COLLANA DEL DIPARTIMENTO DI GIURISPRUDENZA
DELL'UNIVERSITÀ DI PISA

NUOVA SERIE - *Monografie*

Gabriele Rugani

LA REGOLAMENTAZIONE DEI FLUSSI DI DATI PERSONALI DALL'UE VERSO PAESI TERZI

Alla ricerca di un bilanciamento tra espansione del commercio internazionale e *personal data protection*

IUSTITIAM COLIMUS

G. Giappichelli Editore

COLLANA DEL DIPARTIMENTO DI GIURISPRUDENZA
DELL'UNIVERSITÀ DI PISA

Nuova serie – *Monografie*

39

Gabriele Rugani

LA REGOLAMENTAZIONE DEI FLUSSI DI DATI PERSONALI DALL'UE VERSO PAESI TERZI

Alla ricerca di un bilanciamento tra espansione del commercio internazionale e *personal data protection*

G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1231-3
ISBN/EAN 979-12-211-6162-5 (ebook)

Il volume è stato sottoposto a duplice referaggio cieco.

Composizione: Media Print s.r.l. - Livorno

Stampa: Stampatre s.r.l. - Torino

Un ringraziamento speciale a mia moglie Chiara, ai miei genitori, al resto della mia famiglia e a tutti coloro che mi sono stati accanto in questi intensi anni.
Una dedica al mio amico Andrea, in memoria.

La presente opera monografica, sottoposta a referaggi anonimi e definitivamente licenziata in data 31 dicembre 2024, è frutto della ricerca svolta durante il mio Dottorato in Scienze giuridiche – Diritto internazionale ed europeo presso il Dipartimento di Giurisprudenza dell'Università di Pisa (2018-2022), nel periodo trascorso come Visiting Scholar presso l'Institute for Information Law (IViR) dell'University of Amsterdam (2021), nonché durante gli anni da Assegnista di ricerca nell'ambito del PRIN 2017 «Self- and Co- regulation for Emerging Technologies: Towards a Technological Rule of Law» – SE.CO.R.E TECH (2022-2023) e del PRIN 2022 «Artificial Intelligence between generating and tackling gender-based discriminations» – AiGeDi (2024-in corso), entrambi presso il Dipartimento di Giurisprudenza dell'Università di Pisa.

INDICE

pag.

pag.

Parte I

L'ATTUALE DISCIPLINA UNILATERALMENTE ADOTTATA DALL'UE IN MATERIA DI FLUSSI TRANSFRONTALIERI DI DATI PERSONALI

pag.

Parte II

GLI IMPEGNI COMMERCIALI ASSUNTI DALL'UE A LIVELLO INTERNAZIONALE E IL LORO IMPATTO SULLA DISCIPLINA INTERNA

pag.

pag.

INTRODUZIONE: PREMESSE, OBIETTIVO E STRUTTURA DELL'INDAGINE

PREMESSE, OBIETTIVO E STRUTTURA DELL'INDAGINE

Come si può evincere dal suo titolo, ovverosia «La regolamentazione dei flussi di dati personali dall'UE verso Paesi terzi. Alla ricerca di un bilanciamento tra espansione del commercio internazionale e *personal data protection*», la presente trattazione intende concentrarsi sugli strumenti giuridici predisposti dall'Unione europea (UE) per regolamentare i trasferimenti di dati personali che originano dai suoi Stati membri e che hanno come destinazione Paesi terzi. Nel disciplinare la materia, gli strumenti in questione devono cercare di trovare un equilibrio tra due istanze cruciali, ma in tensione tra di loro: da un lato, l'esigenza di favorire simili flussi, in ragione della loro importanza strategica per l'espansione del commercio internazionale; dall'altro lato, la necessità di proteggere i dati personali per tutelare le persone fisiche a cui essi si riferiscono (si è soliti parlare di «*personal data protection*», per l'appunto).

Alla luce di tale oggetto, il presente capitolo introduttivo intende, innanzitutto, illustrare le premesse dell'indagine, ovverosia le caratteristiche generali del fenomeno dei flussi transfrontalieri di dati personali. Nella successiva parte dell'introduzione, invece, ci si concentrerà sull'Unione europea, esponendo l'obiettivo che la trattazione si prefigge: comprendere se l'UE riesca, attraverso i suoi strumenti, a trovare un perfetto bilanciamento tra le esigenze di cui si è detto sopra, oppure se finisca per privilegiarne una a scapito dell'altra e, in quest'ultimo caso, quali siano le ragioni e quali le conseguenze. Di seguito, si illustrerà anche la struttura dell'indagine attraverso cui si tenterà di rispondere al suddetto quesito.

CAPITOLO I

LE PREMESSE DELL'INDAGINE

SOMMARIO: 1. L'economia dei dati e la sua costante espansione a livello globale. – 2. L'importanza, nell'economia dei dati, dei flussi transfrontalieri degli stessi. – 3. La particolarità, tra i flussi transfrontalieri di dati, di quelli riguardanti i dati *personali*. – 4. I diritti che richiedono tutela: il diritto alla *privacy* e quello alla protezione dei dati personali. – 5. Le tecniche normative astrattamente configurabili per bilanciare le esigenze economiche legate ai flussi transfrontalieri di dati personali con la necessità di tutelare i diritti alla *privacy* e alla protezione dei dati. – 5.1. Il «*bottom-up regulatory design*» e il «*top-down regulatory design*». – 5.2. Il «*geographically-based approach*» e l'«*organizationally-based approach*» (o «*accountability approach*»).

1. *L'economia dei dati e la sua costante espansione a livello globale*

Nell'ambito della trasformazione digitale dell'economia mondiale attualmente in corso, il valore che i dati assumono per le imprese è ormai indiscutibile – al punto che essi vengono da tempo comunemente definiti come «il nuovo petrolio» [1] – e, per di più, in costante crescita. Per alcune aziende, i dati rappresentano addirittura le risorse più preziose e, anche al di là di tali casi, l'apporto fornito dalle informazioni alla produzione dei beni e dei servizi è sempre più spesso decisivo: queste facilitano l'ottimizzazione di processi e decisioni, la creazione di nuovi prodotti e il miglioramento di quelli esistenti, nonché una conoscenza più approfondita del mercato e delle opportunità offerte da quest'ultimo [2].

---

[1] THE ECONOMIST, *The world's most valuable resource is no longer oil, but data*, in *www.economist.com*, 6 maggio 2017. Sul punto v. anche, *inter alios*: K. BHAGESHPUR, *Data Is The New Oil – And That's A Good Thing*, in *www.forbes.com*, 15 novembre 2019.

[2] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows. A Business Perspective*, in *OECD Digital Economy Papers*, Numero 297, OECD Publishing, Parigi, Agosto 2020, p. 9. Sul punto v. anche, *inter alios*: UE, Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Costruire un'economia dei dati europea*, 10 gennaio 2017, COM/2017/09 final, § 1; G. MAGALHAES-C. ROSEIRA, *Open government data and the private sector: An empirical view on business models and value creation*, in *Government Information Quarterly*, Luglio 2020, Volume 37, Numero 3, pp. 1-10, spec. p. 1.

A onor del vero, già da diversi decenni le imprese sono solite raccogliere, aggregare e analizzare le informazioni al fine di gestire al meglio le proprie attività commerciali. Tuttavia, è solo negli ultimi anni che si è assistito a un aumento vertiginoso della quantità e della portata dei dati utilizzati dalle aziende di tutto il globo, e che i dati stessi hanno assunto una posizione centrale in un gran numero di modelli commerciali [3].

In particolare, si può dire che siamo oggi di fronte a due tipologie di imprese. Da un lato, le cosiddette «*data-enabled businesses*» (letteralmente, «imprese rese possibili dai dati»): si tratta di attività che possono essere considerate come interamente digitali, nate con i dati («*data native*»). I dati sono la linfa vitale delle loro operazioni, il fattore chiave che consente loro di generare ricavi [4]. Tra queste imprese, possiamo indubbiamente menzionare i cinque colossi del digitale, o «*big tech*», appartenenti alla galassia cosiddetta GAFAM, ovvero Google (la cui società madre prende il nome di Alphabet), Amazon, Facebook (di proprietà di Meta Platforms), Apple e Microsoft. Tali aziende statunitensi, annoverate nel momento in cui si scrive tra quelle di maggior valore al mondo [5], presentano, nonostante l'adozione di modelli differenti, un elemento in comune: la loro essenza risiede infatti nella ricerca, nella raccolta e nel trattamento di dati [6]. Più in generale, possiamo annoverare tra le «*data-enabled businesses*» tutte quelle piattaforme *online* che si affidano ai dati e all'analisi degli stessi («*data analytics*») per permettere l'incontro tra gli utenti e i fornitori di beni e servizi: a titolo esemplificativo, si possono citare Uber, Booking e Airbnb [7]. Facile comprendere che, senza i dati, nessuna delle società appena menzionate potrebbe esistere.

Dall'altro lato, possiamo invece trovare le cosiddette «*data-enhanced businesses*» (letteralmente, «imprese migliorate dai dati»): queste sono attività di tipo più tradizionale, nell'ambito delle quali, però, i dati consentono la creazione di nuovo valore rispetto al passato [8]. Un semplice esempio può essere rappresentato dalle industrie manifatturiere: a tal riguardo, si segnala come uno studio pubblicato già nel 2016, e condotto su circa 18mila stabilimenti (nella fattispecie, statunitensi), abbia dimostrato che quelli che si affidano a decisioni basate

---

[3] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., p. 10.

[4] *Ibid.*

[5] Sul punto v., *inter alios*: M. Szmigiera, *Biggest companies in the world by market capitalization 2021*, in *www.statista.com*, 10 settembre 2021, consultabile al seguente link: *https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/#statisticContainer* (ultimo accesso in data 31 dicembre 2024).

[6] J.C.M. De Bustos-J. Izquierdo-Castillo, *Who will control the media? The impact of GAFAM on the media industries in the digital economy*, in *Revista Latina de Comunicación Social*, 2019, Numero 74, pp. 803-821, spec. p. 812, secondo cui: «*[…] GAFAM adopt different models […]. However, it is possible to identify a common element […]. In short, the essence of GAFAM resides in the search, compilation and management of Big Data*».

[7] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., pp. 10-11.

[8] *Ibid.*, p. 10.

sui dati («*data-driven*») sono caratterizzati da una maggior produttività [9]. Ma si potrebbero citare, *inter alia*, anche i settori automobilistico, energetico e dei servizi finanziari, che fanno ricorso ai dati per prendere le proprie decisioni commerciali tanto di breve quanto di lungo periodo, come evidenziato da un altro studio, pubblicato nel 2019 [10].

Appare dunque evidente come siamo attualmente in presenza di una vera e propria «economia dei dati» («*data economy*»), espressione che più precisamente sta a indicare l'impatto che hanno i dati e il relativo mercato sull'economia nel suo complesso [11]. Calcolarne con esattezza il valore non è affatto agevole [12]. Alcune stime ci permettono tuttavia di capire come esso sia in costante crescita, di anno in anno e in tutto il mondo. Si consideri innanzitutto l'Unione europea: come riportato anche nella Comunicazione della Commissione europea del 10 gennaio 2017 «Costruire un'economia dei dati europea», nel 2014 il valore dell'economia dei dati nell'UE è stato stimato a 257 miliardi di euro, pari all'1,85% del PIL dell'Unione; già nel 2015, tale valore è poi passato a 272 miliardi di euro, ossia l'1,87% del PIL UE, per un incremento annuo del 5,6% [13]. In un successivo documento della Commissione, «*The European Data Market Monitoring Tool*» del 2020, si è poi tentato di calcolare il valore dell'economia dei dati nell'UE senza tener conto del Regno Unito, ovviamente in ragione della Brexit: nonostante ciò, la stima relativa agli altri 27 Stati membri ha comunque sfondato quota 300 miliardi di euro nel 2018, raggiungendo circa 325 miliardi nel 2019 (per un incremento annuo di circa l'8%) e circa 355 miliardi nel 2020 (per un incremento annuo di oltre il 9%) [14]. In uno studio ancor più recente, il c.d. «*European Data Market Study 2021-2023*» del febbraio 2023, la stessa Commissione ha aggiornato ulteriormente le stime: il valore dell'economia dei dati UE avrebbe superato i 450 miliardi nel 2021 e sfiorato i 500 miliardi nel 2022 (per un incremento annuo del 9% circa) [15]. L'economia dei dati rappresenterebbe

---

[9] E. Brynjolfsson-K. McElheran, *Data in Action: Data-Driven Decision Making in U.S. Manufacturing*, U.S. Census Bureau Center for Economic Studies Working Paper 16-06, Washington DC, Gennaio 2016.

[10] E. Hughes-Cromwick-J. Coronado, *The Value of US Government Data to US Business Decisions*, *in Journal of Economic Perspectives*, 2019, Volume 33, Numero 1, pp. 131-146.

[11] UE, Commissione europea, *The European Data Market Monitoring Tool – Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories – D2.9 Final Study Report*, 2020, p. 7; UE, Commissione europea, *European Data Market Study 2021-2023 – D2.4 Second Report on Facts and Figures*, 2023, p. 20.

[12] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., p. 9.

[13] UE, Comunicazione della Commissione europea, *Costruire un'economia dei dati europea*, cit., § 1.

[14] UE, Commissione europea, *The European Data Market Monitoring Tool*, cit., p. 39, secondo cui: «*[…] The new estimations of the Data Economy see the value of 2019 for EU27 to be more than 325 Billion Euro and reaching nearly 355 Billion Euro in 2020, growing at 9.3% […]*».

[15] UE, Commissione europea, *European Data Market Study 2021-2023*, cit., p. 20, secondo cui: «*[…] The value of the data economy for the EU27 has been estimated to reach more than €*

dunque una fetta del PIL dell'Unione sempre più prossima al 4% [16]. Il documento prova, inoltre, a formulare delle previsioni per il 2030: in base a queste ultime, in tale anno il valore della *data economy* nell'UE sarà incredibilmente vicino a 1 bilione di euro, ovvero quasi il 6% del PIL dell'Unione [17]. Tutte cifre che, è bene precisarlo, sono oggetto di costante studio e aggiornamento da parte della Commissione europea, attualmente nell'ambito del c.d. *«European Data Market Study 2024-2026»* [18].

L'economia dei dati è però in costante espansione pure negli altri Paesi del mondo, a partire ovviamente dagli Stati Uniti. Questi ultimi (come si può peraltro intuire anche da alcuni esempi poc'anzi riportati) hanno abbracciato la rivoluzione dei dati più rapidamente ed efficacemente di chiunque altro, e, anche grazie all'apporto delle *big tech* summenzionate, il loro primato appare al momento difficilmente contrastabile: pur essendovi alcune difficoltà nell'effettuare raffronti precisi [19], già «*The European Data Market Monitoring Tool*» del 2020 evidenziava che negli USA l'economia dei dati rappresentava una fetta del PIL grande più del doppio rispetto alla corrispondente fetta nell'Unione europea, così come pressoché doppio risultava essere pure l'incremento annuo [20]. Ma, al di là dell'eccezionale caso statunitense, il fenomeno in questione è riscontrabile ovunque, dal Brasile [21] al Giappone [22] passando per la Cina [23].

Insomma: in tutto il mondo, la *data economy* costituisce una parte importantissima della ricchezza, cresciuta enormemente negli ultimi tempi e destinata a farlo in modo sempre più vertiginoso negli anni a venire. Una crescita, *ça va sans dire*, che va di pari passo con l'incessante sviluppo e la progressiva diffusione

---

450 billion in 2021 […]. In 2022, the data economy will reach the threshold of €500 billion, with an annual growth of 8.7% on 2021 […]».

[16] *Ibid*., secondo cui: «*[…] The estimated share of both direct and indirect impacts on GDP in the EU27 ranges from 3.7% in 2021 to 3.9% in 2022 […]*».

[17] *Ibid*., p. 21, secondo cui: «*[…] In 2030, the data economy for the EU27 is expected to remain slightly below the €1 trillion threshold […]. One of the main results is that […] the share of the data economy as a part of GDP in the EU27 will increase […] to 5.7% in 2030 […]*».

[18] UE, Commissione europea, *The European Data Market Study 2024-2026 - D1 Inception Report*, 2024, p. 11.

[19] UE, Commissione europea, *The European Data Market Monitoring Tool*, cit., p. 68, secondo cui: «*[…] The Data Economy for […] U.S. has been measured in terms of direct and indirect impacts only due to lack of comparable and consistent statistical sources […]*».

[20] *Ibid*., secondo cui: «*[…] even if confined to direct and backward indirect impacts, the U.S. Data Economy represents a share in terms of GDP that is more than double the one of the EU […] with a year-on-year growth that, again, is twice as much than in the EU […]*». Sul punto v. anche: UE, Commissione europea, *European Data Market Study 2021-2023*, cit., pp. 146-147.

[21] UE, Commissione europea, *The European Data Market Monitoring Tool*, cit., pp. 43-44; UE, Commissione europea, *European Data Market Study 2021-2023*, cit., 149-151.

[22] UE, Commissione europea, *The European Data Market Monitoring Tool*, cit., pp. 44-45; UE, Commissione europea, *European Data Market Study 2021-2023*, cit., 151-152.

[23] UE, Commissione europea, *European Data Market Study 2021-2023*, cit., 147-148.

di tecnologie sempre più efficienti basate sull'acquisizione, l'immagazzinamento e l'elaborazione di grandi quantità di dati [24]: si pensi, a titolo esemplificativo, a soluzioni quali il *Cloud Computing* [25] e l'*Internet of Things* [26]. Una menzione specifica, inoltre, deve essere riservata alle tecnologie di intelligenza artificiale (IA), che come noto stanno recentemente ricevendo una particolare attenzione da parte dei regolatori [27], in quanto destinate a cambiare le regole del gioco in numerosissimi settori [28]. Orbene, non si deve dimenticare che il carburante di quegli algoritmi di IA che pervadono ormai le nostre vite è rappresentato proprio dai dati: un'ulteriore circostanza che contribuisce – e contribuirà – a rendere questi ultimi sempre più imprescindibili sul piano commerciale [29].

---

[24] M.C. Meneghetti, *I trasferimenti di dati personali all'estero*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 594-661, spec. pp. 599-600.

[25] Il *Cloud Computing* consiste generalmente in una serie di tecnologie e modelli di servizio incentrati sull'uso e sulla fornitura di applicazioni informatiche, capacità di elaborazione, di archiviazione e spazio di memoria basati su Internet. In dottrina, sul punto, v. *inter alios*: M.C. Meneghetti, *op. cit.*, p. 599.

[26] Il termine *Internet of Things* indica quella categoria di oggetti reali che, attraverso sensori, non solo sono in grado di interagire con il mondo circostante raccogliendo ed elaborando informazioni, ma attraverso la capacità di connettersi ad Internet, possono anche trasferire informazioni e comunicare tra di loro, diventando veri e propri «oggetti intelligenti». In dottrina, sul punto, v. *inter alios*: M.C. Meneghetti, *op. cit.*, pp. 599-600.

[27] In materia di intelligenza artificiale, come noto, l'Unione europea ha recentemente adottato il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio *che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*, 13 giugno 2024, GU L, 12 luglio 2024. L'art. 3, n. 1), del Regolamento definisce un «sistema di IA» come segue: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Si coglie l'occasione per precisare che, tuttavia, il suddetto Regolamento e la tematica dell'intelligenza artificiale non saranno oggetto della presente trattazione.

[28] Sul punto v., *inter alios*: M. Burri, *Creating Data Flow Rules through Preferential Trade Agreements*, in A. Chander-H. Sun (a cura di), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, New York, 2023, pp. 264-291, spec. p. 264, in cui l'intelligenza artificiale viene definita come un vero e proprio «*game changer*».

[29] Sul rapporto tra intelligenza artificiale e commercio v., *inter alios*: K. Irion-J. Williams, *Prospective Policy Study on Articial Intelligence and EU Trade Policy*, Institute for Information Law (IViR), Amsterdam, 2019; A. Chander, *Artificial Intelligence and Trade*, in M. Burri (a cura di), *Big Data and Global Trade*, Cambridge University Press, Cambridge, 2021, pp. 115-127; S. Yakovleva-J. Van Hoboken, *The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade*, Institute for Information Law Research Paper No. 2022-10, Amsterdam, 2022.

2. *L'importanza, nell'economia dei dati, dei flussi transfrontalieri degli stessi*

In un'economia che si rivela, a livello mondiale, sempre più legata ai dati, è facile comprendere come un elemento chiave sia rappresentato dal fatto che una quantità significativa di tali dati deve poter circolare liberamente, e ciò non solo all'interno dei confini degli Stati, ma anche al di là delle frontiere nazionali [30]. La presente trattazione vuole dunque concentrarsi non su ogni questione giuridica rientrante nella galassia dell'economia dei dati, operazione che risulterebbe pretenziosa e impossibile vista l'incredibile ampiezza dell'argomento, ma esclusivamente su quest'ultimo aspetto (anzi, come si vedrà, su determinati profili ancor più specifici di esso).

I flussi transfrontalieri di dati («*cross-border data flows*») procurano incredibili benefici, *in primis*, a quelle che sono state precedentemente definite come «*data-enabled businesses*», ovvero le imprese per cui i dati rappresentano la risorsa più preziosa e che senza gli stessi neppure esisterebbero. Si pensi, ad esempio, al fatto che le piattaforme *online* (come le menzionate Uber, Airbnb, e molte altre) si affidano ai trasferimenti internazionali di dati per fornire i loro servizi digitali a livello globale; allo stesso tempo, esse raccolgono dati riguardanti le transazioni e i comportamenti dei consumatori in vari luoghi del mondo, e tali dati devono poi essere trasmessi oltrefrontiera al fine di essere conservati, aggregati e analizzati [31].

Ma non deve essere sottovalutato il fatto che i flussi internazionali di dati sono almeno altrettanto importanti per le attività di tipo tradizionale, quelle che abbiamo chiamato «*data-enhanced businesses*»: *inter alia*, le aziende minerarie, le catene di negozi alimentari, le banche, le industrie automobilistiche fanno ormai affidamento sulla possibilità di trasferire i dati al di là dei confini e di analizzarli in tempo reale, circostanza da cui traggono grandi benefici le loro catene di approvvigionamento, le loro operazioni, i loro modelli commerciali [32].

Vi è poi un ulteriore elemento da aggiungere: i flussi internazionali di dati, infatti, non sono importanti solo per le grandi società, che siano «*data-enabled*» o «*data-enhanced*». Essi rappresentano un fattore di sviluppo anche per le piccole e medie imprese, che sono sempre più coinvolte nel commercio digitale [33]. Rile-

---

[30] Sul punto v., *inter alios*: R.D. Atkinson, *International Data Flows: Promoting Digital Trade in the 21st Century*, Testimony Before the U.S. House Judiciary Committee – Subcommittee on Courts, Intellectual Property and the Internet, 3 novembre 2015, p. 3.

[31] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., p. 26.

[32] Sull'importanza dei flussi oltrefrontiera di dati anche per le imprese più tradizionali v.: D. Castro-A. McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, Information Technology & Innovation Foundation, Febbraio 2015. Lo studio porta come esempi la società mineraria anglo-australiana Rio Tinto, la catena di negozi di generi alimentari Tesco, la banca olandese ING, nonché la casa automobilistica svedese Volvo. Su quest'ultima v. anche: M. Rentzhog-H. Jonströmer, *No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, Kommerskollegium, Stoccolma, Gennaio 2014, p. 35.

[33] R.D. Atkinson, *op. cit.*, p. 6.

vante sul punto è un contributo del 2014, secondo cui, già all'epoca, facevano ricorso all'analisi dei dati circa il 60% delle imprese europee e statunitensi con 50 o meno dipendenti [34]: facile capire come i *cross-border data flows* possano giocare per simili aziende un ruolo significativo.

Per permettere di comprendere al meglio la portata del fenomeno planetario dei flussi transfrontalieri di dati, si ritiene opportuno anche in questo caso, come si è fatto in precedenza, riportare alcuni numeri. Sul piano del volume, uno studio del 2019 stima che a livello globale i menzionati flussi abbiano superato, già nel 2017, i 700 Tbps, ovvero *terabit* al secondo (si ricorda che 1 *terabit* corrisponde a circa 1 bilione di *bit*, unità di misura dell'informazione); ciò significa che, dal 2005 a tale anno, i flussi in questione sono aumentati di ben 148 volte [35]. Una ricerca ancor più recente, segnatamente del 2022, calcola invece che tra il 2010 e il 2019 essi hanno registrato un tasso di crescita annuo pari al 45%, arrivando a circa 1.500 *terabit* al secondo [36].

Simili numeri, ancorché impressionanti, non rivelano però molto circa il valore economico dei *cross-border data flows*. A tal riguardo si può dunque prendere in considerazione un altro studio, del 2016: quest'ultimo mostrava preliminarmente come, in quel momento, i flussi internazionali di merci, investimenti esteri diretti e dati, unitamente considerati, determinassero un incremento del PIL mondiale di circa il 10% rispetto a quello che si sarebbe verificato in un pianeta senza alcun flusso. Si era stimato che, nel solo 2014, tale valore fosse di quasi 8 bilioni di dollari. Lo studio evidenziava come i flussi internazionali di dati rappresentassero quasi 3 bilioni di tale effetto, esercitando sulla crescita un impatto superiore rispetto a quello dei tradizionali scambi transfrontalieri di merci. Si tratta, ovviamente, di uno sviluppo sensazionale, soprattutto alla luce del fatto che quello dei *cross-border data flows* è un fenomeno affermatosi relativamente di recente [37], che non può far altro che continuare a espandersi

---

[34] V. Espinel, *Executive Survey Shows the Benefits of Data Innovation Across the Whole Economy*, in *BSA Tech Post*, 10 dicembre 2014, secondo cui: «*[…] We commissioned Ipsos Public Affairs to poll 1,500 senior executives and business decision-makes across the United States and Europe about the role of data analytics in their companies. We found a number of things that were surprising: […] data analytics are important to companies of all types and sizes – including an overwhelming majority (60 percent) of small businesses with 50 or fewer employees […]*».

[35] McKinsey Global Institute, *Globalization in Transition: The Future of Trade and Value Chains*, McKinsey&Company, Gennaio 2019, p. 72, secondo cui: «*[…] From 2005 to 2017, the amount of cross-border bandwidth in use grew 148 times larger […]*».

[36] McKinsey Global Institute, *Global flows: The ties that bind in an interconnected world*, McKinsey&Company, Novembre 2022, p. 4, secondo cui: «*Between 2010 and 2019, cross-border data flows increased at a staggering 45 percent annual rate, growing from about 45 to 1,500 terabits per second*».

[37] McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, McKinsey&Company, Marzo 2016, p. 1, secondo cui: «*[…] Our econometric research indicates that global flows of goods, foreign direct investment, and data have increased current global GDP by roughly 10 percent compared to what would have occurred in a world without any flows. This*

drasticamente nei prossimi anni. Per completezza si vuole, inoltre, menzionare un documento ancora precedente (datato 2009) della Conferenza delle Nazioni Unite sul commercio e lo sviluppo («*United Nations Conference on Trade and Development*», o UNCTAD), il quale rilevava come, addirittura nel 2007, circa il 50% degli scambi di servizi a livello globale fosse consentito dalle nuove tecnologie e dai trasferimenti internazionali di dati, percentuale destinata chiaramente a crescere in modo ulteriore [38].

Per riassumere in breve, e semplificare, tutti gli elementi fin qui esposti permettono di evidenziare quanto i flussi transfrontalieri di dati siano rilevanti nell'odierna economia mondiale, per tutti i tipi di azienda. Già oggi, tali flussi hanno un'importanza notevolissima, non solo sul piano del loro volume, ma anche (e soprattutto) su quello del loro valore economico. Ma ciò che, forse, conta ancora di più è il fatto che tali flussi sono destinati ad aumentare in modo esponenziale di anno in anno, fenomeno peraltro strettamente connesso al rapido sviluppo delle tecnologie di cui già si è detto sopra, come le applicazioni di intelligenza artificiale: esse, necessitando di una significativa mole di dati, richiedono anche che i medesimi possano spostarsi facilmente oltre i confini [39].

3. *La particolarità, tra i flussi transfrontalieri di dati, di quelli riguardanti i dati* personali

Come si è anticipato, tuttavia, la presente trattazione non intende prendere in considerazione tutti i flussi transfrontalieri, ma solo quelli che coinvolgono una particolare tipologia di dati. Occorre infatti ricordare, in via preliminare, che i dati possono essere ripartiti in varie categorie. A titolo esemplificativo, una possibile classificazione è quella che distingue tra i dati protetti da diritti di proprietà intellettuale (o da qualsiasi altro diritto avente un effetto analogo), e i dati di dominio pubblico, che al contrario non godono di una simile prote-

---

value was equivalent to $7.8 trillion in 2014 alone. Data flows account for $2.8 trillion of this effect, exerting a larger impact on growth than traditional goods flows. This is a remarkable development given that the world's trade networks have developed over centuries but cross-border data flows were nascent just 15 years ago […]».

[38] UNCTAD, *Information Economy Report 2009 – Trends and Outlook in Turbulent Times*, United Nations Publication, New York/Ginevra, 2009, p. 77. Sul punto v. anche: D. CASTRO-A. MCQUINN, *op cit.*, p. 1, secondo cui: «*[…] the United Nations Conference on Trade and Development (UNCTAD) estimates that about 50 percent of all traded services are enabled by the technology sector, including by cross-border data flows […]*».

[39] Sul punto v., *inter alios*: F.J. SCHWEITZER-I. SACCOMANNO-N.N. SAIKA, *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade – Part 1*, in *The Global Trade Law Journal*, 2024, Volume 1, Numero 2, pp. 103-118, spec. p. 104, secondo cui: «*[…] Cross-border data flows are even more important now with the rapid growth of new AI applications, which depend on massive amounts of data […]*».

zione [40]. Si potrebbe rammentare poi la suddivisione tra dati che sono generati da macchine, e dati che non lo sono [41]. Ma per le imprese è rilevante anche la ripartizione tra dati interni, ovvero raccolti dai diversi rami dell'azienda, e dati esterni, cioè ottenuti da fonti che sono al di fuori rispetto all'impresa stessa [42].

Tuttavia, la distinzione più rilevante, ai nostri fini e non solo, è indubbiamente quella tra dati personali e dati non personali. In particolare, a livello internazionale e fin da quando ha avuto origine l'interesse per la materia (come si vedrà), il «dato personale» («*personal data*») è stato costantemente inteso come qualsiasi informazione riguardante una persona fisica identificata o identificabile, la quale prende il nome di persona interessata («*data subject*»): una simile definizione è stata fornita nell'ambito di varie organizzazioni internazionali, come l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE o anche OECD, ovvero *Organization for Economic Co-operation and Development*) [43], il Consiglio d'Europa (di seguito anche CoE, i.e. *Council of Europe*) [44], e l'Unione

---

[40] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., p. 22, secondo cui la nozione di «*Proprietary data*», definita come «*Data with clearly defined ownership that is protected by Intellectual Property Rights or any other rights with a similar effect […]*», si contrappone a quella di «*Open data (or public domain data)*», definita come «*Data that is publicly available (as opposed to proprietary data), free to use by anyone for any purpose without any legal restrictions. It is not protected by Intellectual Property Rights, copyrights or any other similar legal rights […]*».

