, p. 851 ss.; I.J. LLOYD, *Information Technology law*, 6th. Ed., Oxford, 2011, p. 182 ss.

[11] In tal senso, V. D'ANTONIO – B.M. SABATINO, *Teorie geopolitiche ed economiche dietro la decisione Schrems III*, in *Diritto dell'informazione e dell'informatica*, op. cit., p. 814 ss.

[12] Corte di Giustizia UE, sentenza 06 ottobre 2015, causa C-362/2014, *Maximillian Schrems c. Data Protection Commissioner*. Per approfondimenti sull'argomento, si veda C. GENTILE, *La saga Schrems e la tutela dei diritti fondamentali*, in *Federalismi.it*, 2003, p. 35 ss.; B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorve-*

motivando che l'esistenza di un accordo siglato tra USA e UE per regolare il trasferimento extraeuropeo di dati sensibili non può valere come garanzia di un trattamento corretto, in quanto è comunque necessario che il Paese nel quale sono situate le imprese responsabili del trattamento garantisca un livello di protezione che sia "sostanzialmente equivalente" a quello della Comunità (seppur non identico). La decisione, dunque, muove dall'assenza negli USA di un sistema di regole che assicuri protezione alle persone fisiche, a differenza dell'impianto normativo europeo, che gode, invece, di regole trasparenti e adeguate al perseguimento di tale obiettivo[13].

A seguito della sentenza della Corte si è avuto un vuoto normativo sul flusso di dati tra UE e USA; pertanto, queste ultime si sono attivate al fine di addivenire ad un nuovo accordo, il *Privacy Shield*, cui è stata data successivamente attuazione attraverso la decisione 2016/1250 (denominata "scudo per la privacy")[14], con il quale è stato stabilito un sistema di autocertificazio-

---

glianza di massa, in *Giornale di diritto amministrativo*, 2007, p. 333 ss.; A. MONTERIN, *Dell'incertezza nei trasferimenti di dati personali verso gli Stati Uniti*, in *La Nuova Giurisprudenza Civile Commentata*, 2011, p. 154 ss.; R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost. 2016*, p. 289 ss.; O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di Giustizia in materia di digital privacy come osservatorio privilegiato*, in *Medialaws*, 2018, p. 138 ss.; S. CRESPI, *La tutela dei dati personali UE a seguito della sentenza Schrems,* in *Eurojus*, 2.11.2015.

[13] Le violazioni della *privacy* da parte dello Stato americano sono state rivelate, per la prima volta, dalle dichiarazioni di Edward Snowden, che nel 2013 ha fatto luce sulle operazioni di sorveglianza e compromissione di massa, effettuate dall'Agenzai per la Sicurezza Nazionale statunitense nei confronti di cittadini americani e non. Per maggiori dettagli sulla vicenda, si veda F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale,* in *Federalismi.it,* op. cit.; G. GREENWALD, *No Place to Hide: Edward Snowden, the Nsa, and the U.S. Surveillance State,* New York, Metropolitan Books, 2014.

[14] Sui tratti essenziali di tale decisione si veda, *ex multis*, S. SICA – V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles,* in *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTre-Press, 2016, p. 133 ss; V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in *Diritto dell'informazione e dell'informatica*, op. cit., p. 683 ss.; G.M. RICCIO, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbour Agreement?*, in *Diritto dell'informazione e dell'informatica*, op. cit., p. 856 ss.; A. MANTELERO, *From Safe Harbour to Privacy Shield. The "medieval" sovereignity on personal data*, in *Contratto e impresa/Europa*, 2016, p. 338 ss.; S. MONTELENO –

ne delle imprese americane che trattano i dati dei cittadini europei, al fine di assicurare un livello di protezione maggiore di tali dati.

Medio tempore, alla direttiva 95/45/CE subentrava il nuovo Regolamento generale sulla protezione dei dati, n. 2016/679 (divenuto pienamente applicabile in tutti gli Stati membri il 25 maggio 2018)[15], quale normativa volta al rafforzamento della protezione dei dati, che diviene diritto fondamentale dell'Unione[16]. Il GDPR dedica il Capo V al trattamento transfrontaliero di dati, con lo scopo di fornire una serie di disposizioni idonee alla protezione dei dati trasferiti ad imprese non europee. A tal proposito, l'art. 45 stabilisce la regola generale, secondo la quale la Commissione Europea può consentire, mediante atti di esecuzione, il trasferimento di dati verso un Paese terzo se quest'ultimo garantisce un "livello di protezione adeguato" (ripercorrendo, in tal modo, la scia dell'art. 25 della Direttiva)[17]. L'art. 46, inoltre, completa la norma precedente, in quanto afferma che, pur in assenza di una decisione di adeguatezza della Commissione, la circolazione dei dati è consentita anche attraverso una serie di strumenti che sono appositamente elencati nel se-

---

L. PUCCIO, *The privacy shield update on the state of play of the EU-US data transfer rules: in-depth analysis*, in *European Parliament, Directorate General for Prliamentary Research Services*, 2018; 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 *Diritto dell'Unione* europea, 2016, p. 773 ss.; V. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, op. cit., p. 27 ss.