[41] *Ibid*., secondo cui la nozione di «*Machine generated data*», definita come «*Machine generated data, e.g. machine-to-machine communication (M2M); Internet of Things (IoT), i.e. data collected from sensors*», si contrappone a quella di «*User created data*», definita come segue: «*User created data is data that has been made available by an individual (e.g. telemetry tracking data, consumer behaviour data collected through mobile apps or social media posts). This can be volunteered data (i.e. "active"), observed data (i.e. "passive" or "implicit"), or derived data about a user […]*». Sul punto, v. anche: UE, Comunicazione della Commissione europea, *Costruire un'economia dei dati europea*, cit., § 3.1, secondo cui «[…] I dati generati da macchine sono prodotti da processi, applicazioni o servizi informatici, senza intervento umano diretto, oppure da sensori che trattano informazioni provenienti da apparecchiature, software o macchine, virtuali o reali […]».

[42] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, cit., pp. 22-23, secondo cui da un lato vi è la nozione di «*Internal data*», definita come segue: «*Internal data is data that collected and consolidated from different branches within a business. For example, lists of purchase orders from the sales department, transactions from accounting or any other internal source which is responsible for recording information about a business' commercial interaction*s»; dall'altro, vi è la nozione di «*External data*», definita come segue: «*External data is data not collected internally, but rather obtained from a source outside of company - for instance, by purchasing access to a proprietary database. This could be acquired data as well*».

[43] Sul punto, v.: OECD, *Annex to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL]*, 23 settembre 1980, par. 1, in base a cui: «*For the purposes of these Guidelines: […] b) "personal data" means any information relating to an identified or identifiable individual (data subject) […]*»; OECD, *Annex to the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, as amended by C(2013)79]*, 11 luglio 2013, par. 1, in base a cui: «*For the purposes of these Guidelines: […] b) "Personal data" means any information relating to an identified or identifiable individual (data subject) […]*».

[44] Sul punto, v.: CoE, *Convention for the Protection of Individuals with regard to Automatic*

europea [45]. Viceversa, è non personale qualsiasi dato che non rientri in tale categoria [46], come ad esempio un dato anonimo [47]. La presente trattazione intende occuparsi solo ed esclusivamente dei flussi transfrontalieri che coinvolgono la prima delle due menzionate tipologie, quella dei dati personali [48].

Non si tratta di una scelta casuale. Da un lato, i dati personali sono di importanza fondamentale per l'attività di un'impresa. Sono tali dati che le consentono, ad esempio, di pronosticare il comportamento di una persona: se si hanno informazioni su come quest'ultima ha agito in passato, sarà infatti possibile effettuare previsioni sulla reiterazione di tale condotta in futuro, previsioni che diventeranno sempre più accurate all'aumentare dei dati a disposizione. E, come appare evidente, prevedere la reiterazione di un comportamento noto dell'individuo, anche molto ricco di sfaccettature, può dare un incredibile vantaggio all'impresa: essa sarà così in grado di costruire un contesto digitale ricorrente in cui "dare appuntamento" alla persona, essendo certa di trovarla per offrirle prima degli altri beni e servizi connessi al comportamento reiterato. Si tratta di una possibilità che è già rilevante in molti ambiti, che lo sarà sempre di più, e che permette di capire quanto possano essere preziosi i dati personali dal punto

---

Processing of Personal Data (ETS No. 108), Strasburgo, 28 gennaio 1981, art. 2 («*Definitions*»), in base a cui: «*For the purposes of this Convention: a) "personal data" means any information relating to an identified or identifiable individual ("data subject")*»; CoE, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, Elsinore, 18 maggio 2018, art. 2 («*Definitions*»), in base a cui: «*For the purposes of this Convention: a) "personal data" means any information relating to an identified or identifiable individual ("data subject") […]*».

[45] Sul punto, v.: UE, Direttiva 95/46/CE del Parlamento europeo e del Consiglio *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, 24 ottobre 1995, GU L 281, 23 novembre 1995, pp. 31-50, art. 2 («Definizioni»), in base a cui: «Ai fini della presente direttiva si intende per: a) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata») […]»; UE, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio *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)*, 27 aprile 2016, GU L 119, 4 maggio 2016, pp. 1-88, art. 4 («Definizioni»), in base a cui: «Ai fini del presente regolamento s'intende per: 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») […]».

[46] Sul punto v.: UE, Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*, 14 novembre 2018, GU L 303, 28 novembre 2018, pp. 59-68, art. 3 («Definizioni»), in base a cui: «Ai fini del presente regolamento si intende per: 1) «dati»: i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679 […]».

[47] UE, Regolamento (UE) 2016/679, cit., Considerando 26.

[48] Rimane, di conseguenza, completamente estranea alla presente trattazione la disciplina dettata dall'UE all'interno del Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*, 14 novembre 2018, GU L 303, 28 novembre 2018, pp. 59-68. Neppure i dati anonimi sono dunque oggetto di esame.

di vista economico [49]. Ma anche al di là di tale ipotesi, si può evidenziare più in generale come per la vita di un'azienda i dati personali di clienti, fornitori, partner commerciali o dipendenti risultino indispensabili. È naturale dunque che questa possa avere la necessità di trattarli e, in alcuni casi, anche di trasferirli oltrefrontiera.

Dall'altro lato, trattandosi per l'appunto di dati riferibili a una persona fisica (identificata o comunque identificabile), il loro trattamento e trasferimento fa sorgere problemi di tutela della stessa: rischiano infatti di essere intaccati alcuni suoi diritti consacrati in strumenti giuridici di vario rango, in particolare i diritti alla *privacy* e alla protezione dei dati di carattere personale. Si presti attenzione al fatto che quelli appena menzionati sono a tutti gli effetti due diritti distinti, che non devono essere confusi, e menzionarli entrambi è tutt'altro che un'inutile ripetizione. Giova anzi, a questo punto della trattazione, soffermarsi sul loro significato e sulle differenze intercorrenti tra gli stessi.

4. *I diritti che richiedono tutela: il diritto alla* privacy *e quello alla protezione dei dati personali*

Partendo dal diritto alla *privacy*, o alla vita privata, o alla riservatezza [50], esso consiste fondamentalmente nell'escludere altri dalla conoscenza di vicende strettamente personali e familiari, mantenendo riservate alcune informazioni. Si tratta dunque di un diritto a contenuto negativo [51]. Dal punto di vista storico, le sue radici vengono generalmente ricondotte al celeberrimo articolo «*The Right to Privacy*», scritto dai giuristi statunitensi Samuel D. Warren e Louis D. Brandeis sulla *Harvard Law Review* alla fine del XIX secolo, in cui si faceva riferimento

[49] G. D'Acquisto-F. Pizzetti, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi Giuridica dell'Economia*, Giugno 2019, Numero 1, giugno 2019, pp. 89-108, spec. p. 102. Sul punto v. anche, *inter alios*: M.C. Meneghetti, *op. cit.*, p. 601.

[50] A onor del vero, si segnala come si possa cercare di distinguere ulteriormente anche tali nozioni. A titolo meramente esemplificativo, sulle differenze storiche tra «vita privata» e «*privacy*», v.: G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht, 2014, p. 80 ss.. Sempre sulla differenza tra «vita privata» e «*privacy*», v. anche la pagina del sito del Consiglio d'Europa dedicata al «Diritto al rispetto della vita privata e familiare», consultabile al seguente link: *https://www.coe.int/it/web/echr-toolkit/le-droit-au-respect-de-la-vie-privee-et-familiale* (ultimo accesso in data 31 dicembre 2024), in cui si può leggere: «[…] "Vita privata" ha un significato più ampio della privacy […]». Non è tuttavia questa la sede per approfondire tali possibili distinzioni. Conseguentemente, nella presente trattazione, le espressioni «vita privata», «*privacy*» e «riservatezza» verranno utilizzate indifferentemente per indicare i medesimi concetti.

[51] G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 1-26, spec. p. 13.

al «*right to be let alone*», inteso come riconoscimento dell'inviolabilità della sfera personale e della propria vita privata [52]. Il riconoscimento giuridico del diritto alla *privacy* è però arrivato dopo un lungo e travagliato processo, in cui un ruolo fondamentale è stato ricoperto dalla giurisprudenza: l'opera dei giudici, infatti, non solo ha sollecitato fortemente il dibattito dottrinale sul punto, ma ha anche portato la materia all'attenzione dei legislatori, contribuendo così alla piena affermazione e alla tutela del diritto in questione. Questo è quanto è accaduto non solo negli USA, che essendo caratterizzati da un ordinamento di *common law* attribuiscono notoriamente alla giurisprudenza una posizione di grande rilievo, ma anche in ordinamenti europei di *civil law* [53]. A titolo esemplificativo, in Italia è stata di notevole importanza la sentenza pronunciata nel 1975 nell'ambito del caso c.d. Soraya dalla Corte di Cassazione [54], che poi è tornata sul punto anche successivamente [55].

Il diritto alla *privacy* trova inoltre riconoscimento in numerose fonti a livello internazionale. Innanzitutto, lo si trova nell'art. 12 della Dichiarazione universale dei diritti dell'uomo («*Universal Declaration of Human Rights*»), adottata dall'Assemblea generale delle Nazioni unite nel 1948 [56], nonché nell'art. 17 del Patto internazionale sui diritti civili e politici («*International Covenant on Civil and Political Rights*»), adottato nel 1966 sempre dall'Assemblea generale ONU [57]. Prendendo invece in considerazione più nello specifico il contesto europeo, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), firmata nel 1950 in seno al Consiglio d'Europa, dedica al diritto al rispetto della vita

---

[52] S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 15 dicembre 1890, Volume 4, Numero 5, pp. 193-220.

[53] L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in *Diritti comparati. Comparare i diritti fondamentali in Europa*, 4 dicembre 2014, p. 5.

[54] Cassazione italiana, sentenza del 27 maggio 1975, n. 2129, secondo cui: «[…] Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti […]».

[55] Cassazione italiana, sentenza del 9 giugno 1998, n. 5658, secondo cui le vicende oggetto della riservatezza si riferiscono «[…] ad una certa sfera della vita individuale e familiare, all'illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato alle mura domestiche […]».

[56] UN General Assembly, *Universal Declaration of Human Rights*, Parigi, 10 dicembre 1948, art. 12, in base a cui: «*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*».

[57] UN General Assembly, *International Covenant on Civil and Political Rights*, New York, 16 dicembre 1966, art. 17, in base a cui: «*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks*».

privata e familiare il suo art. 8 [58]. Infine, è assolutamente necessario menzionare la Carta dei diritti fondamentali dell'Unione europea (nota anche come Carta di Nizza) [59], solennemente proclamata il 7 dicembre 2000 e avente dal 1° dicembre 2009 lo stesso valore giuridico dei trattati UE (come si dirà meglio *infra*), l'art. 7 della quale è anch'esso dedicato al «Rispetto della vita privata e della vita familiare» e reca il seguente contenuto: «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

Come già anticipato, diverso dal diritto alla vita privata è invece il diritto alla protezione dei dati personali. Se il primo ha contenuto esclusivamente negativo e si esaurisce nell'escludere l'interferenza altrui, il secondo ha al contrario contenuto positivo: consiste infatti nel diritto del soggetto cui i dati si riferiscono di esercitare un controllo attivo su detti dati, attraverso l'utilizzo di determinati poteri [60]. Nel panorama internazionale, tale diritto è stato introdotto con la Carta dei diritti fondamentali UE, che dedica alla «Protezione dei dati di carattere personale» il suo art. 8, e dunque una posizione distinta e autonoma rispetto a quella del diritto al rispetto della vita privata e familiare [61].

Quello dell'art. 8 Carta di Nizza può dunque apparire come un diritto fondamentale innovativo [62], poiché in quanto tale si manifesta per la prima volta proprio in questo contesto. Tuttavia, a ben vedere, non è poi così nuovo [63]. Esso, come si evince dalla relativa disposizione, presenta sei elementi costitutivi: i) il rispetto del «principio di lealtà» nel trattamento dei dati; ii) la necessità che i dati siano trattati «per finalità determinate»; iii) la necessità di un «fondamento legit-

---

[58] CoE, *Convention for the Protection of Human Rights and Fundamental Freedoms*, Roma, 4 novembre 1950, art. 8 («*Right to respect for private and family life*»), in base a cui: «*1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*».

[59] UE, *Carta dei diritti fondamentali dell'Unione europea*, GU C 202, 7 giugno 2016, pp. 389-405.

[60] G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 10.

[61] UE, *Carta dei diritti fondamentali dell'Unione europea*, cit., art. 8 («Protezione dei dati di carattere personale»), in base a cui: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[62] G. Braibant, *La Charte des Droits fondamentaux de l'Union européenne*, Editions du Seuil, Parigi, 2001, p. 47.

[63] N. Bernsdorff, *Kapitel II, Freiheiten: Artikel 6 Bis 19*, in J. Meyer (a cura di), *Kommentar zur Charta der Grundrechte der Europäischen Union*, Nomos Verlagsgesellschaft, Baden-Baden, 2003, pp. 135-262, spec. p. 160.

timo» del trattamento, che può essere rappresentato dal consenso, ma la legge può prevederne anche altri; iv) il diritto di accesso ai dati personali; v) il diritto alla rettifica dei dati personali; vi) il controllo di un'autorità indipendente [64]. Orbene, gli elementi chiave del diritto alla protezione dei dati personali appena menzionati, in realtà, affondano le proprie radici in strumenti di diritto dell'UE e di diritto internazionale precedentemente esistenti, come illustrato anche nelle «Spiegazioni relative alla Carta dei diritti fondamentali» [65]. I principali capisaldi di tali strumenti, elaborati negli ultimi 4-5 decenni, sono quindi confluiti nell'art. 8 della Carta di Nizza, e devono essere ora tutelati in qualità di componenti di un diritto fondamentale il quale merita protezione di per sé [66]; una qualifica, quella di "fondamentale", che comporta condizioni particolarmente stringenti alle limitazioni di un diritto, le quali devono in ogni caso rispettarne l'essenza [67].

Occorre inoltre sottolineare come il diritto alla protezione dei dati personali si affianchi sempre più spesso al diritto alla vita privata, arrivando talvolta persino a sostituirlo quasi del tutto. Ciò è particolarmente evidente negli strumenti di diritto UE, soprattutto in quello che ad oggi può essere considerato come il principale punto di riferimento in materia: ci si riferisce ovviamente al noto Regolamento (UE) 2016/679 «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)», ancor meglio conosciuto come GDPR («*General Data Protection Regulation*»). Esso si pone in modo pressoché esclusivo come uno strumento a tutela del «diritto alla protezione dei dati personali» [68], mentre del diritto alla vita privata rimangono scarsissime tracce [69]: proprio per questo, certa dottrina

---

[64] G. González Fuster, *op. cit*, p. 204.

[65] UE, *Spiegazioni relative alla Carta dei diritti fondamentali*, GU C 303, 14 dicembre 2007, pp. 17-35.

[66] B. Docquir, *Le droit à la vie privée*, De Boeck-Larcier, Bruxelles, 2008, p. 41.

[67] Sul punto v., *inter alios*: K. Lenaerts, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, 2019, Volume 20, Numero 6, pp. 779-793. Sul punto v. anche la pagina del sito della Commissione europea dedicata a «*fundamental rights*», consultabile al seguente link: *https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/fundamental-rights_en#:~:text=Fundamental%20rights%20define%20what%20individuals,while%20some%20rights%20are%20qualified* (ultimo accesso in data 31 dicembre 2024).

[68] UE, Regolamento (UE) 2016/679, cit., art. 1 («Oggetto e finalità»), par. 2, in base a cui: «Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali».

[69] Il diritto alla vita privata, nel Regolamento (UE) 2016/679, viene menzionato solo nel Considerando 4, in cui però viene messo sullo stesso piano di diversi altri diritti. Tale Considerando, infatti, recita come segue: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fonda-

è arrivata addirittura a parlare di «*Privacy (Almost) Gone*»[70].

Ma la progressiva affermazione del diritto alla protezione dei dati personali si può riscontrare a livello internazionale pure in strumenti giuridici di altre organizzazioni. In particolare merita di essere menzionata, nell'ambito del Consiglio d'Europa, la c.d. «Convenzione 108+» (ovvero la versione modernizzata della Convenzione 108), datata 2018, ma a onor del vero non ancora entrata in vigore. Se nella versione originaria della Convenzione 108, quella del 1981, si faceva riferimento solo al «*right to privacy*»[71], in quella del 2018 subentra infatti anche il «*right to protection of personal data*»[72].

Ricapitolando: il diritto alla *privacy*, più risalente nel tempo, si limita a escludere l'interferenza altrui e a offrire una tutela che possiamo definire "negativa", "statica"; il diritto alla protezione dei dati personali, affermatosi soprattutto negli ultimi decenni, si concretizza invece in poteri di controllo e di intervento: la tutela da esso offerta è dunque "positiva", "dinamica", dal momento che segue i dati nella loro circolazione[73]. Per comprendere ancora meglio l'essenza di quest'ultimo diritto, sviluppatosi come abbiamo visto specialmente in Europa, può essere utile prendere in considerazione in modo rapido la sua versione sudamericana, e soprattutto la significativa denominazione a esso attribuita, ovvero «*habeas data*»: si tratta di una formula che riecheggia, ovviamente, la celeberrima locuzione «*habeas corpus*», il cui significato è «abbi il (tuo) corpo» o ancora meglio «abbi il controllo del tuo corpo»; allo stesso modo, con «*habeas data*» si intende proprio «abbi il controllo dei tuoi dati»[74]. La versione europea

---

mentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[70] G. González Fuster, *op. cit*, pp. 242-245, in cui si afferma anche che: «*[…] The removal of privacy is nonetheless almost complete […]*».

[71] CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981, cit., art. 1 («*Object and Purpose*»), in base a cui: «*The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*».

[72] CoE, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, 2018, cit., art. 3 («*Scope*»), in base a cui: «*1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data […]*».

[73] Sul punto v.: S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e diritto privato*, 2004, Numero 1, pp. 1-12, spec. p. 3; S. Rodotà, *Data Protection as a Fundamental Right*, in S. Gutwirth-Y. Poullet-P. De Hert-C. De Terwangne-S. Nouwt (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 77-82, spec. pp. 79-80.

[74] M.A. Ekmekdjian-C. Pizzolo, *Hábeas data: El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996, p. 2.

di tale diritto è andata senz'altro ancora oltre, non comprendendo solo i diritti di accesso e rettifica, ma anche (come si è visto dai sei "elementi chiave" sopra elencati) una serie di obblighi per chi tratta i dati altrui, il c.d. «titolare del trattamento», nonché il controllo di un'autorità indipendente [75]. Ma il concetto fondamentale è indubbiamente il medesimo.

Si precisa che, proprio in ragione della continua espansione del diritto alla protezione dei dati personali, esso finirà per essere preso in considerazione, nella presente trattazione, ben più rispetto al diritto alla *privacy*. Al tempo stesso, quest'ultimo non deve mai essere perso di vista: si tratta infatti di due diritti profondamente connessi l'uno all'altro, e districarli risulta del tutto impossibile. A ciò, inoltre, occorre aggiungere che i significati di tali nozioni, nonché i loro rapporti reciproci, sono costantemente in evoluzione: non si può non accettare il fatto che le loro definizioni siano mutevoli e i loro legami instabili [76].

5. *Le tecniche normative astrattamente configurabili per bilanciare le esigenze economiche legate ai flussi transfrontalieri di dati personali con la necessità di tutelare i diritti alla* privacy *e alla protezione dei dati*

Finora si è dunque visto quanto, in un'economia mondiale basata sui dati e sui flussi internazionali degli stessi, i trasferimenti oltrefrontiera di dati personali siano particolarmente importanti per lo svolgimento di attività imprenditoriali di ogni tipo. Al tempo stesso si è anche visto come, riferendosi tali dati a delle persone fisiche, i diritti di queste ultime, e nello specifico il diritto alla vita privata e quello alla protezione dei dati personali, possono essere messi a serio rischio da simili flussi: ciò si verifica, in particolar modo, quando vi è la possibilità che lo Stato di destinazione del trasferimento accordi ai diritti in questione una tutela inferiore rispetto al Paese da cui il flusso ha avuto origine. Tale circostanza fa inevitabilmente sorgere delle preoccupazioni circa le sorti delle informazioni trasmesse e può indurre a prevedere determinati limiti e condizioni a simili trasferimenti.

Proprio per questo sono stati elaborati, a livello sia internazionale che nazionale, strumenti giuridici di vario tipo che hanno come scopo proprio quello di bilanciare le due istanze contrapposte: da un lato, l'esigenza di favorire i *cross-border flows of personal data*, in ragione della loro rilevanza strategica per l'espansione del commercio internazionale; dall'altro lato, la necessità di tutelare i diritti degli individui, segnatamente quelli alla *privacy* e alla *personal data protection*, limitando quegli stessi flussi. Tale opera di bilanciamento, tuttavia, può essere effettuata attraverso tecniche normative che presentano tra di loro significative differenze, perché sono spesso frutto di concezioni dei dati personali

[75] G. González Fuster, *op. cit*, p. 269.

[76] *Ibid*., p. 268.

divergenti e, soprattutto, perché possono determinare esiti diversi del bilanciamento medesimo: in alcuni casi appare privilegiata la prima delle due esigenze menzionate, in altri la seconda [77].

È dunque opportuno, prima di procedere oltre, esaminare quali sono le tecniche normative astrattamente configurabili, raggruppandole in alcune categorie, all'interno delle quali le discipline concretamente adottate possono essere sussunte.

5.1. *Il* «bottom-up regulatory design» *e il* «top-down regulatory design»

Una prima classificazione tra modalità di regolamentazione della materia è quella che distingue l'approccio che taluno ha definito «dal basso verso l'alto», o «*bottom-up regulatory design*», e l'approccio che può essere descritto come «dall'alto verso il basso», o «*top-down regulatory design*» [78].

Alla base del primo approccio risiede una concezione che prende prevalentemente in considerazione il valore economico dei dati personali. In una simile ottica, la protezione degli stessi è strumentale soprattutto a generare nei consumatori quella fiducia che rappresenta un elemento essenziale di qualunque rapporto contrattuale, in particolare là dove ci si trovi nel contesto del commercio elettronico [79]. Come evidenziato da certa dottrina, la fiducia può essere considerata a tutti gli effetti come un bene [80]: in quanto tale, è suscettibile di valutazione economica, ma la sua produzione non può essere lasciata interamente al mercato [81]. L'approccio normativo in questione ha dunque come obiettivo ultimo quello

---

[77] Sulla tensione tra le esigenze del commercio internazionale, da un lato, e i diritti alla *privacy* e alla *personal data protection*, dall'altro, nonché sui possibili strumenti per bilanciare le due istanze contrapposte, v. *inter alios*: M. BURRI, *Interfacing Privacy and Trade,* in *Case Western Reserve Journal of International Law*, 2021, Volume 53, Numero 1, pp. 35-87; A. CHANDER-P.M. SCHWARTZ, *Privacy and/or Trade*, in *The University of Chicago Law Review*, 2023, Volume 90, Numero 1, pp. 49-135.

[78] S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, in *World Trade Review*, Luglio 2018, Volume 17, Numero 3, pp. 477-508, spec. p. 483. Sull'argomento (anche se la terminologia utilizzata è differente) v. anche: C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, Oxford, 2013, p. 76 ss.

[79] S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p 482, secondo cui: «*[…] From an economic perspective, the protection of privacy and personal data is a key building block of consumers' trust in suppliers and more generally of their confidence in electronic commerce […]*».

[80] Sul tema della "mercificazione" della fiducia v., *inter alios*: B. BODÓ, *The Commodification of Trust*, Institute for Information Law (IViR) Research Paper No. 2021-01, Amsterdam, 2021.

[81] G. COHEN, *The Negligence-Opportunism Tradeoff in Contract Law*, in *Hofstra Law Review*, 1992, Volume 20, Numero 4, pp. 941-1016, spec. p. 976, secondo cui: «*[…] trust is an extremely valuable and vulnerable resource, which the market alone cannot be counted on to supply […]*». Sul punto v. anche, *inter alios*: H.B. SCHÄFER-C. OTT, *The Economic Analysis of Civil Law*, Edward Elgar Publishing, Cheltenham, 2000, p. 360.

di correggere un fallimento del mercato [82], ristabilendo la fiducia là dove essa sia assente e permettendo dunque i rapporti commerciali. Al contrario, là dove non sia presente una simile necessità, non vi è alcuna ragione per proteggere i dati personali e imporre restrizioni ai flussi dei medesimi. Essendo frutto di una simile concezione, il «*bottom-up regulatory design*» ha come elemento caratteristico il fatto che si prendono le mosse da una situazione teorica in cui i flussi di dati personali sono sempre consentiti e in cui dunque non è prevista alcuna protezione per tali dati; solo in un momento successivo è possibile incrementare il livello di protezione, limitando i flussi, ma esclusivamente al fine di raggiungere gli obiettivi menzionati (ci si sposta quindi «dal basso verso l'alto», per l'appunto) [83].

Al contrario, alla base del secondo approccio risiede una concezione secondo cui i dati personali hanno un valore sociale intrinseco, che va oltre il valore economico attribuito loro dal mercato. In una simile ottica, la protezione dei dati personali viene prevalentemente considerata nella sua dimensione di diritto individuale [84], che non può essere oggetto di scambio e rappresenta anzi «un imperativo sociale strutturale in una democrazia» («*a social structural imperative in a democracy*») [85]: una precondizione di una deliberazione democratica è infatti che gli individui si sentano liberi e siano effettivamente liberi di esprimersi, senza temere indebite conseguenze derivanti dalla raccolta e dal trattamento delle loro informazioni da parte di soggetti pubblici o privati [86]. La tutela non è dunque strumentale rispetto alle esigenze economiche, ma è essa stessa l'obiettivo ultimo della regolamentazione. Di conseguenza, là dove ci si trovi in presenza del «*top-down regulatory design*», la regola che governa i flussi è quella del «divieto con deroghe» («*prohibition with derogations*») [87]: si prendono le mosse da una

---

[82] Sul punto v. anche, *inter alios*: A. Ogus, *Regulation: Legal Form and Economic Theory*, Clarendon Press, Oxford, 1994, p. 29.

[83] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 484, secondo cui: «*[…] It is bottom up because it starts from a theoretical level at which there is no protection and increases just enough to achieve the stated objective […]*».

[84] *Ibid*., pp. 481-482, secondo cui: «*[…] In a broader societal context, personal data thus have intrinsic value beyond the economic value attributed by the market and so does the value of the right to protect personal data. Data have a societal dimension that exceeds the value to particular individuals whose data may be compromised […]*».

[85] A. Rouvroy-Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in S. Gutwirth-Y. Poullet-P. De Hert-C. De Terwangne-S. Nouwt (a cura di), *op. cit.*, pp. 45-76, spec. p. 55.

[86] *Ibid*., secondo cui: «*[…] a precondition to democratic deliberation is that individuals feel free and are free to express themselves without fear of being judged out of context or by public and/or private bureaucracies interpreting their expressed thoughts and behaviours from a distance, on the basis of information collected and processed by them […]*».

[87] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 486.

situazione in cui ai dati personali è garantito un alto livello di protezione e i flussi che coinvolgono gli stessi sono generalmente proibiti; solo in un momento successivo è possibile diminuire il livello di protezione e consentire determinati flussi, ma esclusivamente entro certi limiti, al fine di preservare interessi concorrenti (in questo caso, ci si sposta dunque «dall'alto verso il basso») [88].

5.2. *Il* «geographically-based approach» *e l'*«organizationally-based approach» *(o* «accountability approach»*)*

Un'altra significativa classificazione tra tecniche di regolamentazione dei flussi transfrontalieri di dati personali, proposta da autorevole dottrina, è quella che vede contrapposto il c.d. «*geographically-based approach*», ovvero l'approccio «su base geografica», al c.d. «*organizationally-based approach*», ovvero l'approccio «su base organizzativa» [89].

Per quanto riguarda il primo, esso disciplina i trasferimenti di dati personali in base allo standard di protezione che agli stessi accorda lo Stato di destinazione. Detto in altri termini, si richiede al Paese, verso cui il flusso è diretto, di tutelare sufficientemente i dati personali, non solo predisponendo idonei strumenti giuridici, ma anche facendoli rispettare in concreto [90]. Là dove ciò non avvenga, al contrario, i trasferimenti subiranno delle limitazioni. L'approccio «su base geografica» appare dunque più attento all'esigenza di proteggere i dati personali e, addirittura, può rappresentare uno strumento per incentivare gli Stati destinatari ad adottare normative a tutela di tali dati, in mancanza delle quali non potranno beneficiare di quei flussi tanto importanti per le loro economie [91].

Per quanto invece riguarda il secondo, esso si concentra sulle misure adottate da chi esporta e da chi importa i dati, responsabilizzandoli (per questo si parla anche di «*accountability approach*») [92]. Non ci si basa dunque sullo standard di protezione del Paese di destinazione, ma si obbliga invece il titolare del trattamento a rispettare determinati principi, indipendentemente dall'ubicazione geografica del trattamento stesso: la tutela deve continuare a seguire i dati, anche dopo

---

[88] *Ibid.*, p. 484, secondo cui: «*[…] the starting point of public policy regulation is top-down: a high level of protection, which can be lowered only to the extent necessary to safeguard competing interests […]*».

[89] C. KUNER, *Transborder Data Flows and Data Privacy Law*, cit., p. 64.

[90] *Ibid.*, secondo cui: «*[…] The geographically-based approach regulates data transfers based on the standard of data protection in the country of import. This requires both that a certain level of protection is assured by the legal system of the country in question, and that such protections are actually complied with […]*».

[91] *Ibid.*, p. 66.

[92] *Ibid.*, secondo cui: «*[…] the organizationally based approach […] focuses on measures taken by data exporters and importers to make them 'accountable' for their processing of personal data […]*».

la loro esportazione [93]. Dal punto di vista pratico, la «responsabilizzazione» può comportare che alle imprese sia richiesto di adoperarsi, ad esempio, adottando idonee «politiche sulla *privacy*» (o «*privacy policies*») che siano approvate dalla dirigenza e attuate dal personale; formando i dipendenti al rispetto delle *policies*; predisponendo una supervisione interna e dei programmi di verifica esterni; garantendo la trasparenza agli individui circa le *policies* e il rispetto delle stesse; adottando meccanismi per imporne l'osservanza [94]. Tuttavia, è anche opportuno precisare che l'approccio «su base organizzativa», limitandosi a responsabilizzare coloro che trasferiscono i dati personali a livello internazionale, non comporta delle vere e proprie restrizioni ai flussi stessi [95], risultando di conseguenza meno attento alle esigenze di protezione dei dati personali e più sensibile a quelle economiche. Proprio in ragione di ciò, l'«*organizationally-based approach*» è spesso preferito da chi trasferisce i dati, perché ritenuto più funzionale, e non bisogna fare mistero del fatto che alcuni titolari del trattamento vedano l'«*accountability*» come un modo per liberarsi da sgradite restrizioni [96].

Passando dalle categorie astratte appena individuate alle regolamentazioni concretamente adottate, ci si renderà conto di come, sussumendo queste ultime all'interno delle categorie stesse, si possano avere utili indicazioni fin da subito: si potranno avere indizi importanti, in particolare, circa l'esito del bilanciamento, cioè se finiscano per prevalere i diritti degli individui oppure le esigenze di carattere commerciale. Allo stesso tempo, lo si sottolinea, si tratta unicamente di indizi: per poter addivenire a una conclusione più solida sul punto sarà inevitabile un'analisi ben più approfondita. Ciò anche perché le distinzioni suesposte non sono così nette come può apparire in teoria e perché approcci all'apparenza opposti non si escludono necessariamente a vicenda nella realtà dei fatti [97]: ad esempio, si avrà a che fare con normative che, per trasferire oltrefrontiera dati personali, fanno ricorso sia a meccanismi che sono frutto del «*geographically-based approach*», sia a soluzioni rappresentative dell'«*organizationally-based approach*».

---

[93] *Ibid*., pp. 71-72, secondo cui: «*[…] The accountability approach does not base the protection granted on a specific standard such as 'an adequate level of protection', but instead obliges data controllers to comply with certain privacy principles, no matter where the geographical location of the data processing. As such, it requires that the protections applicable under the law of the data controller continue to apply to processing of the data after they are exported […]*».

[94] *Ibid*., p. 72, secondo cui: «*[…] On a practical level, accountability may require organizations to take steps such as implementing appropriate privacy policies that are approved by senior management and implemented by a sufficient number of staff; training employees to comply with these policies; adopting internal oversight and external verification programmes; providing transparency to individuals as to the policies and compliance with them; and adopting mechanisms to enforce compliance […]*».

[95] *Ibid*., secondo cui: «*[…] Accountability does not specifically restrict transborder data flows […]*».

[96] *Ibid*., p. 74, secondo cui: «*[…] At least in theory, a widespread use of accountability can replace more bureaucratic mechanisms […] it is no secret in the data protection community that some data controllers view accountability as a justification for them to be freed from such burdens […]*».

[97] *Ibid*., p. 76, secondo cui: «*[…] There is overlap between the geographically-based and organizationally-based approaches, so that they are not mutually exclusive […]*».

CAPITOLO II

L'OBIETTIVO E LA STRUTTURA DELL'INDAGINE

SOMMARIO: 1. L'obiettivo. – 2. La struttura. – 2.1. L'attuale disciplina unilateralmente adottata dall'Unione europea. – 2.2. Gli impegni commerciali assunti dall'Unione europea a livello internazionale.

1. *L'obiettivo*

Se finora sono state messe in evidenza le premesse fondamentali della presente indagine, a questo punto è finalmente possibile concentrare l'attenzione su quello che è l'oggetto della trattazione, come si evince dal titolo della medesima e come è già stato anticipato: l'Unione europea e gli strumenti giuridici da essa predisposti per regolamentare i flussi transfrontalieri di dati personali che originano dal suo territorio e sono diretti verso Stati terzi, strumenti attraverso cui l'UE tenta di trovare un bilanciamento tra la promozione dei flussi in questione, da un lato, e la protezione dei dati personali, dall'altro. L'analisi di tale argomento si pone come obiettivo quello di rispondere a un preciso interrogativo: ci si chiederà infatti, e si tenterà di comprendere, se l'Unione riesca attraverso gli strumenti in questione a trovare un perfetto equilibrio tra le due esigenze che vengono in gioco oppure se, nei fatti, finisca per privilegiarne una a scapito dell'altra. Là dove poi si dovesse propendere per questa seconda ipotesi, si proverà a capire quale delle due istanze prevalga e quale sia sacrificata, quali sono le ragioni di ciò e quali invece le possibili conseguenze di tale approccio.

2. *La struttura*

2.1. *L'attuale disciplina unilateralmente adottata dall'Unione europea*

Al fine di rispondere al quesito appena delineato, verrà svolta un'indagine che si strutturerà in due parti. La prima si occuperà dell'attuale disciplina unilateralmente adottata dall'UE in materia di flussi transfrontalieri di dati personali.

Preliminarmente, verranno dedicati alcuni cenni al cammino che ha condotto verso l'elaborazione di tale quadro giuridico: si menzioneranno dunque gli

strumenti giuridici di altre organizzazioni internazionali che hanno preceduto e influenzato l'azione dell'Unione europea nel settore; la genesi della prima normativa UE in materia di protezione e libera circolazione dei dati personali, contenuta nella già citata Direttiva 95/46/CE; nonché le profonde trasformazioni dell'assetto dell'Unione che hanno successivamente indotto a sostituire tale normativa con quella del GDPR.

Dopo tale premessa, sarà possibile concentrarsi sulle attuali regole in materia di trasferimenti di dati personali verso Stati extra-UE. Come si vedrà, il principale strumento per trasmettere i dati personali fuori dal territorio dell'Unione è la c.d. «decisione di adeguatezza», che è adottata dalla Commissione europea e che consente al Paese terzo destinatario della stessa di ricevere i dati personali dall'UE senza ulteriori condizioni, poiché il suo livello di protezione dei dati è «adeguato», per l'appunto. Là dove manchi una decisione di adeguatezza, tuttavia, il trasferimento rimane comunque possibile attraverso meccanismi alternativi: si tratta, in particolare, delle «garanzie adeguate», aventi natura contrattuale (come le clausole contrattuali tipo o le norme vincolanti d'impresa), e delle «deroghe in specifiche situazioni» (come il consenso della persona interessata o la necessità del trasferimento a particolari fini).

Orbene, la trattazione si soffermerà sui suddetti strumenti, prendendo in considerazione non solo il testo delle pertinenti disposizioni, contenute nel Capo V del Regolamento (UE) 2016/679, ma anche la giurisprudenza rilevante e la prassi applicativa. Tutto ciò con un preciso scopo: quello di comprendere come la disciplina unilateralmente adottata dall'UE nell'ambito in questione – per come delineata dal legislatore nel GDPR, interpretata dalla Corte di giustizia nelle sue sentenze e attuata dalla Commissione (attraverso le decisioni di adeguatezza e non solo) – vada a bilanciare la necessità di proteggere i dati personali con quella di favorire i flussi dei medesimi, e se finisca per privilegiarne una rispetto all'altra. In tal caso, si cercherà di dar conto delle ragioni e delle finalità per cui ciò avviene. Nello svolgimento di una simile operazione, le categorie suesposte – «*bottom-up regulatory design*» e «*top-down regulatory design*»; «*geographically-based approach*» e «*organizationally-based approach*» – forniranno indizi assai utili, ma dovranno essere presi in considerazione in modo approfondito vari altri elementi [1].

[1] Poiché il presente lavoro si concentra sui flussi di dati personali per finalità commerciali, al medesimo rimane invece estranea la tematica dei flussi di dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Conseguentemente, non sarà oggetto di trattazione la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, 27 aprile 2016, GU L 119, 4 maggio 2016, pp. 89-131. Neppure ci si occuperà del Capo V di tale Direttiva, dedicato proprio ai «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali» e contenente meccanismi corrispondenti a quelli del GDPR («decisione di adeguatezza», «garanzie adeguate», «deroghe in specifiche situazioni»).

2.2. *Gli impegni commerciali assunti dall'Unione europea a livello internazionale*

Per poter raggiungere l'obiettivo che l'indagine si prefigge, tuttavia, sarà necessario un passaggio ulteriore. Si tratterà infatti di esaminare certi impegni assunti dall'UE a livello internazionale, nello specifico in ambito commerciale, che vanno in vario modo a incidere sulla materia dei flussi transfrontalieri di dati personali, e di interrogarsi sul rapporto esistente tra questi e la disciplina adottata sul punto unilateralmente dall'UE (di cui si è detto sopra).

In primis, verranno analizzati gli obblighi racchiusi nel diritto dell'Organizzazione mondiale del commercio (OMC), e segnatamente nel *General Agreement on Trade in Services* (GATS), concernenti in generale la liberalizzazione dei servizi: tra detti servizi, infatti, figurano anche quelli forniti in modo transfrontaliero che si sostanziano proprio in flussi di dati. Gli obblighi in questione annoverano la clausola della nazione più favorita (CNPF) o «*most-favoured-nation clause*» (MFNC), senza dubbio la più importante previsione del GATS, ma anche le norme in materia di trasparenza, regolamentazione interna, trattamento nazionale e accesso al mercato.

Successivamente, verranno esaminati certi impegni assunti dall'UE non solo nell'ambito del diritto OMC, ma soprattutto in accordi commerciali bilaterali, che riguardano in modo esplicito proprio l'ambito dei flussi oltrefrontiera di dati. Si tratta di veri e propri impegni a trasferire dati (anche detti, proprio per questo, «*data flows commitments*»), i quali sono poi controbilanciati da previsioni finalizzate alla salvaguardia della *privacy* e del diritto alla protezione dei dati personali.

L'analisi sul punto avrà un chiaro scopo: quello di comprendere se l'approccio seguito dall'UE al momento dell'assunzione dei suddetti obblighi internazionali di natura commerciale è coerente, o meno, con il bilanciamento tra interessi che caratterizza la disciplina adottata unilateralmente dalla stessa UE. Nel caso in cui non lo sia, sarà ovviamente necessario capire quale può essere l'impatto di una simile incompatibilità su tale bilanciamento.

Parte I

L'ATTUALE DISCIPLINA UNILATERALMENTE ADOTTATA DALL'UE IN MATERIA DI FLUSSI TRANSFRONTALIERI DI DATI PERSONALI

CAPITOLO I

LA GENESI DELL'ATTUALE DISCIPLINA UE

SOMMARIO: 1. Gli strumenti di diritto internazionale che hanno preceduto e influenzato la disciplina UE. – 1.1. Le Linee guida dell'OCSE. – 1.2. La Convenzione 108 del Consiglio d'Europa. – 2. La prima normativa UE in materia di protezione e libera circolazione dei dati personali: la Direttiva 95/46/CE. – 3. La crescente attenzione dell'ordinamento UE per la protezione dei dati personali nella sua dimensione di diritto fondamentale.

1. *Gli strumenti di diritto internazionale che hanno preceduto e influenzato la disciplina UE*

La disciplina UE in materia di trasferimenti oltrefrontiera di dati personali è stata preceduta, e in certa misura influenzata, da due importanti strumenti di diritto internazionale, che rappresentano anche altrettanti differenti approcci alla regolamentazione della materia. Ci si riferisce alle Linee guida dell'OCSE e alla Convenzione 108 del Consiglio d'Europa.

1.1. *Le Linee guida dell'OCSE*

In primis, occorre fare cenno alle Linee guida sulla protezione della *privacy* e sui flussi transfrontalieri di dati personali («*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*»): l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), o *Organization for Economic Co-operation and Development* (OECD) [1], dopo essersi interessata alla materia

[1] L'Organizzazione per la cooperazione e lo sviluppo economico, fondata nel 1961 e composta originariamente da 18 Stati europei, dagli USA e dal Canada, comprende oggi ben 38 membri, tra cui anche Paesi del Centro e Sud America e della regione asiatico-pacifica. Ancor più precisamente, nel momento in cui si scrive, gli Stati membri dell'OCSE sono: Australia, Austria, Belgio, Canada, Cile, Colombia, Corea del Sud, Costa Rica, Danimarca, Estonia, Finlandia, Francia, Germania, Giappone, Grecia, Irlanda, Islanda, Israele, Italia, Lettonia, Lituania, Lussemburgo, Messico, Norvegia, Nuova Zelanda, Paesi Bassi, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Turchia, Ungheria, USA. L'OCSE ha sede a Parigi e ha come lingue ufficiali l'Inglese e il Francese.

fin dai primi anni '70 del XX secolo [2], ha adottato lo strumento in questione nel 1980 [3], per poi successivamente emendarlo nel 2013 [4]. Pur non essendo giuridicamente vincolanti, le *OECD Guidelines* si sono rivelate estremamente influenti a livello globale [5] e hanno indotto numerosi membri dell'organizzazione, ma anche Stati terzi, a introdurre legislazioni nazionali basate su di esse [6]. Tra i Paesi la cui normativa interna è stata particolarmente influenzata dalle *Guidelines* è possibile citare, a titolo esemplificativo, la Nuova Zelanda [7].

Le Linee guida del 1980, dopo aver dettato alcune disposizioni generali (Parte prima) e certi principi sulla protezione dei dati personali (Parte seconda) [8], dedicavano ai «*Transborder Flows of Personal Data*», definiti come movimen-

---

[2] In dottrina, sulle azioni dell'OCSE in materia di *privacy* e flussi di dati personali, v. *inter alios*: J. Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?*, in *Law and Policy in International Business*, 1978, Volume 10, Numero 4, pp. 1065-66; M.D. Kirby, *International guidelines to protect privacy in transborder data flows*, ANZAAS (Australian & New Zealand Association for the Advancement of Science) Jubilee conference, Adelaide, 15 maggio 1980; J. Michael, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, Dartmouth/UNESCO, Aldershot, 1994; C. Bennet-C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, Aldershot, 2003; H.P. Gassmann, *30 Years After: The Impact of the OECD Privacy Guidelines*, Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP), Parigi, 10 marzo 2010; M.D. Kirby, *The history, achievement and future of the 1980 OECD guidelines on privacy*, in *International Data Privacy Law*, Febbraio 2011, Volume 1, Numero 1, pp. 6-14; OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, Numero 176, OECD Publishing, Parigi, 6 aprile 2011; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht, 2014.

[3] OECD, *Annex to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL]*, 23 settembre 1980.

[4] OECD, *Annex to the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, as amended by C(2013)79]*, 11 luglio 2013.

[5] G. González Fuster, *op. cit.*, p. 80.

[6] D. Wright-P. De Hert-S. Gutwirth, *Are the OECD Guidelines at 30 Showing Their Age?*, in *Communications of the ACM (Association for Computing Machinery)*, 2011, Volume 54, Numero 2, pp. 119-127, spec. p. 122.

[7] Sul punto v., *inter alios*: OECD, *The Evolving Privacy Landscape*, cit., p. 13, secondo cui: «*[…] The explicit reference to the OECD Guidelines in a 2010 amendment to the New Zealand Act is a testament to the Guidelines' enduring influence […]*».

[8] In dottrina, sui principi dettati nelle Linee guida dell'OCSE, v. *inter alios*: D. Wright-P. De Hert-S. Gutwirth, *op. cit.*, pp. 121-122; 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: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 137-167, spec. p. 140; Y. Suda, *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy*, Routledge, New York, 2018, pp. 13-14.

ti di dati personali attraverso le frontiere nazionali [9], la loro Parte terza [10]. La disciplina ivi sancita rappresentava un chiaro esempio di ciò che nell'introduzione del presente lavoro è stato definito «*bottom-up regulatory design*», ovvero un approccio «dal basso verso l'alto» nella regolamentazione della materia: di *default*, i trasferimenti di dati personali tra Stati membri erano sempre consentiti, anzi non potevano proprio essere ostacolati, e di conseguenza il livello di protezione era estremamente basso, se non addirittura inesistente; gli Stati membri avrebbero poi potuto incrementare tale protezione, attraverso una restrizione dei flussi, ma solo in determinati casi [11]. Le esigenze economiche finivano dunque per prevalere su quelle di tutela dei diritti degli individui [12].

Quanto appena detto è tutto fuorché sorprendente. Avendo l'OCSE come obiettivi lo sviluppo dell'economia globale [13] e l'espansione del commercio mondiale [14], tale organizzazione ha sempre cercato di evitare che le normative nazionali creassero delle barriere ai flussi di informazioni, impedendo, in questo modo, la crescita [15]. La preoccupazione più grande era che, utilizzando l'etichetta di «protezione dei dati», si adottassero in realtà misure di ostacolo al libero scambio: da «*data protection*» si sarebbe passati a «*data protectionism*» [16]. Le *Guidelines* avevano dunque il principale scopo di facilitare i flussi transfrontalieri di dati personali, favorendo così lo sviluppo dell'economia internazionale [17].

---

[9] OECD, *Annex to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980, cit., par. 1.

[10] *Ibid*., parr. 15-18. Su tali paragrafi v.: OECD, *Explanatory Memorandum to Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL]*, 23 settembre 1980, §§ 63-68.

[11] Sul punto v.: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, in *World Trade Review*, Luglio 2018, Volume 17, Numero 3, pp. 477-508, spec. p. 485.

[12] C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, Oxford, 2013, p. 36, secondo cui: «*[…] The OECD Guidelines […] focused on the facilitation of global data flows for economic purposes rather than on human rights […]*».

[13] OECD, *Convention on the Organisation for Economic Co-operation and Development*, Parigi, 14 dicembre 1960, art. 1, lett. a).

[14] *Ibid*., art. 1, lett. c).

[15] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, cit., p. 10.

[16] M.D. KIRBY, *International guidelines to protect privacy in transborder data flows*, cit., p. 4.

[17] Sul punto v., *inter alios*: S. NOUWT, *Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, in S. GUTWIRTH-Y. POULLET-P. DE HERT-C. DE TERWANGNE-S. NOUWT (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 275-282, spec. p. 278, secondo cui: «*[…] From these OECD initiatives we can conclude that from an economic perspective, data protection should be considered as a guarantee for the transborder flow of personal data […]*»; M. TZANOU, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, Oxford, 2017, p. 15, secondo cui: «*[…] The Guidelines, adopted on 23 September 1980, place an emphasis on ensuring that the measures introduced to protect personal data would not result in restricting transborder data flows […]*».

L'impostazione poc'anzi descritta è stata confermata, e anzi consolidata, nella versione delle Linee guida frutto dell'emendamento del 2013, la quale dedica ai trasferimenti oltrefrontiera di dati personali la sua Parte quarta [18]. Le disposizioni di riferimento, infatti, non solo mantengono il «*bottom-up regulatory design*» di cui si è detto sopra [19], ma enfatizzano anche gli elementi propri di quello che nell'introduzione del presente lavoro è stato definito «*organizationally-based approach*» (approccio «su base organizzativa»), o anche «*accountability approach*», fondato per l'appunto sulla responsabilizzazione di coloro che trasferiscono i dati: spetta al titolare del trattamento il compito di far fronte ai rischi corsi dai dati personali sotto il suo controllo, indipendentemente dalla loro ubicazione. Un'impostazione, come si è illustrato, più sensibile alle necessità di carattere economico dei titolari medesimi rispetto a quelle di protezione dei dati degli interessati [20].

A margine, giova ricordare come le Linee guida dell'OCSE abbiano influenzato anche altri strumenti di diritto internazionale. Nello specifico, la Cooperazione economica Asia-Pacifico, o «*Asia-Pacific Economic Cooperation*» (APEC) [21], nell'elaborazione del suo «*Privacy Framework*», adottato in una prima versione nel 2005 [22] e in una seconda versione nel 2015 [23], si è dichiaratamente ispirata alle *OECD Guidelines* [24]. Pure tale quadro, sprovvisto di valore giuridico vin-

---

[18] OECD, *Annex to the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013, cit., parr. 16-18. Su tali paragrafi v.: OECD, *Supplementary explanatory memorandum to the Revised Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, as amended by C(2013)79]*, 11 luglio 2013, pp. 29-31.

[19] In dottrina, sul punto v.: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., pp. 484-485, secondo cui: «*[…] Their 2013 revision subordinated the regulation of transborder flows of personal data to economic needs even more than the previous set […] The 2013 Guidelines clearly start from a degree of very low (even non-existent) protection and allow members to increase it only as much as is necessary and require that any restrictions to transborder flows of personal data introduced by domestic legislation be proportionate to the risks presented […]*».

[20] In dottrina, sul rafforzamento del c.d. «*accountability approach*» nelle Linee guida del 2013 v.: M. KUSCHEWSKY, *Revised OECD Privacy Guidelines Strengthen Accountability Principle*, in *Inside Privacy*, 23 settembre 2013.

[21] La Cooperazione economica Asia-Pacifico è un forum economico intergovernativo, istituito nel 1989 e finalizzato a facilitare il commercio e gli investimenti tra gli Stati che ne fanno parte, ovvero 21 Paesi (sia asiatici, che dell'Oceania, che americani) affacciati sull'Oceano Pacifico. Ancor più precisamente, nel momento in cui si scrive, gli Stati membri dell'APEC sono: Australia, Brunei, Canada, Cile, Cina, Corea del Sud, Filippine, Giappone, Hong Kong, Indonesia, Malesia, Messico, Nuova Zelanda, Papua Nuova Guinea, Perù, Russia, Singapore, Stati Uniti, Taiwan, Thailandia, Vietnam. In dottrina, sull'APEC, v. *inter alios*: M. BEESON, *Institutions of the Asia Pacific. ASEAN, APEC and beyond*, Routledge, New York, 2009.

[22] APEC, *Privacy Framework*, Singapore, 2005.

[23] APEC, *Privacy Framework*, Singapore, 2015.

[24] APEC, *Privacy Framework*, 2005, cit., § 5; APEC, *Privacy Framework*, 2015, cit., § 5.

colante, è infatti contraddistinto dall'«*accountability approach*» e dal «*bottom-up regulatory design*», bilanciando così gli interessi in gioco in modo assai simile alle Linee guida [25].

1.2. *La Convenzione 108 del Consiglio d'Europa*

Il secondo strumento che ha preceduto e influenzato la disciplina UE è invece la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale («*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*»), meglio nota come Convenzione 108. Il Consiglio d'Europa, o *Council of Europe* (CoE) [26], interessatosi alle questioni legate alla *privacy* sin dalla fine degli anni '60 del secolo scorso [27], ha adottato lo strumento in questione nel 1981 [28], elaborando poi nel 2018 una versione modernizzata, la «Convenzione 108+»; quest'ultima, che avvicinerebbe ulteriormente il quadro giuridico del CoE a quello dell'UE, nel momento in cui si scrive non è tuttavia ancora entrata in vigore [29].

---

[25] In dottrina, sull'approccio adottato dal «*Privacy Framework*» dell'APEC, v. *inter alios*: C. KUNER, *Transborder Data Flows and Data Privacy Law*, cit., pp. 50-51; L.A. BYGRAVE, *Data Privacy Law. An International Perspective*, Oxford University Press, Oxford, 2014, pp. 75-79; S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 478 ss.

[26] Il Consiglio d'Europa, istituito nel 1949, era composto originariamente da 10 Stati europei: Belgio, Danimarca, Francia, Irlanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Regno Unito e Svezia. Nel momento in cui si scrive, gli Stati membri sono 46: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgio, Bosnia-Erzegovina, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Georgia, Germania, Grecia, Irlanda, Islanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Macedonia del Nord, Malta, Monaco, Montenegro, Norvegia, Paesi Bassi, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Repubblica di Moldova, Romania, San Marino, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Turchia, Ucraina, Ungheria. Ad essi si aggiungono 6 Stati osservatori: Canada, Giappone, Israele, Messico, Santa Sede, Stati Uniti. Il Consiglio d'Europa ha sede a Strasburgo e ha come lingue ufficiali l'Inglese e il Francese.

[27] Tra gli atti adottati dal Consiglio d'Europa in materia di *privacy* v.: COE, *Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments*, 31 gennaio 1968; COE, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, 26 settembre 1973; COE, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, 20 settembre 1974. In dottrina, sul punto v., *inter alios*: F.W. HONDIUS, *The Council of Europe's work in the area of computers and privacy*, Discussion paper of round table on the use of data processing for parliamentary work, Strasburgo, 18-19 maggio 1978; M.D. KIRBY, *International guidelines to protect privacy in transborder data flows*, cit.; M.D. KIRBY, *Informatics and Law Reform*, in *Journal of Law and Information Science*, 1981, Volume 1, Numero 1, pp. 1-22; J. MICHAEL, *op. cit.*; G. GONZÁLEZ FUSTER, *op. cit.*.

[28] COE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, Strasburgo, 28 gennaio 1981.

[29] COE, *Modernised Convention for the Protection of Individuals with Regard to the Processing*

La Convenzione 108 del 1981 rappresenta, ancora oggi, l'unico strumento di diritto internazionale giuridicamente vincolante nel settore [30] e possono aderirvi anche Stati extra-europei [31]. Dopo aver dedicato il «*Chapter I*» alle «*General provisions*» e il «*Chapter II*» ai «*Basic principles for data protection*», essa si occupa nel «*Chapter III*» (art. 12) dei «*Transborder data flows*«: la disciplina ivi dettata prevede che, tra le Parti della Convenzione, i flussi di dati non dovrebbero essere ostacolati, salvo eccezioni, e appare dunque simile a quella delle Linee guida OCSE [32]. Le regole in questione, tuttavia, sono integrate da quelle del Protocollo addizionale del 2001 [33], il quale, con riferimento ai flussi da Stati parte della Convenzione *verso Stati non parte*, abbraccia quello che può essere definito «*top-down regulatory design*» (approccio «dall'alto verso il basso»): si prendono le mosse da una situazione in cui ai dati personali è garantito un elevato livello di protezione e i trasferimenti che coinvolgono gli stessi sono, come regola generale, proibiti; è poi possibile diminuire tale protezione e consentire certi flussi, ma solo in un momento successivo e a determinate condizioni [34].

Le norme del Protocollo addizionale alla Convenzione 108, inoltre, rappresentano un esempio di «*geographically-based approach*» (approccio «su base

---

of Personal Data, Elsinore, 18 maggio 2018. In dottrina, sulla Convenzione 108+, v. *inter alios*: G. Greenleaf, *Renewing Data Protection Convention 108: The Coe's 'Gdpr Lite' Initiatives*, in *Privacy Laws & Business International Report*, 2016, Volume 142, pp. 1-8.

[30] UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, United Nations Publication, New York/Ginevra, 2016, p. 83.

[31] CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981, cit., art. 23 («*Accession by non-member States*»). Gli Stati extra-europei che, nel momento in cui si scrive, hanno aderito alla Convenzione 108 sono: Uruguay (2013), Repubblica di Mauritius (2016), Senegal (2016), Tunisia (2017), Capo Verde (2018), Messico (2018), Argentina (2019) e Marocco (2019).

[32] CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981, cit., art. 12 («*Transborder flows of personal data and domestic law*»). Su tale articolo v.: CoE, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasburgo, 28 gennaio 1981, §§ 62-70. In dottrina, sul punto v., *inter alios*: F.W. Hondius, *A Decade of International Data Protection*, in *Netherlands International Law Review*, 1983, Volume 30, pp. 103-128.

[33] CoE, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasburgo, 8 novembre 2001, art. 2 («*Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention*»). Su tale articolo v.: CoE, *Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, Strasburgo, 8 novembre 2001, §§ 21-33. In dottrina, sul punto v., *inter alios*: G. Greenleaf, *A world data privacy treaty? 'Globalisation' and 'modernisation' of Council of Europe Convention 108*, in N. Witzleb e altri (a cura di), *Emerging Challenges in Privacy Law: Comparative Perspectives*, Cambridge University Press, Cambridge, 2014, pp. 92-138.

[34] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., pp. 484-486.

geografica»), dal momento che pongono l'accento non sul soggetto che trasferisce i dati personali, ma sullo Stato destinatario del flusso, a cui viene richiesto di garantire un livello «adeguato» di protezione ai dati personali.

Indipendentemente da come lo si voglia classificare, non cambia dunque il fatto che il quadro giuridico del Consiglio d'Europa appare, al contrario di quello dell'OCSE, più attento alle esigenze di tutela dei dati personali che non a quelle di carattere economico[35]. Anche in questo caso, non vi è motivo di stupore. Come noto, tra gli scopi principali del CoE figura la promozione in tutta Europa dei diritti umani e delle libertà fondamentali[36], e l'interesse dell'organizzazione per l'ambito in questione nasce proprio con l'obiettivo di proteggere il diritto alla *privacy* nei confronti delle violazioni che possono essere commesse con l'uso dei nuovi metodi scientifici e tecnologici[37]. La suddetta impostazione, inoltre, sarebbe confermata e ulteriormente rafforzata dalla Convenzione 108+ qualora entrasse in vigore[38].

Al tempo stesso, nonostante le differenze nella regolamentazione dei flussi di dati personali, non si può neanche trascurare il fatto che le Linee guida dell'OCSE e la Convenzione 108 del Consiglio d'Europa presentano anche molti tratti in comune e sanciscono principi sulla protezione dei dati assai simili[39]: una logica conseguenza del dialogo costruttivo instauratosi tra le due organizzazioni[40].

---

[35] F.W. Hondius, *A Decade of International Data Protection*, cit., p. 106, secondo cui: «*[…] The thrust of the Council of Europe's Convention is the protection of human rights; that of the OECD Guidelines the facilitation of transborder data flows […]*». Sul punto v. anche, *inter alios*: A. Newman, *Protecting Privacy in Europe: Policy Feedback and Regional Politics*, in S. Meunier-K.R. McNamara (a cura di), *The state of the European Union. Vol. 8. Making history: European integration and institutional change at fifty*, Oxford University Press, Oxford, 2007, pp. 123-138; S. Nouwt, *Towards a Common European Approach to Data Protection*, cit., p. 280.

[36] CoE, *Statute of the Council of Europe*, Londra, 5 maggio 1949, art. 1, lett. a).

[37] G. González Fuster, *op. cit.*, p. 83.

[38] CoE, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, 2018, cit., art. 14 («*Transborder flows of personal data*»). Su tale articolo v.: CoE, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasburgo, 10 ottobre 2018, §§ 102-116.

[39] Tra i principi comuni alle Linee guida dell'OCSE e alla Convenzione 108 del Consiglio d'Europa, si possono menzionare i principi di liceità e correttezza (par. 7 delle Linee guida OCSE e art. 5, lett. a), della Convenzione 108); il principio secondo il quale le finalità del trattamento devono essere determinate (par. 9 delle Linee guida OCSE e art. 5, lett. b), della Convenzione 108); i principi in base a cui i dati devono essere pertinenti rispetto a tali finalità (par. 8 delle Linee guida OCSE e art. 5, lett. c), della Convenzione 108), nonché esatti e aggiornati (par. 8 delle Linee guida OCSE e art. 5, lett. d), della Convenzione 108); la necessità di adottare adeguate misure di sicurezza (par. 11 delle Linee guida e art. 7 della Convenzione 108); la facoltà per la persona interessata di esercitare una serie di diritti, come il diritto ad ottenere determinate informazioni, il diritto di accesso, il diritto di rettifica o cancellazione e il diritto di disporre di una possibilità di ricorso (par. 13 delle Linee guida e art. 8 della Convenzione 108).

[40] J. Michael, *op. cit.*, p. 33.