[15] Sulle differenze tra la direttiva 95/45/CE e il GDPR n. 679/2016 si veda S. SICA – V. D'ANTONIO – G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* op. cit.; G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, op. cit.; F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni,* in *Medialaws*, op. cit., p. 109 ss.; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

[16] A tal proposito, rileva il considerando numero 1 del GDPR 679/2016, dove si afferma che il diritto fondamentale alla tutela dei dati personali è riconosciuto come tale dall'art. 8 della Carta di Nizza e dall'art. 16 del Trattato sul funzionamento dell'Unione europea

[17] L'art. 45 del nuovo GDPR recita espressamente, al primo comma, che "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".

condo comma[18]; tra questi figurano "le clausole tipo di protezione dei dati adottate dalla Commissione", che rilevano nel caso in esame poiché la Commissione, attraverso la decisione n. 2010/87 (modificata tramite la decisione di esecuzione n. 2016/2297), ha approvato una serie di clausole contrattuali, che sono diventate lo strumento principale per regolare il trasferimento di dati verso gli USA dopo la dichiarazione di invalidità dei *Principles*.

Orbene, nel quadro normativo appena illustrato, subentra la sentenza *Schrems II*[19], attraverso la quale i giudici europei si sono espressi sugli strumenti regolatori del trasferimento dei dati al di fuori dei confini della Comunità. Più di precipuo, la Corte ha dichiarato l'invalidità del *Privacy Shield*, in quanto neanche questo accordo sarebbe idoneo a fornire una protezione ade-

[18] L'art. 46 afferma che "possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:
a) Uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) Le norme vincolanti d'impresa in conformità dell'articolo 47;
c) Le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) Le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) Un codice di condotta adottato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;
f) Un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento del paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati."

[19] Corte di Giustizia UE, sentenza 16 luglio 2020, causa C-311/2018, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems*. Sull'argomento, V. D'ANTONIO – B.M. SABATINO, *Teorie geopolitiche ed economiche dietro la decisione Schrems III*, op. cit., p. 814 ss. Gli autori osservano che, seppur la sentenza *de quo* sia generalmente conosciuta come *Schrems II*, appare preferibile denominarla *Schrems III*, per distinguerla dalla causa C-489/2016, del 25 gennaio 2018. Per approfondire quanto deciso nella causa C-311/2018, si veda B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giornale di diritto amministrativo*, op. cit., p. 333 ss.; O. POLLICINO – F. RESTA, *Dati personali, perché la Corte di Giustizia ha annullato il «Privacy Shield». La Corte di Giustizia dell'Unione europea riscrive le trame dei rapporti (e non solo) commerciali tra Europa e Stati Uniti*, in *www.ilsole24ore.com*, 20 luglio 2020.

guata del flusso di dati provenienti dai cittadini europei e diretti alle imprese americane, a causa della forte ingerenza dello Stato nella raccolta dei dati, che avviene per mezzo dei servizi segreti. La Corte, ribadendo quanto affermato in *Schrems I*, fa valere nuovamente la "clausola di adeguatezza", che nel sistema americano si rivela assente a causa della supremazia della sicurezza nazionale sulla tutela della sfera privata dei cittadini. Differentemente dal *Privacy Shield*, i giudici europei si sono pronunciati in senso favorevole sulla validità delle clausole di protezione adottate con la decisione 2010/87; tuttavia tali clausole, avendo natura contrattuale, sono vincolanti esclusivamente per le parti del contratto stesso, e dunque non anche per le autorità pubbliche degli Stati cui vengono inviati i dati.