2. *La prima normativa UE in materia di protezione e libera circolazione dei dati personali: la Direttiva 95/46/CE*

I principi di cui si è detto sopra hanno influenzato profondamente il successivo quadro giuridico dell'Unione europea in materia di protezione e libera circolazione dei dati personali, di cui ora si andrà a dire. L'interesse della (allora) Comunità economica europea per l'ambito in esame risale addirittura ai primi anni '70 del XX secolo [41]. Solo nel 1995, tuttavia, è stato adottato il primo atto giuridicamente vincolante in materia: la Direttiva 95/46/CE «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati» [42]. Come si evince fin dall'intitolazione, la Direttiva si prefissava due «obiettivi gemelli» [43], sanciti poi anche nel Capo I («Disposizioni generali») e segnatamente nell'art. 1: il primo era «la tutela dei diritti e

[41] Tra le iniziative comunitarie in materia di protezione dei dati che hanno preceduto l'adozione della Direttiva 95/46/CE v. *inter alia*: CEE, Comunicazione della Commissione europea al Consiglio, *Community policy on data processing*, 21 novembre 1973, SEC/73/4300 final; CEE, Comunicazione del Parlamento europeo, *Risoluzione sulla tutela dei diritti dei cittadini di fronte al crescente progresso tecnologico nel settore dell'informatica*, GU C 60, 13 marzo 1975, p. 48; CEE, Comunicazione del Parlamento europeo, *Risoluzione relativa alla tutela dei diritti individuali di fronte allo sviluppo del progresso tecnico nel settore dell'informatica*, GU C 100, 3 maggio 1976, p. 27; CEE, Comunicazione del Parlamento europeo, *Risoluzione sulla tutela dei diritti dell'individuo di fronte al crescente progresso tecnico nel settore dell'informatica*, GU C 140, 5 giugno 1979, pp. 34-38; CEE, Comunicazione del Parlamento europeo, *Raccomandazioni del Parlamento alla Commissione e al Consiglio di cui al paragrafo 10 della proposta di risoluzione concernenti i principi cui dovrebbero ispirarsi le norme comunitarie in materia di tutela dei diritti dell'individuo di fronte al recente sviluppo tecnico nel settore dell'informatica*, GU C 140, 5 giugno 1979, pp. 37-38; CEE, Raccomandazione della Commissione europea *concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale*, 29 luglio 1981, GU L 246, 29 agosto 1981, p. 31; CEE, Comunicazione del Parlamento europeo, *Risoluzione sulla tutela dei diritti degli individui di fronte al crescente sviluppo tecnico nel settore dell'informatica*, GU C 87, 5 aprile 1982, pp. 39-41; CEE, Comunicazione della Commissione *concernente la protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e la sicurezza dei sistemi d'informazione*, 24 settembre 1990, COM/90/314 def.; CEE, Proposta di direttiva del Consiglio *concernente la protezione delle persone relativamente al trattamento dei dati personali*, 24 settembre 1990, COM/90/314 def. – SYN 287, GU C 277, 5 novembre 1990, pp. 3-12; UE, Proposta modificata di direttiva del Consiglio *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, 16 ottobre 1992, COM/92/422 def. – SYN 287, GU C 311, 27 novembre 1992, pp. 30-61. In dottrina, sul punto v., *inter alios*: U. BRÜHANN, *La directive européenne relative à la protection des données: fondement, histoire, points forts*, in *Revue française d'administration publique*, Gennaio-marzo 1999, Numero 89, pp. 9-19; L. COUDRAY, *La protection des données personnelles dans l'Union européenne, Naissance et consécration d'un droit fondamental*, Éditions Universitaires européennes, Berlino, 2010; G. GONZÁLEZ FUSTER, *op. cit.*.

[42] UE, Direttiva 95/46/CE del Parlamento europeo e del Consiglio *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, 24 ottobre 1995, GU L 281, 23 novembre 1995, pp. 31-50.

[43] Y. SUDA, *op. cit.*, p. 31.

delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali»[44]; il secondo, invece, era «libera circolazione dei dati personali»[45]. Quest'ultimo risultava di certo l'obiettivo maggiormente enfatizzato: la base giuridica della Direttiva era infatti l'art. 100 A del Trattato CE (come modificato dal Trattato di Maastricht), che consentiva l'adozione, attraverso la procedura di codecisione, di misure aventi per oggetto «l'instaurazione ed il funzionamento del mercato interno»[46]. Si poneva quindi l'accento sulla strumentalità della disciplina in materia di protezione dei dati personali alle esigenze degli scambi intracomunitari: il livello di tutela doveva essere il più possibile equivalente in tutti i Paesi UE proprio nell'ottica di permettere una circolazione dei dati senza ostacoli[47].

Soffermandosi sui singoli obiettivi, comunque, quello di tutela delle persone fisiche era perseguito prevalentemente attraverso principi in larga misura equivalenti a quelli delle Linee guida OCSE e della Convenzione 108 (come anticipato), i quali erano contenuti soprattutto all'interno del Capo II («Condizioni generali di liceità dei trattamenti di dati personali»)[48]. Vi erano però pure altre

---

[44] UE, Direttiva 95/46/CE, cit., art. 1 («Oggetto della direttiva»), par. 1.

[45] *Ibid.*, par. 2.

[46] UE, *Trattato sull'Unione europea*, GU C 191, 29 luglio 1992, pp. 1-110, art. G, in base a cui: «Il trattato che istituisce la Comunità economica europea è modificato conformemente alle disposizioni del presente articolo al fine di creare una Comunità europea […] 22) Il testo dell'articolo 100 A, paragrafo 1, è sostituito dal testo seguente: «1. […] Il Consiglio, deliberando in conformità della procedura di cui all'articolo 189 B e previa consultazione del Comitato economico e sociale, adotta le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno.» […]». Si precisa che l'art. 189 B disciplinava la procedura di codecisione.

[47] Sul punto v.: UE, Direttiva 95/46/CE, cit., Considerando 5, 7 e 8.

[48] Nella Direttiva 95/46/CE, e segnatamente nel Capo II (artt. 5-21), la disposizione più rilevante in materia di principi sulla protezione dei dati personali era certamente l'art. 6. Tra le disposizioni più significative in materia di diritti delle persone interessate si possono menzionare l'art. 10 («Informazione in caso di raccolta dei dati presso la persona interessata»), l'art. 11 («Informazione in caso di dati non raccolti presso la persona interessata»), l'art. 12 («Diritto di accesso»). In materia di misure di sicurezza, si veda l'art. 17 («Sicurezza dei trattamenti»). «Ricorsi giurisdizionali, responsabilità e sanzioni» erano invece disciplinati dal Capo III della Direttiva 95/46/CE (artt. 22-24). In dottrina, sui principi e diritti sanciti dalla Direttiva 95/46/CE, v. *inter alios*: J.J.E. BATURONES, *La regulación de los datos sensibles a la Directiva 95/46/CE*, in *Informática y derecho: Revista iberoamericana de derecho informático*, 1998, Numeri 23-26, pp. 1217-1248; M. GENTOT, *La protection des données personnelles à la croisée des chemins*, in P. TABATONI (a cura di), *La protection de la vie privée dans la société d'information: Tome 3*, Presses Universitaires de France, Parigi, 2000, pp. 24-46; O. DE SCHUTTER, *La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi*, in *Revue trimestrielle des droits de l'homme*, 2003, Numero 54, pp. 627-664; H. HEIL, *Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks*, in A. BÜLLESBACH-S. GIJRATH-Y. POULLET-C. PRINS (a cura di), *Concise European IT Law (Second Edition)*, Kluwer Law International, Alphen aan den Rijn, 2010, pp. 9-32.

disposizioni rilevanti sul punto, come quelle sulle autorità nazionali di controllo [49] e sull'istituzione dell'organismo consultivo noto come «Gruppo di lavoro Articolo 29» [50].

Quanto alla libera circolazione dei dati personali, era fatto espresso divieto agli Stati membri di restringerla o vietarla tra di loro per motivi connessi alla summenzionata tutela. Come risulta evidente, interessava prevalentemente la libera circolazione *intra-UE*; erano però presenti anche disposizioni sui flussi verso Stati *extra-UE*: ci si riferisce segnatamente al Capo IV («Trasferimenti di dati personali verso Paesi terzi») [51]. La disciplina ivi dettata sanciva un «divieto con deroghe»: *ex* art. 25, i flussi verso uno Stato non facente parte dell'UE erano vietati, a meno che tale Paese non garantisse un «livello di protezione adeguato» e fosse dunque destinatario di una «decisione di adeguatezza» della Commissione europea. Mancando tale condizione, i trasferimenti avrebbero comunque potuto essere consentiti sulla base di altri fondamenti giuridici *ex* art. 26: nello specifico, in presenza di «deroghe» (tra cui il caso in cui la persona interessata avesse manifestato il proprio consenso in maniera inequivocabile) o di «garanzie sufficienti» (rappresentate ad esempio da «clausole contrattuali appropriate»). Le disposizioni in questione, tuttavia, erano scarne e non particolarmente approfondite [52].

3. *La crescente attenzione dell'ordinamento UE per la protezione dei dati personali nella sua dimensione di diritto fondamentale*

Negli anni successivi all'adozione della Direttiva 95/46/CE, l'Unione europea è stata interessata da importanti trasformazioni. Nell'ambito delle stesse, la protezione dei dati, nata come uno strumento funzionale alla creazione del mercato interno (la si poteva definire «*market-building device*»), ha ricevuto una crescente attenzione nella sua dimensione di diritto fondamentale [53].

---

[49] UE, Direttiva 95/46/CE, cit., art. 28 («Autorità di controllo»).

[50] *Ibid*., art. 29 («Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali»). In dottrina, sul Gruppo di lavoro «Articolo 29», v. *inter alios*: Y. POULLET, S. GUTWIRTH, *The Contribution of the article 29 Working Party to the construction of a harmonised European Data Protection System; an Illustration of 'Reflexive Governance'*?, in M.V. PEREZ ASINARI-P. PALAZZI (a cura di), *Défis du droit a la protection de la vie privée. Challenges of privacy and data protection law*, Bruylant, Bruxelles, 2008, pp. 570-610.

[51] UE, Direttiva 95/46/CE, cit., art. 25 («Principi») e art. 26 («Deroghe»).

[52] Sugli artt. 25 e 26 della Direttiva 95/46/CE, v. *inter alios*: C. KUNER, *Transborder Data Flows and Data Privacy Law*, cit., pp. 40-49; Y. SUDA, *op. cit.*, pp. 30-37.

[53] M.P. GRANGER-K. IRION, *The right to protection of personal data: the new posterchild of European Union citizenship?*, in S. DE VRIES-H. DE WAELE-M.P. GRANGER (a cura di), *Civil Rights and EU Citizenship. Challenges at the Crossroads of the European, National and Private*

I momenti decisivi in tale cammino sono stati soprattutto due. Il primo è stato la proclamazione il 7 dicembre 2000 della Carta dei diritti fondamentali dell'UE, il cui art. 8 sancisce il «diritto alla protezione dei dati di carattere personale»: gli elementi costitutivi di quest'ultimo affondano le radici non solo nella Direttiva, ma anche nella Convenzione 108 e nelle *OECD Guidelines*; la novità, però, è che da quel momento tali elementi devono essere tutelati quali componenti di un diritto fondamentale che merita protezione di per sé (come si è già illustrato nell'introduzione del presente lavoro).

Il secondo momento è stato invece l'entrata in vigore il 1° dicembre 2009 del Trattato di Lisbona, in seguito a cui non solo l'art. 6, par. 1, del Trattato sull'Unione europea (TUE) attribuisce alla Carta di Nizza lo stesso valore giuridico dei trattati, ma l'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE) fornisce anche una base giuridica *ad hoc* per l'adozione, attraverso la procedura legislativa ordinaria, di una normativa in materia di dati personali: non vi è quindi più il bisogno di trovare il fondamento di tale disciplina in disposizioni concernenti l'instaurazione e il funzionamento del mercato interno.

Di fronte a queste novità, la Direttiva si è presto rivelata non più adatta ai tempi: dopo Lisbona, le istituzioni UE hanno quindi avvertito la necessità, anche in ragione degli sviluppi tecnologici intervenuti *medio tempore*, di un quadro giuridico aggiornato. Quest'ultimo avrebbe dovuto innanzitutto rafforzare i diritti delle persone, in linea con l'importanza che il diritto alla protezione dei dati di carattere personale aveva assunto nell'ordinamento dell'Unione in quegli anni, nonché ottenere una maggior armonizzazione, dato che con lo strumento della Direttiva permaneva una frammentazione giuridica eccessiva [54].

Spheres, Edward Elgar, Cheltenham, 2018, pp. 279-302. Sul punto v. anche: M. TZANOU, *The Fundamental Right to Data Protection*, cit..

[54] Tra gli atti UE all'interno dei quali ci si è interrogati sull'idoneità della Direttiva 95/46/CE a raggiungere gli obiettivi prefissati, v. *inter alios*: UE, Relazione della Commissione, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE)*, 15 maggio 2003, COM/2003/265 def.; UE, Risoluzione del Parlamento europeo *sulla prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI))*, 9 marzo 2004, GU C 102E, 28 aprile 2004, pp. 147-153; UE, Comunicazione della Commissione al Parlamento europeo e al Consiglio *sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati*, 7 marzo 2007, COM/2007/87 def.; UE, Parere del garante europeo della protezione dei dati *sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati*, GU C 255, 27 ottobre 2007, pp. 1-12; UE, Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*, 10 giugno 2009, COM/2009/262 def.; UE, Parere del Garante europeo della protezione dei dati *sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini»*, GU C 276, 17 novembre 2009, pp. 8-20; UE, Parere del Comitato delle regioni *sul tema «Il programma di Stoccolma: sfide e opportunità per un nuovo programma pluriennale per lo spazio di libertà, sicurezza e giustizia dell'UE»*, GU C 79, 27 marzo 2010, pp. 37-44; UE, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione*

Tra gli aspetti meno soddisfacenti della Direttiva, inoltre, figuravano proprio le regole in materia di trasferimenti di dati personali verso Paesi terzi: essi erano stati piuttosto trascurati e sul punto, come si è visto, era stata dettata una disciplina scarna e lacunosa. La conseguenza era una notevole disparità tra Stati membri: il bilanciamento tra le note esigenze contrapposte non era realizzato uniformemente nell'intera Unione, prevalendo a seconda dei casi l'una oppure l'altra. Per questo si rendeva necessaria una disciplina più completa e dettagliata, che chiarisse e semplificasse le regole sui trasferimenti e rafforzasse la protezione degli individui i cui dati fossero trasmessi fuori dall'UE, come riconosciuto dalla stessa Commissione e anche dal Garante europeo della protezione dei dati (GEPD o anche EDPS, ovvero «*European Data Protection Supervisor*»)[55].

Così, nel 2012, la Commissione ha presentato la propria Proposta per l'adozione di un Regolamento generale sulla protezione dei dati[56]. Il suo contenuto è stato fortemente influenzato anche dal fatto che, dopo il Trattato di Lisbona, la Direzione generale della Commissione che si è occupata della materia è cambiata rispetto al passato: se della redazione della Direttiva 95/46/CE si era occupata la Direzione generale «Società dell'informazione e media», o DG INFSO[57], e se della prima fase di revisione della Direttiva stessa si era occupata la Direzio-

---

europea, 4 novembre 2010, COM/2010/609 def.; UE, Parere del Garante europeo della protezione dei dati *sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – «Un approccio globale alla protezione dei dati personali nell'Unione europea»*, GU C 181, 22 giugno 2011, pp. 1-23; UE, Parere del Comitato economico e sociale europeo *in merito alla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Un approccio globale alla protezione dei dati personali nell'Unione europea COM(2010) 609 definitivo*, GU C 248, 25 agosto 2011, pp. 123-129; UE, Risoluzione del Parlamento europeo *su un approccio globale alla protezione dei dati personali nell'Unione europea (2011/2025(INI))*, 6 luglio 2011, GU C 33E, 5 febbraio 2013, pp. 101-110; UE, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo*, 25 gennaio 2012, COM/2012/9 final.

[55] Sulle criticità delle regole in materia di trasferimenti di dati personali verso Paesi terzi contenute negli artt. 25 e 26 della Direttiva 95/46/CE, e sulla necessità di migliorarle, v. *inter alia*: UE, Relazione della Commissione, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati*, cit., § 4.4.5; UE, Comunicazione della Commissione, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, cit., § 2.4.1; UE, Parere del Garante europeo della protezione dei dati *sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – «Un approccio globale alla protezione dei dati personali nell'Unione europea»*, cit., § 58; UE, Comunicazione della Commissione, *Salvaguardare la privacy in un mondo interconnesso*, cit., § 5.

[56] UE, Proposta di Regolamento del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, 25 gennaio 2012, COM/2012/11 final.

[57] La Direzione generale «Società dell'informazione e media», o DG INFSO, è stata successivamente sostituita dalla Direzione generale «Reti di comunicazione, contenuti e tecnologie», o DG Connect.

ne generale «Mercato interno», o DG MARKT [58], della fase di redazione del GDPR si è invece occupata la Direzione generale «Giustizia e consumatori» o DG JUST. Quest'ultima, rispetto alle Direzioni generali che l'avevano preceduta nel settore, è indubbiamente caratterizzata da una maggior sensibilità verso i consumatori che non verso il mercato. Si tratta di una conseguenza pratica della maggior attenzione nei confronti della protezione dei dati nella sua dimensione di diritto individuale derivante dallo stesso Trattato di Lisbona [59].

Al termine di un lungo e complesso *iter legis*, in cui sono emersi vari punti di frizione tra gli attori istituzionali coinvolti sulle modalità con cui perseguire i citati obiettivi [60], ha finalmente visto la luce il Regolamento (UE) 2016/679 [61], che a partire dal 25 maggio 2018 è applicabile in via diretta in tutti gli Stati membri dell'Unione europea [62]. Il suo Capo V (artt. 44-50) è specificamente dedicato ai trasferimenti di dati personali verso Paesi terzi.

---

[58] Le responsabilità della Direzione generale «Mercato interno», o DG MARKT, sono state poi trasferite alla Direzione generale «Mercato interno, industria, imprenditoria e PMI», o DG GROW.

[59] In dottrina, sul punto v., *inter alios*: J. Hildén, *The Politics of Datafication: The Influence of Lobbyists on the EU's Data Protection Reform and its Consequences for the Legitimacy of the General Data Protection Regulation*, University of Helsinki, Helsinki, 2019, p. 71 e p. 94; M. Laurer-T. Seidl, *Regulating the European Data Driven Economy: A Case Study on the General Data Protection Regulation*, in *Policy & Internet*, 2020, pp. 257-277, spec. p. 265, secondo cui: «*[…] DG JUST is a consumer and not a market-oriented DG […]*».

[60] Tra gli atti più rilevanti adottati nel corso dell'*iter legis*, v. *inter alios*: UE, Garante europeo della protezione dei dati, *Opinion on the data protection reform package*, 7 marzo 2012; UE, Parere del Comitato economico e sociale europeo *in merito alla Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, GU C 229, 31 luglio 2012, pp. 90-97; UE, Comunicazione della Commissione al Parlamento europeo *a norma dell'articolo 294, paragrafo 6, del trattato sul funzionamento dell'Unione europea riguardante la posizione del Consiglio sull'adozione di un regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) e che abroga la direttiva 95/46/CE*, 11 aprile 2016, COM/2016/0214 final. In dottrina, sulla procedura che ha portato all'adozione del Regolamento, v. *inter alios*: M. Fumagalli Meraviglia, *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016, Fascicolo 1, pp. 1-39; X. Tracol, *Le règlement et la directive relatifs à la protection des données à caractère personnel*, in *Europe: actualité du droit de l'Union européenne*, 2016, Volume 26, Numero 10, pp. 5-10; G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 1-26.

[61] UE, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio *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)*, 27 aprile 2016, GU L 119, 4 maggio 2016, pp. 1-88.

[62] *Ibid*., art. 99, par. 2.

CAPITOLO II

GLI STRUMENTI DELL'ATTUALE DISCIPLINA UE

SOMMARIO: 1. Considerazioni preliminari all'analisi degli strumenti. – 1.1. Brevi cenni sul Regolamento (UE) 2016/679 nel suo insieme. – 1.2. La nozione di «trasferimento di dati personali». – 1.3. Riflessioni generali sul Capo V del Regolamento. – 2. La decisione di adeguatezza. – 2.1. Il dato testuale del GDPR: l'art. 45. – 2.2. La giurisprudenza della Corte di giustizia: le sentenze *Schrems I* e *Schrems II*. – 2.3. La prassi applicativa della Commissione: le decisioni di adeguatezza attualmente adottate. – 3. Le garanzie adeguate. – 3.1. Il dato testuale del GDPR: l'art. 46 (e l'art. 47). – 3.2. La giurisprudenza della Corte di giustizia: la sentenza *Schrems II*. – 3.3. Le Raccomandazioni dell'*European Data Protection Board* (EDPB) e le *model clauses* della Commissione. – 4. Le deroghe in specifiche situazioni: il dato testuale dell'art. 49 GDPR, gli atti dell'EDPB e la giurisprudenza della Corte di giustizia.

1. *Considerazioni preliminari all'analisi degli strumenti*

1.1. *Brevi cenni sul Regolamento (UE) 2016/679 nel suo insieme*

Prima di concentrarsi sull'attuale disciplina UE in materia di flussi di dati personali, devono essere spese alcune parole sul GDPR nel suo insieme, pur non essendo questa la sede per un'analisi approfondita di tale strumento [1]. Occorre infatti avere ben chiaro che il Regolamento (UE) 2016/679, come in parte anticipato, rafforza notevolmente la posizione delle persone i cui dati vengono trattati, in linea con l'importanza assunta nell'UE dalla protezione dei dati personali nella sua dimensione di diritto fondamentale [2]. Tale rafforzamento è ottenuto attraverso un gran numero di istituti: *inter alia*, si vuole menzionare

[1] Per un'analisi approfondita del Regolamento (UE) 2016/679, invece, v. *inter alios*: S. SICA-V. D'ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016; G. COMANDÉ-G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019; C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020.

[2] UE, Regolamento (UE) 2016/679, cit., art. 1 («Oggetto e finalità»), par. 2.

l'ambito di applicazione territoriale più ampio rispetto al passato, che tenta di estendere le tutele del Regolamento oltre i confini UE (art. 3)[3]; la chiarificazione di alcuni concetti chiave[4]; la conferma e il consolidamento dei principi che già caratterizzavano la Direttiva 95/46/CE, e prima ancora la Convenzione 108 e le Linee guida OCSE[5]; il potenziamento dei diritti degli interessati, ottenuto sia disciplinando in modo più completo e dettagliato quelli preesistenti, sia introducendone di nuovi[6]; il più esteso e puntuale catalogo degli obblighi gravanti

[3] *Ibid*., art. 3 («Ambito di applicazione territoriale»). In dottrina, sull'ambito di applicazione territoriale dell'art. 3 GDPR, v. *inter alios*: M. Gömann, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, in *Common Market Law Review*, 2017, Volume 54, Numero 2, pp. 567-590; A. Spangaro, *L'ambito di applicazione materiale della disciplina del Regolamento europeo 679/2016*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 27-62; C. Cellerino, *L'ambito di applicazione "territoriale" della normativa UE in materia di protezione dei dati personali (GDPR) e l'economia globale dei dati: quale modello regolatorio?*, in S. Dominelli-G.L. Greco (a cura di), *I mercati dei servizi fra regolazione e governance*, Giappichelli, Torino, 2020, pp. 135-156; D.J.B. Svantesson, *Article 3. Territorial Scope*, in C. Kuner-L.A. Bygrave-C. Docksey (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 74-99.

[4] Tra i concetti meglio precisati rispetto al passato si menziona il «consenso dell'interessato», definito dall'art. 4, n. 11, GDPR. In dottrina, sulle «Definizioni» fornite dall'art. 4 GDPR, v. *inter alios*: C. Del Federico-A.R. Popoli, *Le definizioni*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 63-109. Sul consenso dell'interessato, invece, v. *inter alios*: E. Costa, *Article 7. Conditions for consent*, in C. Kuner-L.A. Bygrave-C. Docksey (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 345-354.

[5] Nel GDPR, ai «Principi» è dedicato l'intero Capo II (artt. 5-11). La disposizione più rilevante in materia è certamente l'art. 5 («Principi applicabili al trattamento di dati personali»). In dottrina, su tali principi, v. *inter alios*: W. Kotschy, *The proposal for a new General Data Protection Regulation – problems solved?*, in *International Data Privacy Law*, Novembre 2014, Volume 4, Numero 4, pp. 274-281; G. Malgieri, *I principi generali del Regolamento alla base del trattamento di dati personali*, in G. Comandé-G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 16-20; C. De Terwangne, *Article 5. Principles relating to processing of personal data*, in C. Kuner-L.A. Bygrave-C. Docksey (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 309-320.

[6] Nel GDPR, ai «Diritti dell'interessato» è dedicato l'intero Capo III (artt. 12-23). Tra le disposizioni più rilevanti in materia si possono menzionare l'art. 13 («Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato»), l'art. 15 («Diritto di accesso dell'interessato»), l'art. 16 («Diritto di rettifica»), l'art. 17 («Diritto alla cancellazione («diritto all'oblio»)»), l'art. 18 («Diritto di limitazione di trattamento»), l'art. 20 («Diritto alla portabilità dei dati»), l'art. 21 («Diritto di opposizione»), l'art. 22 («Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione»). In dottrina, su tali diritti, v. *inter alios*: A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 392-472.

sulle figure di titolare e di responsabile del trattamento [7]; l'irrobustimento del ruolo delle autorità nazionali di protezione dei dati [8] e l'introduzione (al posto del Gruppo di lavoro «Articolo 29») del Comitato europeo per la protezione dei dati (CEPD o anche EDPB, ovvero «*European Data Protection Board*») [9].

Al di là di tutte le trasformazioni verificatesi, comunque, rimane centrale anche l'aspetto della libera circolazione dei dati personali all'interno dell'UE [10]. Per incentivarla, viene predisposta una serie di meccanismi aventi tutti la medesima finalità: quella di superare la frammentazione e l'incertezza giuridica, che generavano inutili costi e oneri per le imprese e le disincentivavano dall'espandere le loro attività economiche in altri Stati membri UE, e di ottenere invece – come sopra illustrato – una maggior armonizzazione, assicurando per quanto possibile un'applicazione coerente e omogenea del GDPR in tutta l'Unione [11].

---

[7] Nel GDPR, il «titolare del trattamento» è definito dall'art. 4, n. 7, mentre il «responsabile del trattamento» è definito dall'art. 4, n. 8. Alle figure di «Titolare del trattamento e responsabile del trattamento», e ai loro obblighi, è dedicato l'intero Capo IV GDPR (artt. 24-43). Tra le disposizioni più rilevanti in materia si possono menzionare l'art. 24 («Responsabilità del titolare del trattamento»), l'art. 25 («Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita»), l'art. 30 («Registri delle attività di trattamento»), l'art. 32 («Sicurezza del trattamento»), l'art. 33 («Notifica di una violazione dei dati personali all'autorità di controllo»), l'art. 34 («Comunicazione di una violazione dei dati personali all'interessato»), la Sezione 3 («Valutazione d'impatto sulla protezione dei dati e consultazione preventiva», artt. 35-36), la Sezione 4 («Responsabile della protezione dei dati», artt. 37-39), la Sezione 5 («Codici di condotta e certificazione», artt. 40-43). In dottrina, sugli obblighi di titolare e responsabile del trattamento, v. *inter alios*: M. GAGLIARDI, *Gli adempimenti previsti dal regolamento: quadro generale, registri*, in G. COMANDÉ-G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 63-67; L.A. BYGRAVE, *Data protection by design and by default*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 571-581.

[8] Nel GDPR, alle «Autorità di controllo indipendenti» è dedicato l'intero Capo VI (artt. 51-59).

[9] Nel GDPR, al «Comitato europeo per la protezione dei dati» è dedicata la Sezione 3 del Capo VII (artt. 68-76).

[10] UE, Regolamento (UE) 2016/679, cit., art. 1 («Oggetto e finalità»), par. 3.

[11] Nel GDPR, a «Cooperazione e coerenza» è dedicato l'intero Capo VII (artt. 60-76). In dottrina, sui meccanismi finalizzati ad assicurare cooperazione e coerenza, v. *inter alios*: D. MULA, *Il trattamento dei dati nel territorio dell'Unione e il meccanismo "One Stop Shop"*, in S. SICA-V. D'ANTONIO-G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016, p. 271 ss.; C. D'AGATA, *I meccanismi di comunicazione tra le Autorità di controllo*, in G. COMANDÉ-G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 89-97; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità garanti. Il meccanismo di coerenza*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 690-724.

1.2. *La nozione di «trasferimento di dati personali»*

Quanto alle regole sui «trasferimenti di dati personali verso paesi terzi», contenute come anticipato nel Capo V del GDPR (artt. 44-50), occorre preliminarmente segnalare come il Regolamento (UE) 2016/679 non contenga alcuna definizione di «trasferimento di dati personali», né all'interno della disposizione appositamente dedicata alle «Definizioni», l'art. 4, né all'interno del suddetto Capo V: una lacuna che già contraddistingueva la Direttiva 95/46/CE, ma che il legislatore UE, nonostante varie esortazioni tra cui quelle del Comitato economico e sociale europeo [12] e del Garante europeo della protezione dei dati [13], non ha provveduto a colmare.

Sul significato dell'espressione in questione era intervenuta, nella vigenza della Direttiva 95/46/CE, la Corte di giustizia dell'UE con una sentenza del 2003 nota come *Bodil Lindqvist* [14]. Tale pronuncia abbracciava una nozione restrittiva di trasferimento, ovvero «un atto mirante deliberatamente a trasferire dati personali dal territorio di uno Stato membro verso un paese terzo» [15], rimanendo invece esclusa l'attività di «messa in rete» di dati personali [16]. Una simile soluzione, tuttavia, appare oggi datata e non in linea con il più recente *trend* giurisprudenziale del Giudice di Lussemburgo, che tende invece a massimizzare il livello di protezione dei dati personali trasferiti fuori dall'UE (come si vedrà ampiamente nel proseguo), tanto che autorevole dottrina ha persino affermato che, là dove la Corte avesse modo di esprimersi nuovamente sul punto, molto

---

[12] UE, Parere del Comitato economico e sociale europeo *in merito alla Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*, cit., § 4.6.2.

[13] UE, Garante europeo della protezione dei dati, *Opinion on the data protection reform package*, cit., § 108.

[14] UE, Corte di giustizia, sentenza del 6 novembre 2003, causa C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596. In dottrina, sulla sentenza *Bodil Lindqvist*, v. *inter alios*: A. Giannaccari-T.M. Umbertazzi, *Il caso Lindqvist: i limiti della privacy europea*, in *Danno e responsabilità*, 2004, Numero 4, pp. 377-388; 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 *Giurisprudenza italiana*, 2004, pp. 1805-1809; Y. Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, in *Journal of International Commercial Law & Technology*, 2007, Volume 2, Numero 3, pp. 141-153.

[15] UE, Corte di giustizia, *Bodil Lindqvist*, cit., § 54.

[16] *Ibid*., § 71, in base a cui: «non si configura un «trasferimento verso un paese terzo di dati» […] allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet – caricata presso il suo fornitore di servizi di ospitalità («web hosting provider»), stabilito nello Stato stesso o in un altro Stato membro – dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi». Sul punto v., *inter alios*: C. D'Agata, *Flussi transfrontalieri di dati personali e ruolo del Garante*, in G. Comandé-G. Malgieri (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 97-103, spec. p. 98.

difficilmente giungerebbe alla stessa conclusione dell'epoca [17].