In conclusione, è agevole notare come l'incompatibilità tra UE e USA nella salvaguardia dei dati sensibili rappresenta ancora una falla del sistema che necessita di essere colmata; pertanto, l'obiettivo che si pone la Comunità è proprio quello di cercare di ridurre questa inconciliabilità di impianti giuridici, estendendo i principi europei anche al di fuori dei confini comunitari. In tal senso, i mezzi di tutela che offre l'Unione (e, di conseguenza, i diritti oggetto della protezione), fungerebbero da esempio per tutti quei Paesi in cui il livello di protezione dei dati sensibili incontra ancora svariate problematiche. In materia di trattamento transfrontaliero, dunque, in seguito alla continua espansione della circolazione di dati e al conseguente allontanamento dal principio di territorialità, appare necessario assicurare uniformità tra i diversi ordinamenti, attraverso una cooperazione internazionale che possa riempire i vuoti di tutela. A tal fine, il sistema di garanzia europeo appare sicuramento il candidato migliore da cui prendere le mosse.

3. La ripartizione dei poteri delle autorità all'interno del nuovo quadro normativo europeo

All'interno del contesto appena delineato, si inserisce la delicata questione inerente al potere di azione che spetta alle Autorità di controllo in caso di illecito trattamento di dati che coinvolga più Paesi. A tal proposito, risulta ancora una volta decisivo il passaggio dalla direttiva 95/45/CE al GDPR

679/2016, che ha rielaborato il sistema di competenze in capo alle amministrazioni nazionali, tematica che è stata affrontata anche nel corso della vicenda *Schrems*.

Durante la vigenza della direttiva, l'art. 28 stabiliva che ogni Autorità garante nazionale godesse del potere di azione per tutti i trattamenti che si svolgevano nel proprio territorio, e, di conseguenza, ogni titolare o responsabile del trattamento aveva come punto di riferimento ciascuna autorità coinvolta nel trattamento di dati. Pertanto, la disposizione in esame esaltava il principio di indipendenza di ciascun garante nazionale per azionare la tutela giudiziaria[20]. Questo principio è stato ribadito anche nella sentenza *Schrems I*, dove la Corte ha precisato che per ogni trattamento di dati personali, è d'uopo che le autorità nazionali agiscano in piena indipendenza per assicurare un livello adeguato di tutela dei dati sensibili[21]. Ordunque, sulla base di tale riferimento normativo, ciascun garante poteva agire autonomamente in giudizio anche nell'ipotesi in cui l'illecito trattamento aveva coinvolto più Stati. Tuttavia, attraverso questo sistema, si originavano procedimenti paralleli sulla medesima questione, che terminavano con esiti differenti, poiché le diverse autorità giudiziarie decidevano ognuna sulla base della rispettiva normativa nazionale. Pertanto, la diretta conseguenza di tale meccanismo è stata una confusione giurisprudenziale; è pur vero che la tutela risultava essere più immediata, poiché ciascun cittadino leso poteva adire la propria autorità nazionale, ma l'incoerenza decisionale incideva pesantemente sulla certezza del diritto e sull'economia processuale.

In seguito al tramonto della direttiva, il nuovo GDPR ha riorganizzato la materia del trattamento transfrontaliero di dati sensibili[22], con l'obiettivo di ovviare alle esigenze scalfite dalla precedente normativa. Per questo motivo, è stato introdotto il meccanismo dello sportello unico (*one stop shop*), il quale stabilisce una ripartizione di competenze tra un'autorità capofila (denomi-

[20] Quanto detto emerge anche dal considerando n. 62 della direttiva del '95, il quale afferma che "la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali".

[21] Sul tema, si veda B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giornale di diritto amministrativo*, op. cit., p. 333 ss.

[22] La disciplina è stata inserita nel Capo VI del GDPR n. 679/2016, artt. 51-76.

nata *Leading Supervision Authority*), cioè quella del Paese in cui l'impresa che raccoglie i dati degli internauti ha la sede principale, e le altre autorità interessate nel procedimento avente ad oggetto la circolazione dei dati al di fuori delle frontiere europee[23]. Tuttavia, l'istituto in esame, pur definendo una sorta di "gerarchia" sul potere di azione giudiziale, non esclude del tutto il potere delle autorità "secondarie", atteso che, sulla scorta della nuova normativa, il riparto delle competenze tra i garanti si fonderebbe comunque sui fondamentali principi di cooperazione e coerenza[24]. Nello specifico, l'articolo 61 del GDPR elenca una serie di attività che richiedono la stretta cooperazione tra le diverse autorità di controllo, quali, ad esempio, lo scambio di informazioni utili e l'assistenza reciproca, mentre l'articolo 62 introduce la possibilità per le diverse amministrazioni di svolgere operazioni congiunte (quali, ad esempio, la collaborazione nelle indagini). Al fine di rafforzare maggiormente tale cooperazione, il principio di coerenza emerge laddove l'articolo 64 ha stabilito che, in caso di collaborazione difficoltosa tra le autorità in gioco in un determinato procedimento, vi è la possibilità di adire il Comitato europeo per la protezione dei dati[25], che ha il potere di emettere decisioni vincolanti. Infine, l'articolo 66 consente anche alle autorità non capofila di prendere l'iniziativa in caso di urgente intervento per la protezione dei diritti dei cittadini[26].