Nel cercare di comprendere il significato dell'espressione in esame, l'aiuto probabilmente più significativo arriva piuttosto dal Comitato europeo per la protezione dei dati e dalle sue «Linee guida 5/2021 sull'interazione tra l'applicazione dell'articolo 3 e le disposizioni in materia di trasferimenti internazionali di cui al capo V GDPR», la cui «Versione 2.0» è stata adottata il 14 febbraio 2023 [18]. Esso individua «tre criteri cumulativi […] in base ai quali un trattamento può essere considerato un trasferimento: 1) il titolare del trattamento o il responsabile del trattamento ("esportatore") è soggetto al GDPR per il trattamento in questione; 2) l'esportatore comunica mediante trasmissione o rende altrimenti disponibili a un altro titolare del trattamento, contitolare del trattamento o responsabile del trattamento ("importatore"), i dati personali oggetto del trattamento; 3) l'importatore si trova in un paese terzo, indipendentemente dal fatto che l'importatore sia o meno soggetto al GDPR per il trattamento in questione a norma dell'articolo 3 […]» [19]. Anche tale definizione, tuttavia, non è affatto esente da criticità: in modo particolare, ai sensi della stessa, non si può parlare di trasferimento qualora sia *la persona interessata* a comunicare, direttamente e di propria iniziativa, i dati personali al destinatario [20]; si finisce dunque per trattare in modo diverso una situazione simile a quelle che invece ricadono nella definizione (ovverosia, le trasmissioni di dati tra titolari o responsabili) [21]. Come autorevolmente sostenuto, non ci troviamo di fronte a una delle opere

---

[17] C. KUNER, *Article 44. General principle for transfers*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 755-770, spec. p. 763, secondo cui: «*[…] Thus, if the CJEU were faced today with a case involving facts similar to those in* Lindqvist*, it would likely be reluctant to find that the GDPR does not apply to placing personal data on an internet site […]*».

[18] UE, Comitato europeo per la protezione dei dati, *Linee guida 5/2021 sull'interazione tra l'applicazione dell'articolo 3 e le disposizioni in materia di trasferimenti internazionali di cui al capo V GDPR. Versione 2.0*, 14 febbraio 2023. In dottrina, sulle Linee guida 5/2021, v. *inter alios*: S. YAKOVLEVA, *GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives*, in *European Law Blog*, 9 dicembre 2021; C. KUNER, *Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR*, in *European Law Blog*, 13 dicembre 2021; L. DRECHSLER-S. YAKOVLEVA, *Contribution to the public consultation on the Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Institute for Information Law Research Paper No. 2022-14, Amsterdam, 2022.

[19] UE, Comitato europeo per la protezione dei dati, *Linee guida 5/2021*, cit., § 9.

[20] *Ibid*., § 18, in base a cui: «Inoltre questo secondo criterio non può considerarsi soddisfatto in mancanza di un titolare del trattamento o di un responsabile del trattamento che invii o metta a disposizione i dati a un altro titolare del trattamento o responsabile del trattamento (ossia in mancanza di un "esportatore"), ad esempio nel caso in cui il destinatario riceve i dati direttamente dall'interessato».

[21] Sul punto v.: S. YAKOVLEVA, *GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives*, cit..

meglio riuscite del Comitato (organismo che, come si vedrà, in molte altre circostanze ha invece dato un contributo essenziale al rafforzamento del diritto fondamentale alla protezione dei dati personali): le Linee guida 5/2021, pur provando a chiarire meglio determinati aspetti, come si è visto ne lasciano irrisolti altri, rischiando addirittura di creare vuoti di tutela, e non sembrano in grado di mettere la parola fine all'incertezza che da molti anni caratterizza la questione [22].

1.3. *Riflessioni generali sul Capo V del Regolamento*

Chiuso il doveroso inciso sulla nozione di «trasferimento», è bene tornare al Capo V GDPR. La disciplina ivi contenuta, che ricalca in ciò l'impostazione della Direttiva 95/46/CE, è contraddistinta dall'approccio del «divieto con deroghe» [23]. La conferma di ciò è contenuta già nell'articolo di apertura del Capo, l'art. 44, il quale è rubricato «Principio generale per il trasferimento» e prevede quanto segue: «Qualunque trasferimento di dati personali […] ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo […]» [24]. Detto in altri termini, vi è, in linea di principio, un divieto di trasmettere dati personali fuori dall'Unione. I trasferimenti diventano però consentiti in presenza delle condizioni enunciate dagli articoli successivi, le quali tuttavia sono un *numerus clausus*: al di fuori di tali ipotesi, continua dunque a vigere il divieto, non essendo possibile alcun metodo alternativo [25].

Nello specifico, i meccanismi in virtù dei quali i flussi di dati personali verso Paesi extra-UE possono avere luogo sono tre: il primo è la «decisione di adeguatezza» dell'art. 45, che la Commissione adotta nei confronti di un Paese terzo (o di un'organizzazione internazionale) che garantisca un «livello di protezione adeguato»; poi vi sono le «garanzie adeguate» dell'art. 46, strumenti di natura contrattuale, tra cui spiccano le clausole contrattuali tipo (o SCC, *standard contractual clauses*), e le norme vincolanti d'impresa (o BCR, *binding corporate rules*, art. 47); infine, si trovano le «deroghe in specifiche situazioni» dell'art. 49, ad esempio il consenso dell'interessato e la necessità del trasferimento a determinati fini.

Fra tali strumenti vi è una precisa gerarchia: là dove sussista una decisione di adeguatezza, il flusso troverà in essa il proprio fondamento. In mancanza di una decisione di adeguatezza, ma in presenza di garanzie adeguate, si ricorrerà

---

[22] C. Kuner, *Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR*, cit., secondo cui: «*[…] The Guidelines are not the EDPB's finest hour. They are unclear on some important points and allow gaps in protection, and it is unlikely that they will put an end to the confusion that has long plagued this topic […]*».

[23] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 486.

[24] UE, Regolamento (UE) 2016/679, cit., art. 44 («Principio generale per il trasferimento»).

[25] C. Kuner, *Article 44. General principle for transfers*, cit., p. 762.

a tali garanzie. Infine, là dove manchino entrambe le basi appena menzionate, si valuterà se è possibile giustificare il trasferimento con le deroghe in specifiche situazioni o se esso rimarrà proibito [26].

Il GDPR fa dunque uso di quella tecnica di regolamentazione dei flussi di dati personali che può essere definita «dall'alto verso il basso»: si parte da un elevato livello di protezione e lo si diminuisce solo a certe condizioni. Inoltre, il meccanismo principale contemplato dalla normativa – la decisione di adeguatezza – è un classico esempio di approccio «su base geografica»: si pone infatti l'enfasi sullo Stato verso cui il trasferimento è diretto, restringendo i flussi se non garantisce un certo standard.

Come già esposto, in generale tali tecniche normative sono indicative di una maggiore attenzione per l'esigenza di proteggere i dati personali degli individui rispetto a quella di favorire i flussi per ragioni di carattere commerciale. Tuttavia, non si può addivenire a una valutazione definitiva circa la disciplina in esame semplicemente sussumendo la stessa all'interno di categorie come quelle appena menzionate. Queste ultime forniscono rilevanti indizi, ma nulla più. Un'analisi più approfondita, ipoteticamente, potrebbe anche portare a riflessioni differenti.

Si pensi proprio al caso della Direttiva 95/46/CE: anch'essa, lo si è visto, poteva essere considerata un esempio di «*top-down regulatory design*» e di «*geographically-based approach*». Ciononostante, sarebbe stato avventato affermare che tale atto legislativo, nel regolamentare i flussi, attribuisse una netta prevalenza alla tutela dei diritti fondamentali anziché alle istanze economiche. La Direttiva, infatti, nasceva come strumentale alle esigenze del mercato interno e segnatamente alla libera circolazione dei dati all'interno dell'UE. Alla disciplina dei trasferimenti verso Stati terzi – lo si è detto – non era invece assegnato un ruolo di primo piano, e anzi essa appariva decisamente trascurata; una circostanza che ha cagionato disparità nell'applicazione tra i vari Stati membri e bilanciamenti tra le istanze in gioco di volta in volta differenti.

Non basta quindi soffermarsi sulla tipologia di tecnica normativa utilizzata per addivenire a conclusioni univoche in merito all'esito del bilanciamento: devono essere analizzate molte più circostanze.

A ciò si aggiunge anche un altro fattore: le normative concretamente adottate possono contenere sia elementi propri di un approccio, che elementi caratteristici di quello opposto. E un esempio è proprio rappresentato dal GDPR (che in ciò, peraltro, non differisce dalla Direttiva): è vero che la decisione di adeguatezza è un classico esempio di «*geographically-based approach*»; ma le «garanzie adeguate» di natura contrattuale, tra cui spiccano soprattutto le clausole contrattuali tipo, sono al contrario esempi di «*organizationally-based approach*», più sensibile alle esigenze economiche. Ciò vuol dire che se, ipoteticamente, la normativa e la giurisprudenza UE consentissero un ampio uso di quei meccanismi che sono espressione dell'«*organizationally-based approach*»,

[26] *Ibid*., pp. 764-765.

permettendo magari un trasferimento di massicce quantità di dati attraverso le SCC senza richiedere il rispetto di uno standard di tutela particolarmente elevato, le istanze di carattere commerciale finirebbero chiaramente per prevalere su quelle di tutela dei diritti.

In ragione di quanto appena esposto, per giungere a una valutazione più accurata circa il bilanciamento operato dalla disciplina UE in materia di flussi è necessaria un'indagine ben più approfondita dei vari strumenti contemplati dal GDPR, che non riguardi però solo il testo normativo così come adottato dal legislatore, ma anche la pertinente giurisprudenza della Corte di giustizia e gli atti di implementazione della Commissione.

2. *La decisione di adeguatezza*

2.1. *Il dato testuale del GDPR: l'art. 45*

Innanzitutto, occorre prendere le mosse dalla decisione di adeguatezza – il principale meccanismo contemplato dalla normativa – e ancor più nello specifico dal dato testuale della disposizione rilevante, l'art. 45 del Regolamento (UE) 2016/679[27].

Come si evince dall'art. 45, par. 3, GDPR, dal punto di vista squisitamente giuridico la decisione di adeguatezza è classificabile come atto di esecuzione: per la sua adozione il GDPR rinvia[28] alla «Procedura d'esame» disciplinata dal c.d. «Regolamento Comitologia»[29], nel cui ambito la Commissione è assistita da un comitato composto da rappresentanti degli Stati membri[30]. Sul progetto di atto di esecuzione, proveniente nello specifico dalla già citata Direzione generale «Giustizia e consumatori» della Commissione (DG JUST)[31], si esprime

---

[27] UE, Regolamento (UE) 2016/679, cit., art. 45 («Trasferimento sulla base di una decisione di adeguatezza»), in base a cui: «1. 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 […]».

[28] *Ibid*., art. 93 («Procedura di comitato»), par. 2.

[29] UE, Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio *che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione*, 16 febbraio 2011, GU L 55, 28 febbraio 2011, pp. 13-18.

[30] *Ibid*., art. 3 («Disposizioni comuni»), par. 2.

[31] Sul punto v., *inter alios*: N. GERLACH-J.F. KEUSTERMANS, *Europe and Japan towards the Future – the first post GDPR adequacy decision of the European Commission*, 11th Annual Sedona Conference International Programme on Cross-Border Data Transfers and Data Protection Laws, 14 giugno 2019, secondo cui: «*[…] Before approval, the initial proposal for an adequacy*

con un parere il menzionato comitato: nei casi in cui il parere sia positivo, la Commissione procede all'adozione; nel caso in cui invece il parere sia negativo, il progetto di atto di esecuzione non può essere adottato, circostanza che attribuisce agli Stati membri UE un peso decisivo [32]. Prima di adottare la decisione, la Commissione deve anche consultare il Comitato europeo per la protezione dei dati, il cui parere non è tuttavia vincolante [33].

Premesso doverosamente quanto sopra, la principale osservazione che emerge dalla lettura dell'art. 45 GDPR è che le regole ivi contenute sono assai complete e dettagliate, soprattutto se confrontate con quelle dell'art. 25 della Direttiva 95/46/CE [34].

In primis, vengono meno alcuni elementi della previgente normativa che potevano generare disparità e confusione. La Direttiva, in particolare, lasciava spazio anche agli Stati membri di effettuare autonome valutazioni di adeguatezza nei confronti di Paesi terzi; il rischio era che il livello di protezione dei dati offerto all'interessato in uno Stato extra-UE potesse essere giudicato diversamente [35]. Inoltre, si faceva riferimento all'eventualità che la Commissione constatasse che un Paese terzo *non* garantiva una protezione adeguata; non era tuttavia chiara la differenza tra uno Stato destinatario di una misura di segno negativo e uno che non avesse ricevuto alcun provvedimento [36]. Tali possibilità non sono dunque più contemplate nel GDPR [37].

Vi è inoltre una puntuale regolamentazione non solo della procedura di adozione della decisione di adeguatezza, ma anche di quelle di modifica, sospensione e revoca della stessa, che nella vigenza della Direttiva non erano esplicitamente disciplinate [38]. La decisione di adeguatezza deve essere dunque considerata uno

---

decision, which would originate with the European Commission Directorate-General for Justice and Consumers (DG JUSTICE), has to undergo a multistep formal comitology procedure […]».

[32] UE, Regolamento (UE) n. 182/2011, cit., art. 5 («Procedure d'esame»).

[33] UE, Regolamento (UE) 2016/679, cit., art. 70 («Compiti del comitato»), par. 1, lett. s).

[34] Sulle novità dell'art. 45 del Regolamento (UE) 2016/679 rispetto all'art. 25 della Direttiva 95/46/CE, v. *inter alios*: M.C. Meneghetti, *I trasferimenti di dati personali all'estero*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 594-661; C. Kuner, *Article 45. Transfers on the basis of an adequacy decision*, in C. Kuner-L.A. Bygrave-C. Docksey (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 771-796.

[35] 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 TrE-Press, Roma, 2016, pp. 169-213, spec. p. 178.

[36] Sul punto v., *inter alios*: S. Yakovleva-K. Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 2016, Volume 2, Numero 2, pp. 191-208, spec. p. 203.

[37] Sul punto v., *inter alios*: C. Kuner, *Article 45. Transfers on the basis of an adequacy decision*, cit., p. 775.

[38] Sul punto v., *inter alios*: M.C. Meneghetti, *op. cit.*, p. 623.

strumento "vivo": essa necessita di essere attentamente monitorata dalla Commissione e riconsiderata nel caso in cui intervengano sviluppi che incidano sul livello di protezione garantito dallo Stato extra-UE in questione, come ad esempio modifiche della legislazione o della prassi[39].

Si chiariscono poi le tipologie di decisione adottabili. In particolare, la misura in questione può riguardare non solo un Paese terzo, ma anche un'organizzazione internazionale. Inoltre, circostanza che sul piano pratico ha una rilevanza ben maggiore, la constatazione di adeguatezza può essere rivolta non solo a uno Stato extra-UE nella sua interezza, ma anche solo a un territorio o a uno o più settori specifici all'interno dello stesso: si parla, in questo caso, di adeguatezza parziale o settoriale[40].

L'art. 45 GDPR presenta pure un elenco, più ampio e preciso di quello precedentemente contenuto nella Direttiva, in cui figurano gli elementi che la Commissione deve prendere in considerazione per valutare se l'adeguatezza sia presente o meno. Tra questi, lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione (generale o settoriale), l'attuazione di tale legislazione, la giurisprudenza, un ricorso effettivo in sede amministrativa e giudiziaria, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti, gli impegni internazionali assunti dal Paese terzo (o dall'organizzazione internazionale) in questione. In relazione agli impegni internazionali, si dovrebbe tenere in considerazione soprattutto l'adesione degli Stati extra-UE alla Convenzione 108 del CoE e al suo Protocollo addizionale[41]: sappiamo infatti come in tali strumenti sia possibile rinvenire gran parte dei principi che caratterizzano anche la normativa UE[42]. Quest'ultima affermazione, va evidenziato, diventerebbe ancor più vera qualora entrasse in vigore la Convenzione 108+, che mira proprio a far sì che la normativa del CoE e quella UE rispecchino gli stessi principi[43].

Orbene, tale disciplina della decisione di adeguatezza, ben più solida rispetto al passato, si pone perfettamente in linea con la già menzionata valorizzazione della protezione dei dati personali nella sua dimensione di diritto fondamentale, caratteristica che permea l'intero Regolamento. È infatti chiaro che il rafforzamento della posizione delle persone interessate, ottenuto attraverso un gran numero di istituti disseminati in tutto il GDPR, finirebbe per essere vanificato là dove fosse possibile sfuggire agevolmente alle regole UE trasferendo i dati

---

[39] UE, Comunicazione della Commissione europea al Parlamento europeo e al Consiglio, *Scambio e protezione dei dati personali in un mondo globalizzato*, 10 gennaio 2017, COM/2017/07 final, § 3.1.

[40] *Ibid*.

[41] UE, Regolamento (UE) 2016/679, cit., Considerando 105.

[42] Sul punto v., *inter alios*: C. KUNER, *Transborder Data Flows and Data Privacy Law*, cit., pp. 48-49.

[43] UE, Comunicazione della Commissione europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, cit., § 3.3.1.

personali verso Paesi terzi. Le regole in questione devono dunque impedire che i flussi possano compromettere l'elevato livello di tutela delle persone fisiche assicurato nell'Unione dal Regolamento [44]: proprio per questo, esse assumono un'importanza centrale e risultano estremamente approfondite.

2.2. *La giurisprudenza della Corte di giustizia: le sentenze* Schrems I *e* Schrems II

La disciplina della decisione di adeguatezza ha però assunto una connotazione perfino più marcata grazie all'operato del Gruppo di lavoro «Articolo 29» (e poi del Comitato europeo per la protezione dei dati) [45], secondo cui un Paese terzo per essere «adeguato» deve applicare determinati principi fondamentali contraddistintivi della normativa UE [46]; ma soprattutto grazie alla giurisprudenza della Corte di giustizia dell'UE, che ancor più autorevolmente è andata a riempire di significato il termine «adeguatezza», fin da quando era ancora in vigore la Direttiva 95/46/CE.

La Corte, nelle sentenze della nota vicenda *Schrems*, ha affermato che l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che lo Stato extra-UE assicuri effettivamente un livello di protezione dei diritti fondamentali «*sostanzialmente equivalente*» a quello garantito nell'Unione europea dalla normativa in materia di dati personali letta alla luce della Carta dei diritti fondamentali dell'UE [47]. Ed è proprio attraverso tale rigorosa lettura

---

[44] Sul punto v.: UE, Regolamento (UE) 2016/679, cit., Considerando 101.

[45] UE, Gruppo di lavoro «Articolo 29», *First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy*, 26 giugno 1997, WP 4; UE, Gruppo di lavoro «Articolo 29», *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, 24 luglio 1998, WP 12; UE, Gruppo di lavoro «Articolo 29», *Criteri di riferimento per l'adeguatezza*, 28 novembre 2017 (versione emendata e adottata il 6 febbraio 2018), WP 254 rev. 01; UE, Comitato europeo per la protezione dei dati, *Endorsement 1/2018*, 25 maggio 2018.

[46] In particolare v.: UE, Gruppo di lavoro «Articolo 29», *Criteri di riferimento per l'adeguatezza*, cit., Capitolo 3, in base a cui: «[…] Il sistema di un paese terzo o di un'organizzazione internazionale deve contenere i seguenti principi di contenuto […]: 1) Nozioni […] 2) Criteri di liceità e correttezza del trattamento per fini legittimi […] 3) Il principio della finalità limitata […] 4) Il principio della qualità e della proporzionalità […] 5) Il principio della conservazione dei dati […] 6) Il principio della sicurezza e della riservatezza […] 7) Il principio di trasparenza […] 8) I diritti di accesso, rettifica, cancellazione e opposizione […] 9) Restrizioni ai trasferimenti successivi […]».

[47] UE, Corte di giustizia, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems contro Data Protection Commissioner*, ECLI:EU:C:2015:650, § 73, in base a cui: «[…] l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta

del parametro di «adeguatezza» che il Giudice di Lussemburgo è arrivato ad annullare sia la prima che la seconda decisione che la Commissione aveva adottato nei confronti degli Stati Uniti.

Si vada per ordine. Innanzitutto, la Corte si è interessata alla Decisione «Approdo sicuro» («*Safe Harbor*») del 2000[48], la quale, per superare le distanze tra i due modelli regolatori[49], andava a istituire un sistema che consentiva il trasferimento di dati personali verso le organizzazioni private USA che avessero autocertificato la propria adesione a determinati principi[50]. Tale misura, su cui avevano espresso perplessità sia il Gruppo di lavoro «Articolo 29»[51], che il Parlamento europeo[52], che certa dottrina[53], era finita ancor più sotto i riflettori

---

[…]»; UE, Corte di giustizia, sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, ECLI:EU:C:2020:559, § 94, in base a cui: «[…] A tal riguardo, senza esigere che il paese terzo considerato garantisca un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, l'espressione «livello di protezione adeguato» deve essere intesa […] nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza di tale regolamento, letto alla luce della Carta […]».

[48] UE, Decisione della Commissione 2000/520/CE *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*, 26 luglio 2000, GU L 215, 25 agosto 2000, pp. 7-47.

[49] Sulle caratteristiche della disciplina USA in materia e le differenze con quella UE, v. *inter alios*: P. SCHWARTZ, *Data Processing and Government Administration: The Failure of the American Response to the Computer*, in *Hastings Law Journal*, 1992, Volume 43, Numero 5, pp. 1321-1389; J.R. REIDENBERG, *E-Commerce and Trans-Atlantic Privacy*, in *Houston Law Review*, 2001, Volume 38, Numero 3, pp. 717-749; F. BIGNAMI, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*, 2007, Volume 48, Numero 3, pp. 609-698; G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 23-48.

[50] Sui *Safe Harbor Principles*, v. *inter alios*: S. SICA-V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, cit..

[51] UE, Gruppo di lavoro «Articolo 29», *Opinion 7/99 On the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce*, 3 dicembre 1999, WP 27, p. 13, in cui si può leggere: «*[…] the proposed "Safe Harbor" arrangements as reflected in the current versions of the various documents remain unsatisfactory […]*»; UE, Gruppo di lavoro «Articolo 29», *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*, 16 maggio 2000, WP 32, p. 7, in cui si può leggere: «*[…] the proposed adequacy "finding" refers to a system that is not yet operational […]*».

[52] UE, Risoluzione del Parlamento europeo *sul progetto di decisione della Commissione relativa all'adeguatezza della protezione garantita dai "Principi di riservatezza dell'approdo sicuro" e dalle connesse "Domande frequenti" (Frequently Asked Questions) pubblicati dal Dipartimento del commercio degli Stati Uniti (C5-0280/2000 - 2000/2144(COS))*, 5 luglio 2000.

[53] Sul punto v., *inter alios*: G. GREENLEAF, *Death of the EU Privacy Directive? Choppy waters in the Safe Harbor*, in *Privacy Law & Policy Reporter*, 1999, Volume 6, Numero 6, pp. 81-83; G.

a seguito delle note rivelazioni di Eduard Snowden, in cui erano state delineate le caratteristiche essenziali dei programmi di sorveglianza di massa posti in essere dai servizi di *intelligence* degli USA, e in particolare dalla *National Security Agency* (NSA)[54]: essi prevedevano la raccolta dei dati personali degli utenti dei servizi di telecomunicazione su larga scala e in maniera automatica, secondo la logica della «*big data surveillance*»[55]. Facendo riferimento alle suddette rivelazioni, il giurista e attivista per la *privacy* austriaco Maximillian Schrems[56] ha dato avvio a una vicenda giudiziaria che ha portato la Decisione «Approdo sicuro» a essere annullata da parte della Corte di giustizia, con la sentenza c.d. «*Schrems I*» del 6 ottobre 2015[57] (in linea, peraltro, con quanto aveva suggerito l'Avvocato generale[58]). Il Giudice di Lussemburgo ha infatti ritenuto che, nell'ordinamento statunitense, le deroghe e le restrizioni alla tutela dei dati personali per motivi di sicurezza nazionale non operassero nei limiti dello stretto necessario[59]. La normativa USA consentiva anzi alle autorità pubbliche di accedere

---

GREENLEAF, *Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$*, in *Privacy Law & Policy Reporter*, 2000, Volume 7, Numero 3, pp. 45-47.

[54] Sui programmi di sorveglianza di massa posti in essere dagli USA, v. *inter alios*: C. BOWDEN, *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Document requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Bruxelles, 2013; D.S. KRIS, *On the Bulk Collection of Tangible Things*, in *Journal of National Security Law & Policy*, 2014, Volume 7, Numero 2, pp. 209-295; F. BIGNAMI-G. RESTA, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *Law and Contemporary Problems*, 2015, Volume 78, Numero 4, pp. 231-266; C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza* Safe Harbor *della Corte di giustizia dell'Unione Europea*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 49-71.

[55] Sulla «*big data surveillance*», v. *inter alios*: M. HU, *Small Data Surveillance v. Big Data Cybersurveillance*, in *Pepperdine Law Review*, 2015, Volume 42, Numero 4, pp. 773-844.

[56] Sulla figura di Maximillian Schrems, v. *inter alia*: *Chi è Max Schrems, l'attivista che inguaia Zuckerberg*, in *Il Sole 24 Ore*, 10 ottobre 2015, consultabile al seguente link: *https://st.ilsole24ore.com/art/tecnologie/2015-10-06/la-battaglia-la-privacy-max-schrems-113708.shtml?uuid=ACkBCxAB* (ultimo accesso in data 31 dicembre 2024).

[57] UE, Corte di giustizia, *Maximillian Schrems contro Data Protection Commissioner*, 2015, cit., § 106, in base a cui: «Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida». In dottrina, sulla sentenza *Schrems I*, v. *inter alios*: V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso* Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 7-22.

[58] UE, Avvocato generale Yves Bot, conclusioni del 23 settembre 2015, causa C-362/14, *Maximillian Schrems contro Data Protection Commissioner*, ECLI:EU:C:2015:627, § 237, in base a cui: «[…] La 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, è invalida».

[59] UE, Corte di giustizia, *Maximillian Schrems contro Data Protection Commissioner*, 2015,

in maniera generalizzata al contenuto delle comunicazioni elettroniche e non prevedeva alcuna possibilità per il singolo di avvalersi di rimedi giuridici: era così pregiudicato il contenuto essenziale dei diritti fondamentali sanciti dalla Carta agli articoli 7, 8, nonché 47 (riguardante il diritto a un ricorso effettivo e a un giudice imparziale) [60].

Successivamente, la Corte di giustizia si è occupata anche della Decisione «Scudo UE-USA per la privacy» («*EU-US Privacy Shield*») del 2016 [61]. Quest'ultima, come suggerito dal Gruppo di lavoro «Articolo 29» [62] e come preannunciato dalla medesima Commissione subito all'indomani della sentenza *Schrems I* [63], pur prevedendo un meccanismo pressoché analogo a quello della Decisione «*Safe Harbor*», aveva cercato di correggere i principali difetti della precedente misura [64]. Erano rimaste tuttavia alcune criticità, come evidenziato anche dallo

---

cit., § 92, in base a cui: «[…] Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario […]».

[60] *Ibid*., §§ 93-95.

[61] UE, Decisione di esecuzione (UE) 2016/1250 della Commissione 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*, 12 luglio 2016, GU L 207, 1° agosto 2016, pp. 1-112.

[62] UE, Gruppo di lavoro «Articolo 29», *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, 16 ottobre 2015, p. 1, in base a cui: «*[…] the Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights. Such solutions could be found through the negotiations of an intergovernmental agreement providing stronger guarantees to EU data subjects. The current negotiations around a new Safe Harbour could be a part of the solution. In any case, these solutions should always be assisted by clear and binding mechanisms and include at least obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights […]*».

[63] UE, Comunicazione della Commissione *relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America*, 6 novembre 2015, COM/2015/566 final.

[64] Sul punto v.: UE, Comunicato stampa della Commissione europea, *La Commissione europea e gli Stati Uniti concordano un nuovo quadro per i flussi transatlantici di dati: lo scudo UE-USA per la privacy*, 2 febbraio 2016, in base a cui: «Il nuovo regime prevede: - obblighi severi per le imprese che trattano dati personali di cittadini europei e un controllo rigoroso del rispetto di tali obblighi […]; - chiare garanzie e obblighi di trasparenza per l'accesso del governo degli Stati Uniti […]; - una protezione efficace dei diritti dei cittadini dell'UE e diverse possibilità di ricorso […]». In dottrina, sul *Privacy Shield* v., *inter alios*: M.A. Weiss-K. Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, Congressional Research Service Report, 19 maggio 2016; S. Saluzzo, *Tutela dei dati personali e deroghe in materia di sicurezza nazionale dopo l'entrata in vigore del Privacy Shield*, in *SIDIBlog*, 13 settembre 2016; 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 *Il diritto dell'Unione europea*, 2016, Numero 4, pp. 755-787; N. Pupalova, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?*, University of Oslo, Oslo, 2017; F. Terpan, *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?*, in *European Papers*, 2018, Volume 3, Numero 3, pp. 1045-1059.

stesso Gruppo di lavoro [65], nonché dal Parlamento europeo [66]. Così, sempre su iniziativa di Maximillian Schrems, anche tale seconda misura è stata sottoposta al Giudice di Lussemburgo e, per ragioni simili a quelle viste poc'anzi, è stata dichiarata invalida con la sentenza c.d. «*Schrems II*» del 20 luglio 2020 [67] (nonostante le conclusioni in senso contrario dell'Avvocato generale [68]). Infatti, le limitazioni ai diritti degli articoli 7 e 8 della Carta, derivanti dalla normativa USA in materia di sorveglianza a fini di sicurezza nazionale, ancora una volta non corrispondevano a requisiti «sostanzialmente equivalenti» a quelli richiesti, nel diritto UE, dall'art. 52, par. 1, della Carta stessa; non rispettavano, cioè, il principio di proporzionalità, in quanto non si limitavano allo stretto necessario [69]. Inoltre, il *Privacy Shield* non forniva mezzi di ricorso di fronte a un organo in grado di offrire agli individui garanzie «sostanzialmente equivalenti» a quelle richieste dall'art. 47 della Carta [70].

---

[65] UE, Gruppo di lavoro «Articolo 29», *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 13 aprile 2016, WP 238. In particolare, v. p. 57, in base a cui: «*[…] the WP29 understands […] that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data. The WP29 has consistently held that such data collection, is an unjustified interference with the fundamental rights of individuals […]*».

[66] UE, Risoluzione del Parlamento europeo *sui flussi di dati transatlantici (2016/2727(RSP))*, 26 maggio 2016. In particolare, v. § 4, in base a cui: «[…] l'allegato VI […] chiarisce che […] la raccolta di massa di dati e comunicazioni personali di cittadini non statunitensi è ancora autorizzata in sei casi; […] tale raccolta generalizzata deve essere soltanto "per quanto possibile mirata" e "ragionevole", e quindi non risulta conforme ai più rigorosi criteri di necessità e proporzionalità stabiliti nella Carta».

[67] UE, Corte di giustizia, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, 2020, cit., § 201, in base a cui: «Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione «scudo per la privacy» è invalida». In dottrina, sulla sentenza *Schrems II*, v. *inter alios*: G. Caggiano, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza* Schrems II *della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, Volume XV, Numero 3, pp. 563-585; R.A. Costello, *Schrems II: Everything is Illuminated?*, in *European Papers*, 2020, Volume 5, Numero 2, pp. 1045-1059; C. Kuner, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 17 luglio 2020; M. Nino, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, Volume 14, Numero 3, pp. 733-759.

[68] UE, Avvocato generale Henrik Saugmandsgaard Øe, conclusioni del 19 dicembre 2019, causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, ECLI:EU:C:2019:1145.

[69] UE, Corte di giustizia, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, 2020*,* § 185, in base a cui: «In tali circostanze, le limitazioni alla protezione dei dati personali, che derivano dalla normativa interna degli Stati Uniti in materia di accesso e utilizzo, da parte delle autorità pubbliche statunitensi, di tali dati trasferiti dall'Unione verso gli Stati Uniti e che la Commissione ha valutato nella decisione «scudo per la privacy», non sono inquadrate in modo da corrispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dall'articolo 52, paragrafo 1, seconda frase, della Carta».

[70] *Ibid*., § 197, in base a cui: «[…] il meccanismo di mediazione di cui alla decisione «scudo per la privacy» non fornisce mezzi di ricorso dinanzi a un organo che offra alle persone i cui

In definitiva la Corte, mediante la valorizzazione degli articoli 7 e (soprattutto) 8 della Carta, ha compiuto una vera e propria opera di innalzamento del parametro di «adeguatezza» in uno di «sostanziale equivalenza», al fine di assicurare anche fuori dall'UE la continuità del livello di protezione ivi garantito. Tale lettura ha portato, *de facto*, a valutare l'ordinamento statunitense alla luce dei principi caratterizzanti quello dell'Unione e, conseguentemente, a dichiarare invalide entrambe le Decisioni «Approdo sicuro» e «Scudo UE-USA per la privacy». L'interpretazione appena descritta – perfettamente in linea con il progressivo rafforzamento della *data protection* nella sua dimensione di diritto fondamentale che ha caratterizzato l'Unione fin dall'inizio del III millennio – risulta dunque indubbiamente a favore della tutela delle persone fisiche, e ciò anche a costo di sacrificare le esigenze economiche rappresentate dalla necessità di incentivare quanto più possibile i flussi transfrontalieri [71].

Per comprendere ancora meglio la giurisprudenza *Schrems*, inoltre, occorre ricordare come essa non sia di certo isolata rispetto al resto dell'operato della Corte di giustizia. Al contrario, si colloca in un filone giurisprudenziale che ha preso avvio nel 2014 e nell'ambito del quale il Giudice di Lussemburgo si è mosso nella prospettiva di ampliare il più possibile il margine della protezione dei dati personali accordata agli individui, sempre attraverso la massima valorizzazione degli articoli 7 e 8 della Carta [72]. Di tale filone fanno parte le pronunce *Digital Rights Ireland* [73], *Google Spain* [74], *Tele2 Sverige* [75], *Google*

---

dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta».

[71] Sul punto v., *inter alios*: O. Pollicino-M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta-V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 73-112.

[72] *Ibid*., p. 75.

[73] UE, Corte di giustizia, sentenza del 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, ECLI:EU:C:2014:238.

[74] UE, Corte di giustizia, sentenza del 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, ECLI:EU:C:2014:317. In particolare, v. § 97 e § 99, in base a cui i «diritti fondamentali derivanti dagli articoli 7 e 8 della Carta […] prevalgono, in linea di principio, […] sull'interesse economico del gestore del motore di ricerca […]». In dottrina, sulla sentenza *Google Spain*, v. *inter alios*: G. Finocchiaro, *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: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 113-135; O. Pollicino, *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, 16 ottobre 2019, Numero 19.

[75] UE, Corte di giustizia, sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB contro Post-och telestyrelsen, e Secretary of State for the Home Department contro Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970. In dottrina, sulla sentenza

contro *CNIL*[76], nonché il Parere 1/15[77]. Anche nelle citate sentenze, le ragioni dei diritti fondamentali finiscono costantemente per prevalere di fronte alle esigenze contrapposte[78]: in particolare, tra gli interessi che vengono sacrificati, troviamo quello alla sorveglianza a fini di sicurezza e di lotta alla criminalità; ma, circostanza ancor più rilevante ai nostri fini, a soccombere sono anche le esigenze di carattere economico[79].

2.3. *La prassi applicativa della Commissione: le decisioni di adeguatezza attualmente adottate*

La decisione di adeguatezza richiede dunque, ai sensi della disciplina UE e (ancor di più) della giurisprudenza della Corte di giustizia, uno standard di protezione elevatissimo. Ciò la rende estremamente difficile da adottare: nel momento in cui si scrive, la Commissione, all'interno della quale la Direzione competente è DG JUST (come si è detto), ha indirizzato tale misura solo nei confronti di 15 Stati extra-UE.

Sul punto, giova preliminarmente ricordare come non vi sia alcuna necessità di adottare una decisione di adeguatezza nei confronti dei tre Paesi dell'Associazione europea di libero scambio (EFTA) membri dello Spazio economico europeo (SEE): Islanda, Liechtenstein e Norvegia[80]. Con la Decisione del Comitato misto SEE N. 154/2018[81], infatti, il Regolamento (UE) 2016/679 è stato inte-

---

Tele2 Sverige, v. *inter alios*: E. Spiller, *La sentenza Tele2 Sverige: verso una* Digital Rule of Law *europea?*, in *IANUS*, 2017, Numero 15-16, pp. 279-309.

[76] UE, Corte di giustizia, sentenza del 24 settembre 2019, causa C-507/17, *Google LLC contro Commission nationale de l'informatique et des libertés* (CNIL), ECLI:EU:C:2019:772. In particolare, v. § 45, in base a cui i «diritti fondamentali derivanti dagli articoli 7 e 8 della Carta […] prevalgono, in linea di principio […] sull'interesse economico del gestore del motore di ricerca».

[77] UE, Corte di giustizia, Parere del 26 luglio 2017, 1/15, ECLI:EU:C:2017:592. In dottrina, sul Parere 1/15, v. *inter alios*: M. Mendez, *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, in *European Papers*, Volume 2, Numero 3, pp. 803-818; C. Kuner, *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 2018, Volume 55, Numero 3, pp. 857-882.

[78] O. Pollicino-M. Bassini, *La Corte di giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 9 gennaio 2017, p. 9.

[79] O. Pollicino-M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit., pp. 89-90.

[80] Sul punto v., *inter alios*: C. Kuner, *Article 45. Transfers on the basis of an adequacy decision*, cit., p. 786, secondo cui: «*[…] no adequacy decision is needed with regard to data transfers to the three EEA countries […]*».

[81] SEE, Decisione del Comitato misto SEE N. 154/2018 *che modifica l'allegato XI (Comunicazione elettronica, servizi audiovisivi e società dell'informazione) e il protocollo 37 (contenente l'elenco di cui all'articolo 101) dell'accordo SEE*, 6 luglio 2018, GU L 183, 19 luglio 2018, pp. 23-26.

grato nell'Accordo SEE [82]: ciò comporta, *inter alia*, che ai tre Stati appena citati si applichino le stesse norme in materia di trasferimenti transnazionali di dati personali che si applicano ai 27 Paesi dell'UE [83].

Quanto alle decisioni di adeguatezza concretamente adottate, la Commissione le classifica in tre categorie. La prima comprende quelle nei confronti di Paesi «che sono strettamente integrati con l'Unione europea e i suoi Stati membri» [84]: ci si riferisce, segnatamente, a Svizzera (2000) [85], Guernsey (2003) [86], Isola di Man (2004) [87], Jersey (2008) [88], Isole Fær Øer (2010) [89] e Andorra (2010) [90]. In tutti questi casi la Commissione, forte di un parere positivo del Gruppo di lavoro «Articolo 29» [91], non ha avuto particolari difficoltà a valutare come adeguata la protezione fornita: proprio per il fatto che i Paesi in questione sono strettamente integrati con l'UE e i suoi Stati membri, le loro norme in materia sono basate su quelle dell'Unione [92], talvolta addirittura «ampiamente

---

[82] SEE, *Accordo sullo Spazio economico europeo*, 2 maggio 1992, Oporto, GU L 1, 3 gennaio 1994, pp. 3-570.

[83] Sul punto v., *inter alios*: M.C. MENEGHETTI, *op. cit.*, p. 605.

[84] UE, Comunicazione della Commissione europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, cit., § 3.1.

[85] UE, Decisione della Commissione 2000/518/CE *riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE*, 26 luglio 2000, GU L 215, 25 agosto 2000, pp. 1-3.

[86] UE, Decisione della Commissione 2003/821/CE *sulla adeguata protezione dei dati personali in Guernsey*, 21 novembre 2003, GU L 308, 25 novembre 2003, pp. 27-28.

[87] UE, Decisione della Commissione 2004/411/CE *sulla adeguata protezione dei dati personali nell'Isola di Man*, 28 aprile 2004, GU L 151, 30 aprile 2004, pp. 50-53.

[88] UE, Decisione della Commissione 2008/393/CE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali a Jersey*, 8 maggio 2008, GU L 138, 28 maggio 2008, pp. 21-23.

[89] UE, Decisione della Commissione 2010/146/UE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione fornita dalla legge delle Isole Fær Øer sul trattamento dei dati personali*, 5 marzo 2010, GU L 58, 9 marzo 2010, pp. 17-19.

[90] UE, Decisione della Commissione 2010/625/UE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali ad Andorra*, 19 ottobre 2010, GU L 277, 21 ottobre 2010, pp. 27-29.

[91] UE, Gruppo di lavoro «Articolo 29», *Opinion No 5/99 on the level of protection of personal data in Switzerland*, 7 giugno 1999, WP 22; UE, Gruppo di lavoro «Articolo 29», *Opinion 5/2003 on the level of protection of personal data in Guernsey*, 13 giugno 2003, WP 79; UE, Gruppo di lavoro «Articolo 29», *Opinion 6/2003 on the level of protection of personal data in the Isle of Man*, 21 novembre 2003, WP 82; UE, Gruppo di lavoro «Articolo 29», *Opinion 8/2007 on the level of protection of personal data in Jersey*, 9 ottobre 2007, WP 141; UE, Gruppo di lavoro «Articolo 29», *Opinion 9/2007 on the level of protection of personal data in the Faroe Islands*, 9 ottobre 2007, WP 142; UE, Gruppo di lavoro «Articolo 29», *Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra*, 1° dicembre 2009, WP 166.

[92] In particolare v.: UE, Decisione della Commissione 2003/821/CE, cit., Considerando 7; UE, Decisione della Commissione 2004/411/CE, cit., Considerando 7.

basate» [93], e ne ricalcano dunque i più importanti principi.

La seconda categoria annovera invece le decisioni concernenti Paesi che hanno avuto, qualche anno fa, «un ruolo di pioniere nell'elaborazione di leggi sulla protezione dei dati nella loro regione» [94], ovverosia Uruguay (2012) [95] e Nuova Zelanda (2013) [96]. A seguito anche in questi casi di pareri favorevoli del Gruppo di lavoro [97], la Commissione ha ritenuto che, nonostante la significativa lontananza dagli ordinamenti europei dei sistemi in questione, questi ultimi fossero particolarmente all'avanguardia e presentassero quei principi fondamentali caratteristici di un livello di protezione adeguato [98]. Ciò anche grazie alla familiarità dei due Stati con gli strumenti internazionali in materia: l'Uruguay è stato infatti il primo Paese non europeo a ratificare la Convenzione 108 e il relativo Protocollo [99], mentre la normativa neozelandese è stata fortemente influenzata dai principi delle Linee guida OCSE [100]. Occorre tuttavia evidenziare, a onor del vero, che le due misure in questione sono estremamente brevi e scarne, caratteristica che peraltro accomuna tutte le decisioni adottate nella vigenza della Direttiva. Specie in ragione della distanza degli ordinamenti in questione da quelli UE, sarebbe stato forse lecito aspettarsi una motivazione più approfondita.

La terza e ultima categoria, infine, è quella che include le decisioni riguardanti «importanti partner commerciali» dell'Unione europea [101]. Si tratta di

---

[93] In particolare, v.: UE, Decisione della Commissione 2008/393/CE, cit., Considerando 7; UE, Decisione della Commissione 2010/625/UE, cit., Considerando 7.

[94] UE, Comunicazione della Commissione europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, cit., § 3.1.

[95] UE, Decisione di esecuzione della Commissione 2012/484/UE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica orientale dell'Uruguay in relazione al trattamento automatizzato di tali dati*, 21 agosto 2012, GU L 227, 23 agosto 2012, pp. 11-14.

[96] UE, Decisione di esecuzione della Commissione 2013/65/UE *a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Nuova Zelanda*, 19 dicembre 2012, GU L 28, 30 gennaio 2013, pp. 12-14.

[97] UE, Gruppo di lavoro «Articolo 29», *Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay*, 12 ottobre 2010, WP 177; UE, Gruppo di lavoro «Articolo 29», *Opinion 11/2011 on the level of protection of personal data in New Zealand*, 4 aprile 2011, WP 182.

[98] In particolare v.: UE, Decisione di esecuzione della Commissione 2012/484/UE, cit., Considerando 9; UE, Decisione di esecuzione della Commissione 2013/65/UE, cit., Considerando 10.

[99] Sul punto v.: UE, Decisione di esecuzione della Commissione 2012/484/UE, cit., Considerando 13.

[100] UE, Gruppo di lavoro «Articolo 29», *Opinion 11/2011 on the level of protection of personal data in New Zealand*, cit., p. 2 e p. 15.

[101] UE, Comunicazione della Commissione europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, cit., § 3.1.

Canada (2002) [102], Argentina (2003) [103], Israele (2011) [104], Giappone (2019) [105], Regno Unito (2021) [106], Repubblica di Corea (2022) [107], nonché, nel momento in cui si scrive, Stati Uniti: pur avendo la saga *Schrems* portato all'annullamento sia del «*Safe Harbor*» che del «*Privacy Shield*» (come illustrato), nel 2023 la Commissione ha adottato una terza decisione di adeguatezza, meglio nota con il nome di «*EU-US Data Privacy Framework*» (su cui *infra*) [108].

L'adozione delle misure rientranti in quest'ultima categoria ha spesso reso necessaria l'elaborazione di soluzione creative, come le già menzionate decisioni settoriali, poiché sarebbe stato impossibile valutare come adeguato l'ordinamento del Paese terzo nella sua interezza.

Lo si può vedere, innanzitutto, per la decisione concernente il Canada: come peraltro era stato suggerito pure dal Gruppo di lavoro [109], essa copre soltanto i trasferimenti a destinatari soggetti al «*Canadian Personal Information Protection and Electronic Documents Act*» (PIPEDA) [110], ovverosia «organizzazioni del settore privato che rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali», rimanendo esclusi gli altri

---

[102] UE, Decisione della Commissione 2002/2/CE *conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)*, 20 dicembre 2001, GU L 2, 4 gennaio 2002, pp. 13-16.

[103] UE, Decisione della Commissione 2003/490/CE *conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina*, 30 giugno 2003, GU L 168, 5 luglio 2003, pp. 19-22.

[104] UE, Decisione della Commissione 2011/61/UE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte dello Stato d'Israele in relazione al trattamento automatizzato di tali dati*, 31 gennaio 2011, GU L 27, 1° febbraio 2011, pp. 39-42.

[105] UE, Decisione di esecuzione (UE) 2019/419 della Commissione *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone a norma della legge sulla protezione delle informazioni personali*, 23 gennaio 2019, GU L 76, 19 marzo 2019, pp. 1-58.

[106] UE, Regolamento di esecuzione (UE) 2021/1772 della Commissione *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito*, 28 giugno 2021, GU L 360, 11 ottobre 2021, pp. 1-68.

[107] UE, Decisione di esecuzione (UE) 2022/254 della Commissione *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica di Corea nel quadro della legge sulla protezione delle informazioni personali [notificata con il numero C(2021) 9316]*, 17 dicembre 2021, GU L 44, 24 febbraio 2022, pp. 1-90.

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

[109] UE, Gruppo di lavoro «Articolo 29», *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, 26 gennaio 2001, WP 39.

[110] UE, Decisione della Commissione 2002/2/CE, cit., art. 1.

destinatari [111]. Un discorso assai simile vale anche per la misura riguardante Israele: in linea anche in questo caso con il parere del Gruppo [112], essa non si applica qualora il trasferimento dall'UE e il successivo trattamento siano effettuati esclusivamente tramite strumenti non automatizzati [113].

Ancor più complessa è poi la vicenda che coinvolge il Giappone [114]. Con riguardo a tale Stato, in primo luogo, è stato necessario adottare una decisione settoriale – peraltro confermata *in toto* nell'aprile 2023 a seguito di riesame della Commissione [115], su cui non sono mancati i rilievi dell'EDPB [116]– che copre esclusivamente i trasferimenti a operatori economici che gestiscono informazioni personali, cosiddetti «PIHBO», soggetti alla legge detta «APPI» (Legge sulla protezione delle informazioni personali); è invece escluso il trattamento di dati che rientra nell'ambito di applicazione di altre leggi, che pure sono presenti [117]. In secondo luogo, soprattutto, è stato indispensabile completare l'ordinamento giapponese con delle «Norme integrative» (adottate da un'autorità di controllo indipendente, la Commissione per la protezione delle informazioni personali o «PPC»), applicabili esclusivamente ai dati trasferiti dall'UE; al contrario, esse non si applicano ai dati personali dei singoli in Giappone o provenienti da Paesi diversi da quelli dell'Unione (*rectius*, del SEE) [118]. Solo ricorrendo a tali tecniche è stato possibile addivenire a una valutazione di adeguatezza [119]. Si tratta, tuttavia, di un'architettura che non convince pienamente né il Comitato europeo per la protezione dei dati [120], né il Parlamento europeo [121], i

---

[111] *Ibid*., Considerando 5.

[112] UE, Gruppo di lavoro «Articolo 29», *Opinion 6/2009 on the level of protection of personal data in Israel*, 1° dicembre 2009, WP 165.

[113] UE, Decisione della Commissione 2011/61/UE, cit., art. 1, par. 1.

[114] Sulla decisione di adeguatezza adottata nei confronti del Giappone, v. *inter alios*: G. Greenleaf, *Japan and Korea: Different paths to EU adequacy*, in *Privacy Laws & Business International Report*, 2018, Numero 156, pp. 9-11; F.Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, in *Harvard Journal of Law & Technology*, 2020, Volume 33, Numero 2, pp. 661-691.

[115] UE, Relazione della Commissione al Parlamento europeo e al Consiglio *sul primo riesame del funzionamento della decisione di adeguatezza relativa al Giappone*, 3 aprile 2023, COM/2023/275 final; UE, Commissione europea, *Commission Staff Working Document accompanying the document "Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan"*, 3 aprile 2023, SWD/2023/75 final.

[116] UE, Comitato europeo per la protezione dei dati, *Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan*, 18 luglio 2023.

[117] Sul punto v.: UE, Decisione di esecuzione (UE) 2019/419, cit., Considerando 9.

[118] Sul punto v.: UE, Decisione di esecuzione (UE) 2019/419, cit., Considerando 15.

[119] *Ibid*., art. 1, par. 1.

[120] UE, Comitato europeo per la protezione dei dati, *Parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone*, 5 dicembre 2018.

[121] UE, Risoluzione del Parlamento europeo *sull'adeguatezza della protezione dei dati personali offerta dal Giappone (2018/2979(RSP))*, 13 dicembre 2018.

quali non si sono espressi favorevolmente sul punto. In particolare, una decisione così strutturata solleva seri interrogativi circa la sua attuazione operativa, essendovi il concreto rischio di elusione degli obblighi previsti dalle Norme integrative [122]. Peraltro, le medesime criticità, i.e. l'ambito di applicazione limitato e il ricorso a «Garanzie supplementari», interessano anche la decisione di adeguatezza concernente la Repubblica di Corea [123], con ogni probabilità in misura minore, in ragione del più elevato livello di protezione garantito in quest'ultimo Paese [124].

È stato necessario trovare una soluzione creativa pure nel caso del Regno Unito: al fine di dare una risposta ad almeno alcuni dei rilievi critici formulati sempre dall'EDPB [125] e (in modo ancor più netto) dal Parlamento [126], la Commis-

---

[122] Sul punto v.: UE, Comitato europeo per la protezione dei dati, *Parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone*, cit., § 30, in base a cui: «[…] a seguito di una attenta analisi del progetto di decisione di adeguatezza della Commissione nonché del quadro giuridico giapponese per la protezione dei dati, il CEPD rileva la persistenza di un certo numero di preoccupazioni, congiuntamente alla necessità di ulteriori chiarimenti. Inoltre, questa specifica tipologia di adeguatezza, che combina un quadro nazionale esistente con ulteriori norme specifiche, solleva anche interrogativi circa la sua attuazione operativa […]»; UE, Risoluzione del Parlamento europeo *sull'adeguatezza della protezione dei dati personali offerta dal Giappone*, cit., § 12, in base a cui: «[…] le ulteriori tutele previste dalle disposizioni complementari sono limitate ai dati personali trasferiti dall'Europa, per cui gli operatori economici che devono trattare contemporaneamente dati personali giapponesi ed europei saranno obbligati a conformarsi alle disposizioni complementari, garantendo, ad esempio, mezzi tecnici ("tagging") od organizzativi (ad esempio, la conservazione in una banca dati dedicata) per poter identificare tali dati personali durante tutto il loro "ciclo di vita"; invita la Commissione a monitorare la situazione onde evitare potenziali scappatoie che consentirebbero agli operatori di eludere gli obblighi previsti dalle disposizioni complementari trasferendo i dati attraverso paesi terzi».

[123] UE, Decisione di esecuzione (UE) 2022/254, cit., art. 1, par. 1. Sul punto v.: UE, Comitato europeo per la protezione dei dati, *Parere 32/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nella Repubblica di Corea*, 24 settembre 2021.

[124] Sul punto v.: G. Greenleaf, *The Draft Korea Adequacy Decision: Submission to European Union Authorities*, in *University of New South Wales Law Research Series*, 2021, Numero 52, p. 14, secondo cui: «*Korea has had the strongest data privacy law in Asia for the past decade, together with the most effective enforcement. Once the 2020 legislative reforms remedied the mis-match between the EU's requirements for an independent DPA, and the distribution of enforcement powers within Korea, the country was well-positioned to be the subject of a positive adequacy Decision. The Commission's positive Decision concerning Korea's data protection system sets out a strong case for Korea providing adequate protection, but has shortcomings […]. It is unlikely that a stronger case could be made for any other country in the Asia-Pacific. The Korea Decision […] is far more convincing than the Commission's Japan Decision […]*».

[125] UE, Comitato europeo per la protezione dei dati, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 13 aprile 2021.

[126] UE, Risoluzione del Parlamento europeo *sull'adeguata protezione dei dati personali da parte del Regno Unito (2021/2594(RSP))*, 21 maggio 2021. In dottrina, su tale Risoluzione del Parlamento europeo, v. *inter alios*: A. Bowering, *Data adequacy: Doubts cast on UK's commitment to privacy protection*, in *UCL Europe Blog*, 7 giugno 2021.

sione ha escluso dall'ambito di applicazione della relativa decisione di adeguatezza [127] i trasferimenti di dati personali verso il Regno Unito a fini di controllo dell'immigrazione, ai quali può applicarsi la troppo ampia «esenzione per motivi di immigrazione» rispetto a determinati diritti degli interessati prevista dalla normativa UK [128]. Ciò potrebbe comportare, anche in questo caso, problemi sul piano dell'attuazione operativa: vi è infatti il timore che i dati trasferiti dall'Unione possano comunque rientrare, in alcuni casi, nell'ambito di applicazione dell'«*immigration exemption*», circostanza che determinerebbe un'eccessiva compressione dei diritti delle persone interessate [129].

Alcune riflessioni le merita anche la decisione di adeguatezza che, nonostante le vicende della saga *Schrems*, interessa attualmente gli Stati Uniti. Dopo l'annullamento del «*Privacy Shield*», le parti hanno intensificato i dialoghi al fine di addivenire a una nuova misura rispettosa delle pronunce rese dalla Corte di giustizia. In data 7 ottobre 2022, il Presidente USA Joseph R. Biden Jr. ha firmato l'«*Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*», finalizzato a rafforzare la *privacy* degli individui nell'ambito delle attività di *intelligence* e, ancor più nello specifico, ad assicurare che tali attività siano necessarie e proporzionate al perseguimento di obiettivi di sicurezza nazionale ben definiti, nonché a istituire opportuni meccanismi di ricorso e di vigilanza [130]. Ritenendo tali modifiche normative soddisfacenti, il 10 luglio 2023 la Commissione ha adottato il «*Data Privacy Framework*», decisione di adeguatezza che si basa su un meccanismo assai simile a quello delle due precedenti: essa consente infatti i trasferimenti di dati personali dall'UE alle organizzazioni statunitensi che, essendosi volontariamente impegnate a rispettare un insieme di principi [131], sono inserite nell'elenco degli aderenti al quadro per la protezione dei dati personali («*Data Privacy Framework List*») [132]. Non si può però dire che le criticità siano definitivamente superate: come evidenziato dall'EDPB, nonostante il decreto presidenziale abbia introdotto miglioramenti sostanziali, si renderà necessario monitorare quanto nella prassi tali modifiche saranno effettivamente in grado di limitare le attività di *intelligence* [133]. Peraltro,

---

[127] Si precisa che la decisione di adeguatezza riguardante il Regno Unito, ai sensi del suo art. 4, scadrà, salvo proroghe, il 27 giugno 2025 (c.d. «*sunset clause*»). Tale termine di scadenza rappresenta un *unicum* per una decisione di adeguatezza.

[128] UE, Regolamento di esecuzione (UE) 2021/1772, cit., art. 1.

[129] A. Choromidou, *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS*, in *International Data Privacy Law*, 2021.

[130] Sull'*Executive Order* del President Biden, v. *inter alios*: G. Scorza, *Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire*, in *AgendaDigitale*, 10 ottobre 2022; H. Ruschemeier, *Nothing new in the west? The executive order on US surveillance activities and the GDPR*, in *European Law Blog*, 14 novembre 2022.

[131] UE, Decisione di esecuzione (UE) 2023/1795, cit., Considerando 9.

[132] *Ibid*., art. 1.

[133] UE, Comitato europeo per la protezione dei dati, *Parere 5/2023 relativo al progetto di*

dopo il primo anno di funzionamento della decisione e dunque nella seconda metà del 2024, la Commissione ha già svolto una prima revisione della medesima, con esito positivo [134], ma l'EDPB ha comunque invitato a continuare tale opera di monitoraggio [135].

Si coglie a questo punto l'occasione per evidenziare come, in verità, alcune problematiche circa la sorveglianza da parte delle autorità pubbliche si pongano non solo per gli Stati Uniti, ma anche riguardo ad altri Paesi nei confronti dei quali la Commissione ha adottato decisioni appartenenti alla seconda e alla terza delle illustrate categorie: basti pensare che non solo gli USA, ma anche Canada, Nuova Zelanda e Regno Unito fanno parte (insieme all'Australia) dei cosiddetti «Cinque Occhi» o «*Five Eyes*», un gruppo ristretto di Paesi impegnati in programmi di sorveglianza di massa [136]. Ma considerazioni simili possono essere fatte, ad esempio, anche per Israele. Si tratta, in buona sostanza, di ordinamenti strutturati in maniera tale da garantire la prevalenza delle esigenze di sicurezza dello Stato su quelle di salvaguardia della *privacy* individuale [137]. Nonostante ciò, il fatto che l'accesso ai dati da parte delle autorità non determini ingerenze sproporzionate nei diritti degli interessati è un aspetto che non è sempre puntualmente dimostrato nelle relative decisioni di adeguatezza, soprattutto in quelle brevi e scarne adottate nella vigenza della Direttiva (ci si riferisce, ad esempio, ai casi di Canada, Nuova Zelanda, Israele). Le misure in questione necessitano dunque di essere strettamente monitorate da parte della Commissione europea; quest'ultima, a tal proposito, ha recentemente condotto un primo riesame delle 11 decisioni più risalenti tra quelle in vigore, decidendo in data 15 gennaio 2024 di confermarle in blocco, senza eccezioni [138]. Un'operazione su cui, però, l'EDPB ha espresso alcune riserve [139].

---

decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali nel contesto del quadro per la protezione dei dati UE-USA, 28 febbraio 2023.

[134] UE, Relazione della Commissione al Parlamento europeo e al Consiglio *sul primo riesame periodico del funzionamento della decisione di adeguatezza relativa al quadro UE-USA per la protezione dei dati personali*, 9 ottobre 2024, COM/2024/451 final.

[135] UE, Comitato europeo per la protezione dei dati, *EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 4 novembre 2024.

[136] Sul punto v., *inter alios*: O. Tene, *The show must go on*, in *www.iapp.org*, 17 luglio 2020.

[137] 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*, cit., pp. 756-757.

[138] UE, Relazione della Commissione europea al Parlamento europeo e al Consiglio *sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE*, 15 gennaio 2024, COM/2024/7 final; UE, Commissione europea, *Commission Staff Working Document "Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC" accompanying the document "Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC"*, 15 gennaio 2024, SWD/2024/3 final.

[139] UE, Comitato europeo per la protezione dei dati, *EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC*, 5 dicembre 2024.

Dopo aver preso in esame le decisioni di adeguatezza finora adottate dalla Commissione, si può dunque affermare che, mentre quelle appartenenti alla prima delle menzionate categorie non sollevano particolari problemi, quelle rientranti nella seconda e (ancor di più) nella terza presentano invece alcune criticità. Si tornerà su tali criticità in seguito, risultando esse estremamente rilevanti ai fini della presente trattazione.

Al di là di tali questioni riguardanti singole decisioni, tuttavia, si vuole portare nuovamente l'attenzione sull'aspetto di portata generale già menzionato in apertura del presente argomento: solo un numero piuttosto limitato di Paesi beneficia di una decisione, proprio in conseguenza dell'elevatissimo livello di protezione richiesto dalla nozione di «adeguatezza». Un simile standard comporta che il procedimento di valutazione da parte della Commissione, magari dopo essersi protratto per anni, possa avere un esito negativo [140]. Ad esempio, non si è giunti all'adozione di decisioni di adeguatezza, nonostante le aspettative degli Stati coinvolti, nei casi dell'Australia, in ragione delle perplessità espresse nel 2001 dal Gruppo di lavoro «Articolo 29» [141]; del Marocco, che non ha superato il relativo test al termine del primo decennio del nuovo millennio [142]; nonché del Principato di Monaco, pur essendovi in tal caso un parere sostanzialmente favorevole del Gruppo di lavoro [143]. Inoltre, in aggiunta agli Stati per i quali la valutazione non si è conclusa nel modo sperato, ve ne sono molti di più che neppure hanno tentato di ottenere una decisione, consci presumibilmente delle difficoltà che avrebbero incontrato nel vedere il loro livello di protezione dei dati personali riconosciuto come «adeguato» [144].

In conclusione, dopo aver analizzato normativa, giurisprudenza e prassi, è dunque possibile affermare che la decisione di adeguatezza, per come configurata nel Regolamento (UE) 2016/679, per come interpretata dalla Corte di giustizia

---

[140] Sul punto v., *inter alios*: C. KUNER, *Transborder Data Flows and Data Privacy Law*, cit., pp. 65-66.

[141] UE, Gruppo di lavoro «Articolo 29», *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 26 gennaio 2001, WP 40, p. 6, secondo cui: «*[…] On the basis of the above, the working party considers that data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet the above mentioned concerns […]*». Sul punto v., *inter alios*: N. BLACKMORE, *Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific*, in *www.kennedyslaw.com*, 26 marzo 2019.

[142] Sul punto v., *inter alios*: H. CHENAOUI, *Moroccan data protection law: Moving to align with EU data protection?*, in *www.iapp.org*, 11 settembre 2018; F. TASSINARI, *The Externalization of Europe's Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows*, in *Peace & Security – Paix et Sécurité Internationales*, 2021, Numero 9, p. 9.