Nel contesto normativo appena delineato, si inserisce la questione pregiudiziale che il giudice del rinvio ha sottoposto alla Corte di Giustizia,

[23] L'art. 56 del GDPR dispone che "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

[24] Capo VI del GDPR n. 679 del 2016, artt. 60-67

[25] Il Comitato europeo per la protezione dei dati è un organismo indipendente, il cui obiettivo è quello di assicurare una coerente attuazione del Regolamento 679/2016.

[26] Più di preciso, il comma 1 dell'articolo 66 recita "In circostanze eccezionali, qualora ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, un'autorità di controllo interessata può, in deroga al meccanismo di coerenza di cui agli articoli 63, 64 e 65, o alla procedura di cui all'articolo 60, adottare immediatamente misure provvisore intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi. L'autorità di controllo comunica senza ritardo tali misure e la motivazione della loro adozione alle altre autorità di controllo interessate, al comitato e alla Commissione".

avente ad oggetto una corretta interpretazione dell'articolo 58, comma 5, del GDPR. La norma in esame afferma che "Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso"; pertanto, il giudice belga si è domandato se, alla luce dell'introduzione del meccanismo dello sportello unico e del necessario rispetto dei principi di cooperazione e coerenza nel riparto delle competenza tra le autorità, tale disposizione dovesse essere interpretata nel senso che, in caso di illecito trattamento transfrontaliero di dati personali, soltanto l'autorità capofila (e, nel caso di specie, la *Data Protection Commission*) sarebbe legittimata ad adire il giudice nazionale (dunque, nel caso in esame, il giudice irlandese), oppure se ciò competerebbe altresì alle altre autorità interessate (pertanto, anche alla CPVP).

La Corte risponde a tale quesito facendo leva proprio sui principi e sulle disposizioni precedentemente analizzati. Lo scopo del nuovo GDPR è quello di assicurare una applicazione delle regole in esso contenute che sia il più uniforme possibile, sopperendo, in tal modo, alle lacune sorte in vigenza della direttiva e garantendo una protezione più forte dei diritti dei cittadini. Per il perseguimento di questo obiettivo, è necessario che le amministrazioni nazionali rispettino i ruoli che il regolamento attribuisce alle stesse, il quale non stabilisce una competenza esclusiva in capo alla *Leading Authority*, ma concede a questa un ruolo di primazia, che va eseguito nella piena osservanza dei principi di cooperazione e coerenza, nonché delle disposizioni del GDPR[27].

[27] Paragrafo 74 della sentenza in esame, la Corte dichiara testualmente che "l'articolo 55, paragrafo 1 e gli articoli da 56 a 58 nonché da 60 a 66 del regolamento 2016/679, in combinato disposto con gli articoli 7, 8 e 47 della Carta, devono essere interpretati nel senso che un'autorità di controllo di uno Stato membro, la quale, in forza della normativa nazionale adottata in esecuzione dell'articolo 58, paragrafo 5, di tale regolamento, abbia il potere di intentare un'azione dinanzi a un giudice di tale Stato membro e, se del caso, di agire in sede giudiziale in caso di presunta violazione di detto regolamento, può esercitare tale potere con riguardo al trattamento transfrontaliero di dati, pur non essendo l'«autorità di controllo capofila» ai sensi dell'articolo 56, paragrafo 1, dello stesso regolamento con riguardo a siffatto trattamento di dati, purché ciò avvenga in una delle situazioni in cui il regolamento 679/2016 conferisce a tale autorità di controllo la competenza

In conclusione, va rilevato che il meccanismo dello sportello unico si pone come punto di partenza per il superamento delle difficoltà esistenti durante la vigenza della direttiva, in quanto rappresenta uno strumento utile per bilanciare le esigenze di certezza del diritto e di celerità processuale da un lato, e il rispetto dei principi europei dall'altro.

4. Rilievi conclusivi

Con la presente pronuncia la Corte risolve le questioni interpretative in merito al comma 5 dell'articolo 58 del GDPR. La norma in questione, infatti, va letta nel senso che è pur vero che il potere di azione in caso di illecito trattamento transfrontaliero spetta all'autorità capofila ma, nei casi previsti dal regolamento e precedentemente esposti, è concesso un potere di azione anche alle autorità secondarie al fine di assicurare un equo bilanciamento tra i principi di semplificazione e celerità della tutela da un lato, e i principi di cooperazione e coerenza dall'altro.