[143] UE, Gruppo di lavoro «Articolo 29», *Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco*, 19 luglio 2012, WP 198, p. 19, secondo cui: «*[…] In conclusion, pursuant to all the above and to compliance with the Agreement, the Working Party considers that the Principality of Monaco guarantees an adequate level of protection […]*».

[144] Sul punto, e segnatamente sugli Stati dell'area asiatico-pacifica che non hanno neppure cercato di ottenere una decisione di adeguatezza, v. *inter alios*: N. BLACKMORE, *op. cit.*.

e per come (tendenzialmente) applicata dalla Commissione, è uno strumento che privilegia indubbiamente le esigenze di protezione dei dati rispetto a quelle degli scambi commerciali.

3. *Le garanzie adeguate*

3.1. *Il dato testuale del GDPR: l'art. 46 (e l'art. 47)*

L'indagine, tuttavia, deve focalizzarsi anche sul caso in cui manchi una decisione di adeguatezza. Come si è già detto, infatti, in tale situazione è possibile ricorrere ai meccanismi alternativi: un'ipotetica interpretazione di questi ultimi che ne consentisse un ampio utilizzo, senza richiedere uno standard di tutela particolarmente elevato, potrebbe modificare radicalmente l'impostazione della disciplina nel suo insieme in senso opposto a quello visto finora (rendendo *de facto* inutile l'atteggiamento di rigore in punto di decisione di adeguatezza).

Il passaggio successivo è dunque un esame delle «garanzie adeguate» di natura contrattuale, che parta ancora una volta dal testo del GDPR e quindi, nella fattispecie, dall'art. 46: in tale disposizione, figurano le clausole contrattuali tipo, anche dette «*standard contractual clauses*» (SCC) o ancora «*model clauses*»; le clausole contrattuali *ad hoc*; le norme vincolanti d'impresa o «*binding corporate rules*» (BCR); gli strumenti tra autorità pubbliche; i codici di condotta; nonché i meccanismi di certificazione [145].

Giova prendere le mosse dalle clausole contrattuali, le uniche tra le garanzie che venivano menzionate esplicitamente già dall'art. 26, par. 2, della Direttiva (si parlava di «clausole contrattuali appropriate»), e segnatamente meritano un'attenzione particolare le *standard contractual clauses* [146]: in assenza di una decisione di adeguatezza, rappresentano infatti lo strumento maggiormente utilizzato dalle società commerciali per il trasferimento di dati personali fuori dall'UE [147]. Si tratta di un meccanismo che prevede la sottoscrizione, da parte dei soggetti tra cui avviene il flusso (*data exporter* e *data importer*), di un testo contrattuale, in forza del quale le parti si impegnano a garantire un adeguato livello di protezione dei

[145] UE, Regolamento (UE) 2016/679, cit., art. 46 («Trasferimento soggetto a garanzie adeguate»).

[146] Sulle clausole contrattuali tipo, v. *inter alios*: C. Kuner, *Article 46. Transfers subject to appropriate safeguards*, in C. Kuner-L.A. Bygrave-C. Docksey (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 797-812.

[147] G.M. Riccio, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in G. Resta-V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 215-238, spec. p. 227.

dati trasferiti; esse hanno tra le parti la medesima efficacia vincolante di un qualsiasi strumento contrattuale [148]. Per come disciplinate dal Regolamento, tuttavia, le *model clauses* presentano anche rilevanti problemi proprio sul piano della loro funzionalità. A differenza delle clausole contrattuali *ad hoc*, esse sono adottate dalla Commissione europea (oppure da un'autorità nazionale di controllo, ma poi comunque approvate dalla Commissione) circostanza che le rende anelastiche, non essendo modificabili a opera delle parti, e fa sì che non possano trovare applicazione in tutte le tipologie di contratti [149]. Inoltre, essendo clausole da inserire all'interno di un regolamento contrattuale, non deve essere sottovalutato il fatto che le SCC determinino un aumento dei costi transattivi, dal momento che gravano l'importatore di una vasta gamma di obblighi e responsabilità [150].

Le c.d. clausole contrattuali «*ad hoc*», al contrario, sono stipulate in totale autonomia dalle parti del trasferimento, adattandosi alle loro esigenze. Tuttavia, il rovescio della medaglia è che si rende necessaria una specifica approvazione da parte dell'autorità garante nazionale competente. Ciò comporta che tali clausole presentino il difetto di non essere particolarmente affidabili, sottoponendo le parti all'alea della valutazione della menzionata autorità [151].

Passando invece alle norme vincolanti d'impresa [152], con tale espressione si intende il complesso di *policy* aziendali, norme tecniche, strumenti di sicurezza e attività di *training* e *audit* adottati dalle società di un gruppo per assicurare una tutela adeguata ai trattamenti di dati personali all'interno del gruppo stesso [153]. Pur non figurando nel testo della Direttiva, le BCR non sono una novità introdotta dal Regolamento: già all'inizio degli anni 2000, infatti, certe autorità nazionali di protezione dei dati hanno iniziato ad approvare alcune norme vincolanti d'impresa, qualificandole come «garanzie sufficienti» *ex* art. 26, par. 2, della Direttiva [154]. Di fronte a tale fenomeno, il Gruppo di lavoro «Articolo 29»

---

[148] M.C. MENEGHETTI, *op. cit.*, p. 640.

[149] Sul punto v., *inter alios*: G.M. RICCIO, *Model Contract Clauses e Corporate Binding Rules*, cit., p. 237; A. MATTOO-J.P. MELTZER, *International Data Flows and Privacy: The Conflict and Its Resolution*, in *Journal of International Economic Law*, Dicembre 2018, Volume 21, Numero 4, pp. 769-789, spec. p. 777.

[150] Sul punto v., *inter alios*: G.M. RICCIO, *Model Contract Clauses e Corporate Binding Rules*, cit., p. 228.

[151] M.C. MENEGHETTI, *op. cit.*, p. 644.

[152] Sulle norme vincolanti d'impresa, v. *inter alios*: C. KUNER, *Article 47. Binding corporate rules*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 813-824.

[153] M.C. MENEGHETTI, *op. cit.*, p. 644.

[154] In particolare, nel luglio 2002, due insiemi di BCR della società *DaimlerChrysler* (riguardanti, rispettivamente, i dati dei dipendenti e quelli dei clienti/fornitori) sono stati approvati dalla Conferenza delle autorità di protezione dei dati tedesche; nel novembre 2002, un set di BCR proposto dall'Associazione tedesca delle assicurazioni (GDV) è stato approvato dalla medesima Conferenza; nel luglio 2003, sono state approvate le BCR della società *General Electric* riguardanti i dati dei dipendenti; nel novembre 2003, sono state approvate le BCR della società *Deutsche*

si è dedicato in modo estremamente approfondito a fissare quelli che avrebbero dovuto essere i requisiti delle BCR [155], requisiti che sono poi confluiti in larga misura nel GDPR e segnatamente nell'art. 47 [156]. In particolare, secondo il Regolamento, le BCR devono essere giuridicamente vincolanti, applicarsi a tutti i membri del gruppo, conferire espressamente agli interessati diritti azionabili e presentare il contenuto minimo indicato nella disposizione di riferimento; inoltre, anche in questo caso si rende necessario un controllo da parte dell'autorità competente. Quanto appena detto, tuttavia, fa sì che le norme vincolanti d'impresa presentino rilevanti limiti: possono essere adoperate solo all'interno di un gruppo imprenditoriale e non nei rapporti con le società terze; possono richiedere tempi considerevoli per la loro approvazione; presentano costi non trascurabili, essendo indispensabile destinare risorse umane alla loro redazione e ai rapporti con l'autorità [157].

Quanto agli strumenti tra autorità pubbliche, essi possono essere ulteriormente distinti in due categorie. La prima è quella degli «strumenti giuridicamente

---

Telekom (riguardanti sia i dati dei dipendenti che quelli dei clienti); il 4 maggio 2004, l'autorità austriaca ha approvato le BCR di una banca di tale Stato. In dottrina, sul punto v.: C. KUNER, *Article 47. Binding corporate rules*, cit., p. 815.

[155] In particolare v.: UE, Gruppo di lavoro «Articolo 29», *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3 giugno 2003, WP 74; UE, Gruppo di lavoro «Articolo 29», *Model Checklist, Application for approval of Binding Corporate Rules*, 25 novembre 2004, WP 102; UE, Gruppo di lavoro «Articolo 29», *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"*, 14 aprile 2005, WP 107; UE, Gruppo di lavoro «Articolo 29», *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, 14 aprile 2005, WP 108; UE, Gruppo di lavoro «Articolo 29», *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, 10 gennaio 2007, WP 133; UE, Gruppo di lavoro «Articolo 29», *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 giugno 2008, WP 153; UE, Gruppo di lavoro «Articolo 29», *Working Document Setting up a framework for the structure of Binding Corporate Rules*, 24 giugno 2008, WP 154; UE, Gruppo di lavoro «Articolo 29», *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, 24 giugno 2008 (versione emendata e adottata il 8 aprile 2009), WP 155 rev. 04; UE, Gruppo di lavoro «Articolo 29», *Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*, 6 giugno 2012, WP 195; UE, Gruppo di lavoro «Articolo 29», *Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities*, 17 settembre 2012, WP 195a; UE, Gruppo di lavoro «Articolo 29», *Explanatory Document on the Processor Binding Corporate Rules*, 19 aprile 2013 (versione emendata e adottata il 22 maggio 2015), WP 204 rev. 01; UE, Gruppo di lavoro «Articolo 29», *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, 27 febbraio 2014, WP 212.

[156] UE, Regolamento (UE) 2016/679, cit., art. 47 («Norme vincolanti d'impresa»).

[157] Sul punto v., *inter alios*: G.M. RICCIO, *Model Contract Clauses e Corporate Binding Rules*, cit., pp. 237-238; A. MATTOO-J.P. MELTZER, *op. cit.*, p. 777; C. KUNER, *Article 47. Binding corporate rules*, cit., p. 821.

vincolanti e aventi efficacia esecutiva tra autorità pubbliche o organismi pubblici». Tra questi, possono essere indubbiamente citati gli accordi PNR («*Passenger Name Record*»), concernenti il trattamento e il trasferimento delle registrazioni dei nominativi dei passeggeri: simili accordi sono stati conclusi con l'Australia [158] e con gli Stati Uniti [159], mentre sono in via di negoziazione con Canada e Giappone [160]. Un altro esempio è poi l'accordo tra UE e USA sul TFTP («*Terrorist Finance Tracking Programme*»), concernente il trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione agli USA ai fini del programma di controllo delle transazioni finanziarie dei terroristi [161]. Tali strumenti, essendo giuridicamente vincolanti, non richiedono alcuna approvazione da parte dell'autorità di controllo competente. La seconda categoria annovera invece le «disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati»; tra i suddetti accordi amministrativi si possono menzionare, a titolo esemplificativo, i *memorandum* di intesa. In questa seconda ipotesi sarà invece necessario ottenere l'autorizzazione dell'autorità di controllo competente, circostanza che dipende dall'assenza di un'efficacia giuridica vincolante tra le parti pubbliche contraenti [162]. In ogni caso, che appartengano alla prima o alla seconda categoria, resta comunque il fatto che gli strumenti in questione coinvolgono esclusivamente autorità pubbliche: di conseguenza, possono giovare ben poco alle imprese, che interessano maggiormente ai fini della presente trattazione.

Infine, si arriva ai codici di condotta e ai meccanismi di certificazione, strumenti di nuovo conio. I primi sono dettagliatamente disciplinati dall'art. 40 GDPR, in base a cui gli Stati membri, le autorità di controllo, il Comitato e la Commissione incoraggiano l'elaborazione di codici di condotta «destinati a contribuire alla corretta applicazione del […] regolamento» [163]; i codici possono essere elaborati, modificati o prorogati da associazioni o da altri organismi rappresentanti le cate-

---

[158] UE, *Accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record – PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera*, 29 settembre 2011, GU L 186, 14 luglio 2012, pp. 4-16.

[159] UE, *Accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna*, 14 dicembre 2011, GU L 215, 11 agosto 2012, pp. 5-14.

[160] Sul punto v., *inter alia*, la pagina del sito del Consiglio europeo e del Consiglio dell'Unione europea dedicata a «*Passenger data*», consultabile al seguente link: *https://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/* (ultimo accesso in data 31 dicembre 2024).

[161] UE, *Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi*, 28 giugno 2010, GU L 195, 27 luglio 2010, pp. 5-14.

[162] UE, Regolamento (UE) 2016/679, cit., Considerando 108.

[163] *Ibid*., art. 40, par. 1.

gorie dei titolari o dei responsabili del trattamento, e hanno dunque lo scopo di precisare l'applicazione di alcuni aspetti GDPR[164]. Quanto ai meccanismi di certificazione, essi sono disciplinati dall'art. 42 del Regolamento, secondo cui gli Stati membri, le autorità di controllo, il Comitato e la Commissione incoraggiano (in particolare a livello di Unione) l'istituzione di meccanismi di certificazione della protezione dei dati «allo scopo di dimostrare la conformità al […] regolamento dei trattamenti effettuati» dai titolari e responsabili [165]. Sia i codici di condotta che i meccanismi di certificazione, tuttavia, presentano rilevanti caratteristiche in comune con le BCR: devono essere giuridicamente vincolanti, conferire agli interessati diritti azionabili ed essere approvati dall'autorità competente [166]. Delle BCR, conseguentemente, hanno anche i poc'anzi illustrati limiti.

L'analisi appena svolta permette quindi di dire che, stando al dato normativo del Regolamento (UE) 2016/679, le garanzie adeguate (nessuna esclusa) non appaiono come strumenti in grado di fronteggiare efficacemente un'importante mole di scambi transnazionali di dati [167].

3.2. *La giurisprudenza della Corte di giustizia: la sentenza* Schrems II

Esattamente come nel caso della decisione di adeguatezza, anche in quello delle garanzie adeguate non si può giungere a conclusioni solide senza aver prima preso in considerazione la rilevante giurisprudenza della Corte di giustizia.

Indubbiamente, è ancora una volta la sentenza *Schrems II* quella che fornisce le indicazioni più rilevanti in tema di garanzie adeguate. Anche queste ultime, secondo il Giudice di Lussemburgo, devono essere idonee a garantire che i dati personali trasferiti fuori dall'Unione godano di un livello di protezione «sostanzialmente equivalente» a quello assicurato nell'UE dal Regolamento letto alla luce della Carta. Tale standard, dunque, deve essere garantito indipendentemente da quale sia la disposizione del Capo V sul cui fondamento viene effettuato un trasferimento di dati personali verso un Paese terzo (e, quindi, non solo quando si parla di decisioni di adeguatezza) [168].

---

[164] *Ibid*., art. 40, par. 2.

[165] *Ibid*., art. 42, par. 1.

[166] Sul punto v., *inter alios*: C. KUNER, *Article 46. Transfers subject to appropriate safeguards*, cit..

[167] Sul punto v., *inter alios*: G.M. RICCIO, *Model Contract Clauses e Corporate Binding Rules*, cit., p. 238.

[168] UE, Corte di giustizia, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*, 2020, cit., § 92, in base a cui: «Sebbene l'articolo 46 del RGPD non precisi la natura dei requisiti che derivano da tale riferimento a «garanzie adeguate», «diritti azionabili» e «mezzi di ricorso effettivi», occorre rilevare che tale articolo è contenuto nel capo V del suddetto regolamento e deve essere pertanto letto alla luce dell'articolo 44 di detto regolamento, rubricato «Principio generale per il trasferimento», il quale dispone che «[t]utte le disposizioni [di detto capo] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche

Nello specifico, la Corte si sofferma sulle più importanti tra tali garanzie, le SCC, che nell'ambito della vicenda *Schrems* avevano mostrato debolezze non indifferenti: era infatti apparso chiaro come, essendo strumenti di tipo contrattuale tra l'esportatore e l'importatore dei dati, esse non vincolassero le autorità pubbliche dei Paesi terzi, che potevano non rispettarle e accedere indisturbatamente ai dati. Proprio per rimediare a tali criticità, la Corte afferma che può rivelarsi necessario che il titolare (o il responsabile) del trattamento completi il contenuto delle clausole contrattuali tipo attraverso l'adozione di «misure supplementari», in modo da ottenere comunque il livello di protezione richiesto [169]. Qualora, invece, il titolare (o il responsabile) non sia in grado di adottare misure sufficienti a tal fine, esso, o in subordine l'autorità di controllo competente, ha l'obbligo di sospendere o porre fine al trasferimento di dati personali verso il Paese extra-UE interessato [170]; tale potere è infatti attribuito all'autorità di controllo dall'art. 58, par. 2, lett. j), del GDPR.

La Corte, in buona sostanza, rende le SCC delle «mini-decisioni di adeguatezza» (o «decisioni di adeguatezza su scala ridotta») [171], e mira a evitare che esse vengano utilizzate dalle società commerciali come mere finzioni giuridiche. Spesso tali società, per legittimare i trasferimenti di dati personali verso Stati extra-UE, si sono limitate a inserire le SCC nei loro contratti, rispettando il dato formale, ma disinteressandosi di quello sostanziale, ovvero della concreta messa in opera del meccanismo in questione e del rischio concreto che le autorità pubbliche del Paese terzo potessero avere accesso agevolmente a simili dati [172]. Questo, stando alla pronuncia *Schrems II*, non sarà più possibile.

In buona sostanza, con la pronuncia del 16 luglio 2020 il Giudice di Lussemburgo è andato a limitare, ancor di più rispetto a quanto già facesse il testo del GDPR, la possibilità di ricorrere alle garanzie adeguate, precisando che esse possono essere adoperate solo qualora sia assicurato uno standard di protezione estremamente elevato (*rectius*, «sostanzialmente equivalente» a quello UE).

---

garantito dal [medesimo] regolamento non sia pregiudicato». Tale livello di protezione deve, di conseguenza, essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo».

[169] *Ibid.*, §§ 132-134.

[170] *Ibid.*, § 135, in base a cui: «Qualora il titolare del trattamento o il responsabile del trattamento, stabiliti nell'Unione, non possano adottare misure supplementari sufficienti a garantire tale protezione, essi o, in subordine, l'autorità di controllo competente, sono tenuti a sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato. Tale ipotesi ricorre in particolare nel caso in cui il diritto di tale paese terzo imponga al destinatario di un trasferimento di dati personali proveniente dall'Unione obblighi in contrasto con dette clausole e, pertanto, atti a rimettere in discussione la garanzia contrattuale di un livello di protezione adeguato contro l'accesso delle autorità pubbliche di detto paese terzo a tali dati».

[171] C. KUNER, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, cit.; R.A. COSTELLO, *op. cit.*, p. 1053.

[172] 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*, cit., pp. 752-753.

3.3. *Le Raccomandazioni dell'*European Data Protection Board *(EDPB) e le* model clauses *della Commissione*

Nella medesima direzione indicata dalla Corte nella sentenza *Schrems II* vanno anche alcuni atti di poco successivi provenienti da altri attori istituzionali. In data 10 novembre 2020, infatti, il Comitato europeo per la protezione dei dati ha adottato due documenti: si tratta delle «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» [173] e delle «Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza» [174]. Le «Raccomandazioni 2/2020» rappresentano una guida destinata agli esportatori di dati e finalizzata a permettere loro di comprendere quali Paesi stranieri siano dotati di normative in materia di sorveglianza che siano rispettose degli standard europei; le «Raccomandazioni 01/2020» cercano invece di approfondire la nozione di «misure supplementari», da adottare – proprio là dove lo Stato terzo non offra sufficienti garanzie circa l'accesso delle autorità pubbliche ai dati personali – per poter comunque trasferire i dati sulla base delle SCC.

I criteri enunciati in tali Raccomandazioni, tuttavia, appaiono decisamente rigorosi. Ciò comporta, in primo luogo, che sia molto difficile per uno Stato extra-UE soddisfare i requisiti elencati, circostanza che costringe i titolari o i responsabili ad adottare «misure supplementari»; in secondo luogo, che anche l'adozione di «misure supplementari» rispettose delle condizioni richieste sia particolarmente difficile. Tutto ciò rende ancor più arduo il ricorso alle clausole contrattuali tipo e il trasferimento di dati. Non sorprende dunque che taluno abbia definito l'adozione delle summenzionate raccomandazioni, in modo improprio ma significativo, una sorta di «*Schrems III*» [175].

Infine, in data 4 giugno 2021, la Commissione ha adottato la Decisione di esecuzione (UE) 2021/914 «relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679» [176],

---

[173] UE, 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*, 10 novembre 2020, seconda versione del 18 giugno 2021 (adottata dopo la consultazione pubblica).

[174] UE, Comitato europeo per la protezione dei dati, *Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza*, 10 novembre 2020.

[175] Sul punto v.: T. Christakis, *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)*, in *European Law Blog*, 13 novembre 2020; T. Christakis, *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)*, in *European Law Blog*, 16 novembre 2020; T. Christakis, *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)*, in *European Law Blog*, 17 novembre 2020.

[176] UE, Decisione di esecuzione (UE) 2021/914 della Commissione *relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio*, 4 giugno 2021, GU L 199, 7 giugno 2021, pp. 31-61.

che ha sostituito le precedenti Decisioni della Commissione medesima in materia di SCC [177]. Essa detta in materia di *model clauses* una disciplina più dettagliata e puntuale rispetto al passato, che non solo riflette numerose delle novità del Regolamento (UE) 2016/679, ma tiene anche in debita considerazione i dettami contenuti nella stessa sentenza *Schrems II*, collocandosi quindi sulla stessa lunghezza d'onda rispetto alla Corte di giustizia [178]. In particolare, la nuova Clausola 14 obbliga le parti a garantire di non avere motivo di ritenere che la legislazione e le prassi del Paese terzo di destinazione, compresi eventuali requisiti di comunicazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscano all'importatore di rispettare gli obblighi che gli incombono a norma delle SCC [179]. La nuova Clausola 15, invece, obbliga l'importatore ad accettare di informare prontamente l'esportatore (e, ove possibile, l'interessato) nel caso in cui riceva da un'autorità pubblica una richiesta giuridicamente vincolante di comunicare i dati personali trasferiti in conformità delle clausole, oppure nel caso in cui venga a conoscenza di qualunque accesso diretto effettuato da autorità pubbliche. L'importatore, inoltre, accetta di riesaminare la legittimità della richiesta di comunicazione e di contestarla qualora, dopo un'attenta valutazione, concluda che sussistono fondati motivi per ritenere che essa sia illegittima. Infine, quando risponde a una richiesta di comunicazione, l'importatore accetta di fornire la quantità minima di informazioni consentite [180]. Emerge chiaramente una notevole attenzione per la delicata tematica dell'accesso ai dati personali da parte delle autorità pubbliche degli Stati extra-UE [181].

Una volta forniti simili elementi, è dunque possibile giungere alla seguente

---

[177] UE, Decisione della Commissione 2001/497/CE *relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE*, 15 giugno 2001, GU L 181, 4 luglio 2001, pp. 19-31; UE, Decisione della Commissione 2004/915/CE *che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi*, 27 dicembre 2004, GU L 385, 29 dicembre 2004, pp. 74-84; UE, Decisione della Commissione 2010/87/CE *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*, 5 febbraio 2010, GU L 39, 12 febbraio 2010, pp. 5-18.

[178] Sul punto v., *inter alios*: G. Ercolani, *Novità in materia di protezione dei dati personali: la Commissione europea adotta nuove clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento 2016/679 UE*, in *Eurojus.it*, 24 giugno 2021.

[179] UE, Decisione di esecuzione (UE) 2021/914, cit., Allegato, Clausola 14 («*Legislazione e prassi locali che incidono sul rispetto delle clausole*»).

[180] *Ibid*., Clausola 15 («Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche»).

[181] Sulla Decisione di esecuzione della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, v.: UE, Comitato europeo per la protezione dei dati e Garante europeo della protezione dei dati, *Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi per le materie di cui all'articolo 46, paragrafo 2, lettera c), del regolamento (UE) 2016/679*, 14 gennaio 2021.

valutazione: così come le decisioni di adeguatezza, pure le garanzie adeguate (SCC *in primis*, ma anche tutte le altre) stando al testo del GDPR, all'interpretazione della Corte di giustizia, nonché agli atti adottati dalla Commissione e non solo, devono essere considerate come strumenti che privilegiano chiaramente le esigenze di protezione dei dati a discapito di quelle degli scambi commerciali, dato che permettono i flussi solo a condizioni assai stringenti.

4. *Le deroghe in specifiche situazioni: il dato testuale dell'art. 49 GDPR, gli atti dell'EDPB e la giurisprudenza della Corte di giustizia*

Sulle «deroghe in specifiche situazioni» dell'art. 49 del Regolamento, infine, si potrà essere più rapidi [182]. Esse occupano la posizione più bassa a livello gerarchico tra gli strumenti del Capo V GDPR e sono, in particolare: il consenso della persona interessata; la necessità del trasferimento all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento; la necessità del trasferimento alla conclusione o all'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona a favore dell'interessato; la necessità del trasferimento per importanti motivi di interesse pubblico; la necessità del trasferimento per accertare, esercitare o difendere un diritto in sede giudiziaria; la necessità del trasferimento per tutelare gli interessi vitali dell'interessato o di altre persone; il trasferimento effettuato a partire da un registro; la necessità del trasferimento per il perseguimento degli interessi legittimi cogenti del titolare del trattamento [183].

Simili deroghe sono pensate per situazioni in cui nel Paese terzo verso cui i dati sono destinati *non* vi sia un livello di protezione adeguato, ma i rischi per la persona interessata siano relativamente ridotti, oppure nel caso in cui altri interessi (pubblici, ovvero quelli della stessa persona interessata) prevalgano sul diritto alla protezione dei dati di tale persona [184]. Si tratta in sostanza di una "valvola di sicurezza", che consente di effettuare trasferimenti internazionali di dati personali qualora ciò sia richiesto da altri importanti diritti e libertà [185]:

---

[182] Sul punto v., *inter alios*: C. KUNER, *Article 49. Derogations for specific situations*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 841-856.

[183] UE, Regolamento (UE) 2016/679, cit., art. 49 («Deroghe in specifiche situazioni»).

[184] UE, Gruppo di lavoro «Articolo 29», *Transfers of personal data to third countries*, 1998, cit., p. 24, secondo cui: «*These exemptions […] for the most part concern cases where the risks to the data subject are relatively small or where other interests (public interests or those of the data subject himself) override the data subject's right to privacy*».

[185] C. KUNER, *Article 49. Derogations for specific situations*, cit., p. 843, secondo cui: «*[…] the derogations in effect function as a 'safety valve' to allow transfers when there is an overriding societal interest that they take place, whether because the risks to the transfers are small, or because such risks are overridden by other important rights and interests […]*».

come noto, la protezione dei dati non è infatti un diritto assoluto [186].

Tuttavia, tale *ratio* richiede che le deroghe siano interpretate *restrittivamente* e che esse non possano fornire un quadro adeguato a lungo termine in caso di trasferimenti ripetuti o anche strutturali di dati personali. Altrimenti, si andrebbe a contraddire la loro natura eccezionale.

L'esigenza di ricorrere alle deroghe con parsimonia emerge, innanzitutto, dal testo dell'art. 49, che prevede diverse restrizioni al loro utilizzo [187]. Basti pensare a quanto disposto dal par. 1, lett. a), in materia di consenso dell'interessato: esso non solo deve presentare tutti i requisiti richiesti in via generale per qualunque forma di consenso dall'art. 4, n. 11, del Regolamento [188], ma deve essere anche manifestato «esplicitamente» e ottenuto solo dopo che l'interessato è stato «informato dei possibili rischi di siffatti trasferimenti […] dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate». Merita poi di essere evidenziato che, con riferimento a quasi tutte le altre deroghe, l'art. 49 GDPR prevede che il trasferimento debba essere «necessario» a perseguire specifiche finalità. È dunque richiesto il superamento di un vero e proprio «test di necessità».

Inoltre, il fatto che le deroghe debbano essere interpretate restrittivamente è stato precisato pure dal Gruppo di lavoro «Articolo 29» e (in seguito) dal Comitato in svariati documenti [189], nonché soprattutto dalla costante giurisprudenza della Corte di giustizia, espressa anche in sentenze già citate come *Digital Rights Ireland* e *Schrems I*: per il Giudice di Lussemburgo, infatti, tutte le deroghe ai diritti fondamentali devono operare entro i limiti dello stretto necessario [190].

---

[186] Sul punto v., *inter alia*: UE, Corte di giustizia, sentenza del 9 novembre 2010, cause riunite C-92/09 e C-93/09*, Volker e Markus Schecke GbR e Hartmut Eifert contro Land Hessen*, ECLI:EU:C:2009:284, § 48, in base a cui: «Il diritto alla protezione dei dati personali non appare tuttavia come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale».

[187] Sul punto v.: C. Kuner, *Article 49. Derogations for specific situations*, cit., p. 846.

[188] UE, Regolamento (UE) 2016/679, cit., art. 4 («Definizioni»), in base a cui: «Ai fini del presente regolamento s'intende per: […] 11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento […]».

[189] Sul punto v., *inter alia*: UE, Gruppo di lavoro «Articolo 29», *Transfers of personal data to third countries*, 1998, cit., p. 24, secondo cui: «*As exemptions from a general principle, they must be interpreted restrictively*». V. anche: UE, Gruppo di lavoro «Articolo 29», *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, 25 novembre 2005, WP 114; UE, Comitato europeo per la protezione dei dati, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, 25 maggio 2018.

[190] Sul punto v., *inter alia*: UE, Corte di giustizia, *Digital Rights Ireland*, cit., § 52, in base a cui: «Per quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale, secondo la costante giurisprudenza della Corte, richiede in ogni caso che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario […]»; UE, Corte di giustizia, *Maximillian Schrems contro Data Protection Commissioner*, 2015,

È quindi possibile completare il quadro, affermando che anche per le deroghe in specifiche situazioni valgono, in punto di bilanciamento tra esigenze di *personal data protection* e interessi economici, le medesime considerazioni già svolte in merito alle decisioni di adeguatezza e alle garanzie adeguate.

cit., § 92, in base a cui: «[…] la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario».

Capitolo III

GLI OBIETTIVI DELL'ATTUALE DISCIPLINA UE

Sommario: 1. La continuità del livello di tutela garantito nell'Unione. – 2. L'esportazione degli standard UE in materia di protezione dei dati personali. – 2.1. La promozione dei diritti fondamentali. – 2.2. Le finalità di tipo strategico. – 3. I punti deboli dell'approccio dell'UE.

1. *La continuità del livello di tutela garantito nell'Unione*

Dall'indagine poc'anzi svolta, è dunque emerso chiaramente che la disciplina unilateralmente adottata dall'Unione europea in materia di trasferimenti di dati personali verso Stati extra-UE, per come delineata dal legislatore nel Regolamento (UE) 2016/679, per come interpretata dalla Corte di giustizia nelle sue sentenze e anche per come attuata dalla Commissione in alcuni atti, effettua un'opera di bilanciamento in cui le esigenze di protezione dei dati personali prevalgono chiaramente su quelle di carattere commerciale.