La Corte, dunque, pone fine alla diatriba giurisprudenziale intercorsa nel periodo compreso tra l'entrata in vigore del regolamento e l'attuale sentenza qui esposta, nel quale si sono susseguiti e contrapposti due orientamenti[28]. Secondo il primo, le autorità di controllo, pur non capofila, avrebbero sempre la competenza di agire in tali ipotesi; tuttavia, interpretando il comma 5 dell'articolo 58 in tal modo, verrebbe meno la *ratio* della "gerarchia" imposta dallo sportello unico. In base al secondo orientamento, invece, solo le *leading authorithies* godrebbero di tali poteri; tale lettura renderebbe però vane le disposizioni del regolamento che fanno riferimento alle ipotesi in cui le autorità non capofila possano prendere l'iniziativa. Pertanto, la lettura più convincente è proprio quella data dalla Corte, che pone una soluzione me-

ad adottare una decisione che accerti che il trattamento in questione viola le norme in esso contenute, nonché nel rispetto delle procedure ci cooperazione e di coerenza previste da tale regolamento".

[28] Corte di Giustizia UE, Concl. Avv. Gen. Michal Bobek, 13.01.2021, n. 645/19.

diana, basata sull'attuazione dei principi di cooperazione e coerenza nel rispetto della "gerarchia" imposta dal nuovo istituto[29].

In conclusione, la presente decisione è utile per riflettere sulla *ratio* dell'istituto introdotto dal GDPR, ovvero quella di assicurare un procedimento semplificato che garantisca una tutela più ampia alle persone fisiche in caso di illecito trattamento transfrontaliero di dati personali. Pertanto, emerge chiaramente una tendenza unificatrice del legislatore, che se da un lato si pone l'obiettivo di circoscrivere il potere di autonomia espressamente evidenziato dalla direttiva del '95, dall'altro mira ad assicurare la collaborazione tra le autorità. Di siffatto meccanismo ne beneficia, di conseguenza, il principio di certezza del diritto: infatti, applicando un procedimento di tale portata, in caso di circolazione dei dati personali al di là del territorio nazionale e oltre i confini dell'Unione, si evita che l'autorità di ciascuna nazione agisca indipendentemente dalle altre; in tal modo si manifesterebbe un pluralismo di decisioni sulla medesima questione (come accadeva in passato), che potrebbe anche condurre a risultati divergenti, poiché ciascuno Stato procederebbe sulla base dei propri principi e delle rispettive normative. Diversamente, l'istituto *de quo* consente a tutte le autorità degli Stati membri, i cui cittadini subiscono le violazioni, di agire nel rispetto del proprio "ruolo", assicurando, così, una stretta cooperazione che si candida quale papabile soluzione per garantire ai cittadini una tutela più forte in caso di illecito trattamento di dati personali. Tutto ciò, ovviamente, in un contesto più ampio del livello prettamente nazionale, quale conseguenza dell'incessante allontanamento dal principio di territorialità e del continuo accrescimento della circolazione dei dati a livello extranazionale.

D'altro canto, va sottolineato che il *one stop shop* contiene anche profili di criticità; a tal proposito, si osserva che il meccanismo in esame consente alle imprese che gestiscono i dati di poter effettuare una selezione dell'Autorità di vigilanza, attraverso la scelta della sede principale dell'impresa. Da ciò ne scaturisce anche una tutela meno diretta per gli internauti che hanno trasferito i propri dati ad imprese situate al di fuori della propria nazione, in quanto, come rilevato in precedenza, la tutela diventa

[29] Si potrebbe dire che la competenza dell'autorità capofila è la regola, mentre quella delle altre autorità è l'eccezione.

meno diretta, data la difficoltà che si riscontra nella distanza tra l'utente e la *leading authorithy*.

Sulla base di quanto approfondito, non si può che auspicare, *de iure condendo*, un intervento del legislatore europeo (e non solo) sia in materia di trattamento transfrontaliero di dati, che possa garantire una gestione degli stessi più sicura da parte di imprese straniere, sia sull'istituto del meccanismo dello sportello unico, che, seppur abbia inciso positivamente sulla valenza dei principi di certezza del processo e di necessaria celerità processuale, presenta alcuni aspetti che si scontrano con la tutela dei diritti dei cittadini.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future.
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442