Tale impostazione, ai sensi della quale la tutela dei diritti viene sempre più rafforzata, mentre è sempre più complesso per i dati personali lasciare l'Unione europea, ha indubbiamente molteplici finalità.

Innanzitutto, lo si è anticipato, le istituzioni UE si vogliono assicurare che il livello di tutela delle persone fisiche garantito nell'Unione dal GDPR non sia compromesso attraverso trasferimenti dei loro dati verso Paesi terzi. Si tratta di un obiettivo esplicitato anche nei Considerando del Regolamento stesso [1], nonché soprattutto nell'art. 44, in base a cui tutte le disposizioni del Capo V «sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal […] regolamento non sia pregiudicato». Infatti, se fosse possibile trasmettere con facilità i dati personali verso Stati extra-UE in cui non vi sono sufficienti salvaguardie, l'intera operazione di irrobustimento dei diritti degli individui compiuta nel GDPR attraverso innumerevoli istituti finirebbe per essere vanificata: proprio per questo, si rende indispensabile una disciplina tanto rigorosa.

[1] UE, Regolamento (UE) 2016/679, cit., Considerando 101.

2. *L'esportazione degli standard UE in materia di protezione dei dati personali*

Al tempo stesso, non si può trascurare la presenza di altre finalità. L'Unione europea ha anche l'obiettivo, peraltro nient'affatto celato, di esportare i propri elevati standard di protezione dei dati personali verso un numero più ampio possibile di Paesi terzi. Questi ultimi, se vogliono consentire alle entità presenti sul proprio territorio, e in modo particolare alle imprese, di ricevere dati personali dall'UE e di avere accesso al mercato UE, devono infatti adottare, e pure implementare efficacemente, legislazioni rispettose dei più importanti principi della disciplina UE in materia di *personal data protection* [2]. I sistemi giuridici di tali Stati finiscono dunque per essere ricondotti, attraverso meccanismi di incentivazione e coercizione, sotto quello che è stato ribattezzato come «*data realm*» (letteralmente, «regno dei dati») dell'Unione europea, espressione con cui si intende l'approccio proprio dell'UE nella regolamentazione dei dati [3].

Quanto appena descritto può essere considerato a pieno titolo come un aspetto di quello che l'autrice Anu Bradford ha definito «*Brussels effect*»: con tale espressione si intende proprio l'influenza sulle normative di Paesi terzi che l'Unione europea esercita unilateralmente grazie alla propria posizione centrale nell'economia globale [4]. Tale influenza è possibile solo in ragione del fatto che nell'UE, in relazione all'ambito in esame, sono presenti determinate condizioni. In particolare, un mercato interno di grandissime dimensioni («*market power*») [5]; un'efficace capacità di regolamentazione («*regulatory capacity*») [6]; una certa rigidità degli standard («*strict rules*») [7]; il fatto che la regolamentazione sia rivolta a obiettivi anelastici («*inelastic targets*»), come i consumatori (mentre i capitali, ad esempio, sono mobili, e là dove le regole siano ritenute sfavorevoli possono essere trasferiti in un'altra giurisdizione, ciò non vale per i consumatori, che sono tipicamente immobili; un'impresa che intenda offrire loro i propri beni o servizi, non potendo «spostarli», non può neppure scegliere la normativa da applicare) [8]; e la non divisibilità degli standard («*nondivisibility of standards*»):

---

[2] Sul punto v., *inter alios*: W. Höglund, *Exporting data protection law. The extraterritorial reach of the GDPR*, Umeå Universitet, Umeå, 2018, p. 26.

[3] S.A. Aaronson-P. Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 2018, Volume 21, Numero 2, pp. 245-272.

[4] A. Bradford, *The Brussels Effect*, in *Northwestern University Law Review*, Volume 107, Numero 1, 2012, pp. 1-68; A. Bradford, *The Brussels effect: How the European Union rules the world*, Oxford University Press, Oxford, 2020.

[5] A. Bradford, *The Brussels Effect*, 2012, cit., pp. 11-12.

[6] *Ibid*., pp. 12-14.

[7] *Ibid*., pp. 14-16.

[8] *Ibid*., pp. 16-17.

non si può cioè decidere di applicare tali standard solo nei rapporti con l'UE; al contrario, una volta abbracciati, essi devono essere applicati globalmente [9].

I requisiti appena elencati sono presenti in vari settori, nei quali l'Unione è quindi riuscita a esercitare la propria influenza su Stati terzi: si tratta, *inter alia*, dei settori della concorrenza [10], della salute dei consumatori [11], della protezione dell'ambiente [12], della sicurezza dei cibi [13]. Ma, come anticipato, si riscontrano tali elementi anche nell'ambito della protezione dei dati: ciò è asserito anche dalla stessa Bradford [14] (che fa proprio riferimento alle regole UE in materia di trasferimenti di dati verso Paesi terzi [15]). In particolare, secondo altra dottrina, nel settore in esame il «*Brussels effect*» sarebbe principalmente frutto delle notevoli dimensioni del mercato UE e del fatto che la regolamentazione è rivolta a quelli che la Bradford definisce «obiettivi anelastici», nella fattispecie le persone i cui dati vengono trattati («*data subjects*»); sono comunque presenti anche gli altri tre fattori [16].

L'intenzione di esportare gli standard UE in materia di *personal data protection*, deve essere evidenziato, era presente fin dalle origini, ed è stata una delle ragioni che ha portato all'adozione del nuovo quadro giuridico. A titolo esemplificativo, nella Comunicazione della Commissione del 2009 su «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», si affermava che l'Unione avrebbe dovuto svolgere «una funzione motrice per lo sviluppo e la promozione di norme internazionali in materia di protezione dei dati personali» [17]. E ancora, nella Comunicazione della Commissione del 2010 intitolata «Un approccio globale alla protezione dei dati personali nell'Unione europea», si enfatizzava l'obiettivo dell'Unione di porsi come un «punto di riferimento per paesi terzi nel regolamentare la protezione dei dati», rappresentando «una forza trainante per lo sviluppo e la promozione di norme internazionali di protezione dei dati personali, sia giuridiche che tecniche, in conformità con gli strumenti pertinenti dell'UE e degli Stati membri in materia di protezione dei dati» [18].

---

[9] *Ibid*., pp. 17-19.

[10] *Ibid*., pp. 19-22.

[11] *Ibid*., pp. 26-29.

[12] *Ibid*., pp. 29-31.

[13] *Ibid*., pp. 32-35.

[14] *Ibid*., pp. 22-26.

[15] *Ibid*., p. 24.

[16] O.J. Gstrein-A.J. Zwitter, *Extraterritorial application of the GDPR: promoting European values or power?*, in *Internet Policy Review*, 2021, Volume 10, Numero 3, pp. 1-30, spec. p. 4.

[17] UE, Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*, 10 giugno 2009, COM/2009/262 def., § 2.3.

[18] UE, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, 4 novembre 2010, COM/2010/609 def., § 2.4.2.

Orbene, trascorsi alcuni anni dall'entrata in vigore del GDPR è possibile asserire che i risultati raggiunti sul punto sono rilevanti. Ad esempio, nella Comunicazione della Commissione del 24 giugno 2020 intitolata «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» si può leggere quanto segue: «Il regolamento generale sulla protezione dei dati si è già rivelato un punto di riferimento fondamentale a livello internazionale e ha svolto un ruolo di catalizzatore per numerosi paesi in tutto il mondo al fine di prendere in considerazione l'introduzione di norme moderne sulla tutela della vita privata» [19].

I risultati ottenuti dall'UE nell'esportazione dei propri standard in materia di *personal data protection* sono mostrati in modo ancor più evidente dal noto autore Graham Greenleaf. Quest'ultimo redige periodicamente delle liste in cui sono elencati quei Paesi extra-UE che hanno adottato normative in materia di protezione dei dati quasi sempre ispirate al GDPR. Un recente documento di tal genere, intitolato «*Global data privacy laws 2023: 162 national laws and 20 Bills*», mostra per l'appunto come al 2023 siano ben 162 gli Stati che hanno elaborato simili discipline [20]: si tratta di cinque Paesi in più rispetto al 2022 [21], 17 in più rispetto al 2021 [22], 20 in più rispetto al 2020 [23] e 30 in più rispetto al 2019 [24]; un chiaro segnale dell'influenza del Regolamento (UE) 2016/679. A onor del vero, come peraltro precisato dallo stesso Greenleaf, l'inclusione dei Paesi nell'elenco dipende solo dal dato formale consistente nell'adozione di *data privacy laws*, mentre nulla dice circa l'effettiva implementazione di tali normative o circa la presenza di meccanismi di sorveglianza posti in essere dalle autorità pubbliche che possono compromettere la tutela accordata agli individui (aspetti che invece, lo si è detto, sono di estrema importanza ai fini della valutazione dell'adeguatezza) [25]; tuttavia, le liste di Greenleaf permettono comunque di capire come il

---

[19] UE, 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*, 24 giugno 2020, COM/2020/264 final, p. 14.

[20] G. Greenleaf, *Global data privacy laws 2023: 162 national laws and 20 Bills*, in *Privacy Laws & Business International Report*, 2023.

[21] G. Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, in *Privacy Laws & Business International Report*, 2022.

[22] G. Greenleaf, *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*, in *Privacy Laws & Business International Report*, 2021.

[23] G. Greenleaf, *2020 Ends a Decade of 62 New Data Privacy Laws*, in *Privacy Laws & Business International Report*, 2020.

[24] G. Greenleaf, *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*, in *Privacy Laws & Business International Report*, 2019.

[25] Sul punto v.: G. Greenleaf, *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*, cit., pp. 1-2, secondo cui: «*[…] Inclusion of a law only means that it meets […] minimum formal requirements […], and says nothing about whether the laws are*

quadro giuridico UE in materia di protezione dei dati sia davvero diventato un punto di riferimento a livello internazionale [26].

Merita altresì di essere precisata una circostanza: le modalità attraverso cui l'Unione europea esporta verso Paesi terzi, e verso i soggetti ivi ubicati, i propri standard in materia di protezione dei dati personali sono molteplici. La presente trattazione si concentra in particolare sulle regole del Capo V GDPR, che con tutta probabilità rappresentano la modalità migliore di perseguire il menzionato scopo. Come è già stato precisato, le norme in questione obbligano gli Stati extra-UE, là dove essi vogliano consentire alle entità presenti sul proprio territorio di ricevere dati personali dall'Unione, ad adottare e implementare efficacemente legislazioni rispettose dei più importanti principi della disciplina UE in materia di *personal data protection*.

Ma non si deve certo trascurare il ruolo del citato art. 3 dello stesso GDPR, che delinea l'ambito di applicazione territoriale del nuovo quadro giuridico. In base al suo par. 2, il Regolamento «si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che *non* [enfasi aggiunta] è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione». In altri termini, vi è la possibilità che il GDPR trovi applicazione nel caso di trattamenti effettuati da titolari o responsabili extra-UE, qualora il loro *target* sia il mercato europeo o, comunque, i soggetti che si trovano nell'UE.

Anche in questo caso, siamo evidentemente di fronte a un tentativo di estensione (unilaterale) di tutele, considerate importanti da parte delle istituzioni UE, oltre i confini del territorio dell'Unione stessa. Chiaramente, la modalità con cui si cerca tale estensione è diversa rispetto a quella che caratterizza il Capo V GDPR: qui non si inducono i Paesi terzi ad adottare legislazioni rispettose dei principi UE, ma si richiede direttamente alle singole entità ubicate in tali Paesi, le quali vogliono offrire beni o servizi a interessati che si trovano nell'Unione (o monitorare i loro comportamenti), di conformarsi alle norme del Regolamento (UE) 2016/679. Ma la finalità ultima è la medesima, che, come si è visto, consiste nell'esportazione oltrefrontiera degli standard UE in materia di protezione dei dati personali [27].

---

effectively enforced (a much more complex and contentious enterprise, as 'adequacy' assessments show), or about the data surveillance context in which such laws exist and which may largely nullify their potential benefits […]».

[26] Sull'impatto del GDPR sugli ordinamenti giuridici di Stati extra-UE v., *inter alios*: M. Casoria-E.M. Alsarraf, *The Impact of the GDPR on Extra-EU Legal Systems: The Case of the Kingdom of Bahrain*, in M. Tzanou (a cura di), *Personal Data Protection and Legal Developments in the European Union*, IGI Global, Hershey, 2019, pp. 224-237.

[27] Sull'ambito di applicazione territoriale del GDPR e sull'estensione delle tutele realizzata grazie allo stesso v., *inter alios*: O.J. Gstrein-A.J. Zwitter, *op. cit.*.

Vi è inoltre un'altra precisazione da fare. Finora, si è detto di come la più volte menzionata opera di esportazione avvenga attraverso gli istituti del GDPR, e dunque unilateralmente. Ma essa potrebbe avvenire anche sfruttando strumenti di tipo multilaterale, a cui l'Unione non ha certo rinunciato (in questi casi, giova specificarlo, non si parla di «*Brussels effect*», espressione che descrive esclusivamente un'influenza unilaterale) [28]. Si fa ovviamente riferimento agli strumenti del Consiglio d'Europa, ovvero la Convenzione 108 del 1981 e ancor di più la Convenzione 108+ del 2018: l'Unione europea, da un lato, ha lavorato per avvicinare quanto possibile il contenuto di tale trattato a quello del GDPR e far sì che rispecchiasse gli stessi principi del Regolamento; dall'altro, spinge affinché la Convenzione 108+ venga ratificata da un rilevante numero di Paesi, non solo UE, ma anche extra-UE e pure extra-europei: si ricorda infatti che, così come lo strumento originario, anche la Convenzione 108+ ha aspirazione universale, potendo essere ratificata anche da Stati non membri del CoE. In virtù di quanto illustrato, la Convenzione 108+, là dove entrasse in vigore, potrebbe contribuire anch'essa «alla convergenza verso un insieme di standard elevati di protezione dei dati» a livello internazionale [29].

In definitiva, lo si ripete, l'approccio dell'Unione ha tra i suoi obiettivi quello di esportare i principi UE verso Paesi terzi [30]. A ciò occorre aggiungere un'ulteriore riflessione: tale esportazione ha, a sua volta, varie finalità.

2.1. *La promozione dei diritti fondamentali*

In primo luogo, vi è indubbiamente un puro e semplice intento di promuovere i diritti fondamentali a livello globale. Nel momento in cui gli Stati extra-UE, e le entità in essi ubicate, abbracciano standard più elevati di *personal data protection* a beneficiarne saranno i cittadini non solo dell'Unione, ovunque i loro dati si trovino, ma di tutto il globo. Ciò è perfettamente in linea con gli obiettivi dell'azione esterna dell'UE per come delineata nei Trattati: essa, infatti, si prefigge di promuovere nel resto del mondo i principi che hanno informato la creazione, lo sviluppo e l'allargamento dell'Unione, tra cui democrazia, Stato di diritto, universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, rispetto della dignità umana, principi di uguaglianza e di solidarietà [31].

---

[28] A. Bradford, *The Brussels Effect*, 2012, cit., p. 46.

[29] UE, Comunicazione della Commissione europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, cit., § 3.3.1.

[30] Sul punto, v. anche: K. Irion-M. Burri-A. Kolk-S. Milan, *Governing "European values" inside data flows: Interdisciplinary perspectives*, in *Internet Policy Review*, 2021, Volume 10, Numero 3.

[31] UE, *Trattato sull'Unione europea (versione consolidata)*, GU C 202, 7 giugno 2016, pp. 13-46, art. 21.

2.2. *Le finalità di tipo strategico*

In secondo luogo, però, vi sono anche finalità di tipo strategico, che consistono nel tentare di conferire un vantaggio competitivo alle imprese dell'Unione rispetto alle società concorrenti extra-UE. Le prime, infatti, possono mantenere il loro approccio in materia di protezione dei dati, essendo abituate ormai da alcuni decenni ai principi caratterizzanti la normativa UE. Al contrario, le seconde saranno costrette a conformarsi agli standard dell'Unione: dovranno dunque modificare le proprie pratiche commerciali e adeguare le proprie operazioni a livello globale, sostenendo a tal fine costi non indifferenti [32]. L'alternativa sarebbe quella di non poter ricevere e trattare i dati personali degli europei, del cui valore economico finirebbero per beneficiare le sole imprese europee: anche in tal caso, dunque, vi sarebbe per queste ultime un vantaggio competitivo [33].

Quanto appena esposto permette di comprendere una circostanza: quello che, durante l'intero corso della trattazione, è stato costantemente definito come un conflitto tra esigenze di tutela dei diritti fondamentali, da un lato, e istanze di carattere commerciale, dall'altro, assume in realtà contorni molto più complessi. Anche dietro la protezione dei dati personali e la conseguente limitazione dei flussi, infatti, si celano considerazioni di carattere economico, consistenti nella volontà di proteggere le imprese dell'Unione dall'agguerrita concorrenza di società di altri Paesi, statunitensi *in primis*, ma non solo.

3. *I punti deboli dell'approccio dell'UE*

Ricapitolando, fin qui si è dunque illustrato l'approccio della disciplina UE, ai sensi del quale la tutela dei diritti viene sempre più rafforzata, mentre è sempre più complesso per i dati personali lasciare l'Unione europea, nonché le finalità di tale approccio.

È ora possibile proseguire, svolgendo altre considerazioni. Ma ciò non prima di aver segnalato che, dall'indagine della disciplina UE, sono emersi anche alcuni elementi che potrebbero rappresentare delle vere e proprie crepe all'interno dell'appena descritta costruzione, rischiando di comprometterla. Ci si riferisce ad aspetti non tanto della normativa o della giurisprudenza, quanto piuttosto dell'operato della Commissione: infatti, è vero che quest'ultima si è dimostrata in generale parsimoniosa nell'adozione delle decisioni di adeguatezza, che nel momento in cui si chiude il presente scritto riguardano solo 15 Stati; ed è pure

[32] A. Bradford, *The Brussels Effect*, 2012, cit..

[33] Sui vantaggi economici di cui beneficiano i Paesi che sono destinatari di decisioni di adeguatezza rispetto a quelli che non lo sono, v. *inter alios*: M.F. Ferracane.-B. Hoekman-E. Van Der Marel-F. Santi, *Digital Trade, Data Protection and EU Adequacy Decisions*, RSC Working Paper 2023/37, Firenze, 2023.

vero che alcune di tali misure, di cui beneficiano i Paesi strettamente integrati con l'Unione europea e con i suoi Stati membri, non presentano particolari problemi; ma è anche vero, e lo si è visto, che talune decisioni, concernenti soprattutto importanti partner commerciali dell'UE, sollevano determinate criticità: esse appaiono motivate prevalentemente da ragioni di carattere economico, anziché dalla presenza di livelli di protezione «adeguati» nei Paesi in questione, circostanza che ha reso necessaria l'elaborazione di soluzioni creative, come decisioni settoriali (si tratta di casi come quelli di Canada, Israele, Giappone, Regno Unito, Repubblica di Corea, Stati Uniti). Si tornerà a breve su simili decisioni, e sull'impatto che esse possono avere sul disegno complessivo appena descritto.

Parte II

GLI IMPEGNI COMMERCIALI ASSUNTI DALL'UE A LIVELLO INTERNAZIONALE E IL LORO IMPATTO SULLA DISCIPLINA INTERNA

CAPITOLO I

GLI OBBLIGHI, CONTENUTI NEL DIRITTO DELL'OMC, CONCERNENTI IN GENERALE LA LIBERALIZZAZIONE DEI SERVIZI

SOMMARIO: 1. La possibile incompatibilità *prima facie* della disciplina UE con gli obblighi del GATS. – 1.1. La clausola della nazione più favorita. – 1.2. Gli altri obblighi generali: le norme in materia di trasparenza e quelle sulla regolamentazione interna. – 1.3. Gli impegni specifici: le norme in materia di trattamento nazionale e accesso al mercato. – 2. Le difficoltà nel giustificare le violazioni *prima facie* del GATS. – 2.1. L'integrazione economica. – 2.2. Le eccezioni generali.

Dopo aver risposto al primo dei due quesiti in cui la domanda di ricerca illustrata in apertura era stata scomposta, occorre ora concentrarsi sul secondo. Ci si deve dunque interrogare circa determinati impegni assunti dall'UE a livello internazionale, nello specifico in ambito commerciale, che vanno in vario modo a incidere sulla materia dei flussi transfrontalieri di dati personali. In particolare, serve chiedersi se essi siano coerenti con l'approccio proprio della disciplina interna UE, nonché se, in caso contrario, possa esservi un impatto di qualche tipo su quest'ultimo.

Innanzitutto, giova riflettere sugli obblighi concernenti in generale la liberalizzazione dei servizi contenuti nel *corpus* normativo dell'Organizzazione mondiale del commercio (OMC o anche WTO, ovvero *World Trade Organization*), organizzazione che, come noto, annovera tra i suoi membri sia gli Stati dell'UE che la stessa Unione europea e ha fra i suoi obiettivi l'espansione del commercio di beni e servizi, nonché la conseguente riduzione degli ostacoli agli scambi [1]. Tra gli strumenti facenti parte del diritto dell'OMC, oltre al *General Agreement on Tariffs and Trade* (GATT), i.e. l'accordo generale sulle tariffe doganali e sul commercio, ne figura uno che sancisce obblighi assai rilevanti ai fini della presente trattazione: ci si riferisce al *General Agreement on Trade in Services* (GATS), finalizzato proprio alla liberalizzazione degli scambi di servizi [2].

---

[1] WTO, *Agreement Establishing the World Trade Organization*, Marrakesh, 15 aprile 1994. In dottrina, per un'ampia e approfondita analisi dell'Organizzazione mondiale del commercio, v. *inter alios*: P. PICONE-A. LIGUSTRO, *Diritto dell'organizzazione mondiale del commercio*, CEDAM, Padova, 2002; G. VENTURINI (a cura di), *L'Organizzazione Mondiale del Commercio*, Giuffrè, Milano, 2015.

[2] WTO, *Annex 1B to the Agreement Establishing the World Trade Organization – General*

Il GATS, che ai sensi dell'art. I si applica ai «provvedimenti adottati dai membri che incidono sugli scambi di servizi» («*measures by Members affecting trade in services*»), definisce il termine «servizio» («*service*») come «qualunque servizio fornito in qualsivoglia settore» («*any service in any sector*»), rimanendo esclusi solo quelli forniti nell'esercizio dei poteri governativi [3]. Si è optato, in buona sostanza, per non procedere a una vera definizione di servizio, scelta che secondo certa dottrina costituirebbe uno dei punti di forza del GATS: esso può essere così applicato a fattispecie nuove e precedentemente non previste, tra cui anche il commercio elettronico [4]. Sul punto, in verità, erano stati espressi alcuni dubbi: gli Stati Uniti, a titolo esemplificativo, si erano detti preoccupati per la mancanza di indicazioni che chiarissero se tale settore dovesse essere regolato o meno dagli obblighi OMC sugli scambi di servizi [5]. La questione, tuttavia, è stata definitivamente chiarita dagli organi dell'OMC, nell'ambito di alcune controversie tra cui «*US – Gambling*» [6] e «*China – Publications and Audiovisual Products*» [7]: è stata infatti ribadita la «neutralità tecnologica» («*technological neutrality*») del GATS – nel senso che esso non contiene alcuna previsione che distingua tra i diversi mezzi tecnologici attraverso i quali un servizio può essere fornito [8] – e

Agreement on Trade in Services, Marrakesh, 15 aprile 1994. In dottrina, per un'analisi del *General Agreement on Trade in Services*, v. *inter alios*: C. DORDI, *L'Accordo generale sul commercio dei servizi*, in G. VENTURINI (a cura di), *L'Organizzazione Mondiale del Commercio*, Giuffrè, Milano, 2015, pp. 151-197.

[3] WTO, *General Agreement on Trade in Services*, cit., art. I («*Scope and Definition*»), parr. 1 e 3.

[4] C. ARUP, *The New World Trade Organization Agreements: Globalizing Law Through Services and Intellectual Property*, Cambridge University Press, Cambridge, 2001, p. 102.

[5] Sul punto v., *inter alios*: S.A. AARONSON, *The Digital Trade Imbalance and Its Implications for Internet Governance*, in *Global Commission on Internet Governance Paper Series*, 2016, Numero 25, p. 6.

[6] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, 10 novembre 2004, WT/DS285/R, § 6.285; WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, 7 aprile 2005, WT/DS285/AB/R, § 180 ss.. In dottrina, per una panoramica generale del caso «*US – Gambling*», v. *inter alios*: A.P. PETROVA, *The WTO Internet Gambling Dispute as a Case of First Impression: How to Interpret Exceptions Under GATS Article XIV(a) and How to Set the Trend for Implementation and Compliance in WTO Cases Involving "Public Morals" and "Public Order" Concerns?*, in *Richmond Journal of Global Law & Business*, 2006, Volume 6, Numero 1, pp. 45-76.

[7] WTO, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products. Report of the Panel*, 12 agosto 2009, WT/DS363/R; WTO, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products. Report of the Appellate Body*, 21 dicembre 2009, WT/DS363/AB/R, §§ 363-365. In dottrina, per una panoramica generale del caso «*China – Publications and Audiovisual Products*», v. *inter alios*: E. D'ALTERIO, «*Il bruco e la farfalla*». *Libertà di commercio ed eccezione culturale*, in *Giornale di diritto amministrativo*, 2010, Numero 8, pp. 847-857. V. anche: T. VOON, *China and Cultural Products at the WTO*, in *Legal Issues of Economic Integration*, 2010, Volume 37, Numero 3, pp. 253-259.

[8] Sul punto v.: WTO, Council for Trade in Services, *Work Programme on Electronic Com-*

conseguentemente anche l'applicabilità dell'accordo al commercio elettronico [9].

Con l'espressione «scambio di servizi» («*trade in services*»), invece, il GATS intende quattro diverse modalità di fornitura («*modes of supply*») di un servizio [10]. In questa sede, quella che interessa maggiormente è senz'altro la c.d. «fornitura transfrontaliera» («*mode 1*»): essa non prevede infatti alcuno spostamento di persone fisiche, essendo l'oggetto della fornitura a viaggiare; si pensi, ad esempio, alle attività di consulenza fornite via *e-mail*. Tale «*mode of supply*» svolge dunque un ruolo di primaria importanza nella distribuzione di quei servizi ad alto contenuto tecnologico, divenuti essenziali al giorno d'oggi, che si sostanziano proprio in flussi di dati [11].

Affinché possano essere prestati i servizi di cui sopra, è quindi necessario che siano consentiti i trasferimenti oltrefrontiera di dati; là dove questi ultimi siano invece vietati o limitati, ciò può rappresentare un ostacolo al citato obiettivo di liberalizzazione nel settore dei servizi. Si cominciano dunque a intravedere, fin da subito, i potenziali attriti tra il GATS e la disciplina UE in materia di flussi di dati personali [12].

Proprio alla luce di quanto appena esposto è necessario interrogarsi approfonditamente sulla compatibilità della normativa dell'Unione europea in materia di flussi di dati personali con gli obblighi sanciti dal GATS. Tale accordo, come menzionato poc'anzi, si applica infatti ai «provvedimenti adottati dai membri che incidono sugli scambi di servizi», categoria in cui rientra indubbiamente anche la regolamentazione UE in esame: quest'ultima, per l'appunto, è astrattamente in grado di inibire o addirittura prevenire la prestazione di servizi a livello internazionale, attraverso la limitazione dei trasferimenti dei dati personali necessari alla loro fornitura [13]. Trattandosi di «*measures affecting trade in services*», esse sono quindi soggette al GATS e ai vincoli ivi contenuti.

Si tratta perciò di vedere, in primo luogo, se la pertinente disciplina del Regolamento (UE) 2016/679 e i provvedimenti adottati ai sensi della stessa (su tutti, le decisioni di adeguatezza) rispettino o meno tali obblighi; in secondo luogo, in caso di incompatibilità *prima facie*, se le norme UE in questione possano esse-

---

merce – Progress Report to the General Council, adopted by the Council for Trade in Services on 19 July 1999, 27 luglio 1999, S/L/74, § 4, in base a cui: «*[…] It was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied […]*».

[9] Sul punto v. anche, *inter alios*: G.M. Ruotolo, *La disciplina multilaterale del commercio digitale*, in *Diritto pubblico comparato ed europeo*, 2014, Numero 4, pp. 1887-1919.

[10] WTO, *General Agreement on Trade in Services*, cit., art. I («*Scope and Definition*»), par. 2.

[11] P. Picone-A. Ligustro, *op cit.*, pp. 367-368.

[12] Sul punto v., *inter alios*: A. Chander-P.M. Schwartz, *Privacy and/or Trade*, in *The University of Chicago Law Review*, 2023, Volume 90, Numero 1, pp. 49-135.

[13] C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, Oxford, 2013, p. 52, secondo cui: «*The obligations of the GATS might seem to conflict with legislative regulation of transborder data flows, since the latter can inhibit or even prevent the provision of services internationally by restricting the transfer of personal data needed to perform them*».

re giustificate ai sensi di una delle eccezioni previste dallo stesso GATS [14]. Pur non essendoci mai stata, nell'ambito del sistema di risoluzione delle controversie dell'organizzazione, una procedura finalizzata a contestare la disciplina UE in questione [15], alcuni rapporti degli organi OMC (e specialmente dell'Organo di appello) si rivelano assai utili in tale opera di indagine [16].

1. *La possibile incompatibilità* prima facie *della disciplina UE con gli obblighi del GATS*

1.1. *La clausola della nazione più favorita*

Innanzitutto, il GATS contiene degli «obblighi generali», i quali vincolano tutti i membri dell'OMC (salva un'esplicita esclusione attraverso le c.d. «liste di deroga»). Tra questi obblighi spicca la *clausola della nazione più favorita* (CNPF) o «*most-favoured-nation clause*» (MFNC) dell'art. II, senza dubbio la più importante previsione dell'accordo [17]: essa impone a ogni membro di accordare ai servizi e ai prestatori di servizi degli altri membri, in via immediata e incondizionata, un trattamento non meno favorevole di quello accordato ad analoghi servizi e prestatori di servizi di qualsiasi altro Paese [18].

Affinché si possa parlare di una violazione della CNPF da parte della normativa UE sono dunque necessari due elementi: innanzitutto, un giudizio di «analogia» o «similarità» («*likeness*») tra servizi o prestatori di servizi; in secondo luogo, la presenza di un «trattamento meno favorevole» («*less favourable treatment*») accordato dalla disciplina UE in esame.

---

[14] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements*, Institute for Information Law (IViR), Amsterdam, 2016, p. 26.

[15] Sul punto v., *inter alios*: F. Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements*, in *European Papers*, 2019, Volume 4, Numero 3, pp. 881-894, spec. p. 884.

[16] Tra i più importanti: WTO, *European Communities – Regime for the Importation, Sale and Distribution of Bananas. Report of the Appellate Body*, 9 settembre 1997, WT/DS27/AB/R; WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit.; WTO, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products. Report of the Appellate Body*, cit.; WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body*, 14 aprile 2016, WT/DS453/AB/R.

[17] Sulle radici storiche della clausola della nazione più favorita v., *inter alios*: F. Marrella, *Manuale di diritto del commercio internazionale. Contratti internazionali, imprese globali ed arbitrato*, CEDAM, Padova, 2017, p. 709.

[18] WTO, *General Agreement on Trade in Services*, cit., art. II («*Most-Favoured-Nation Treatment*»).

Per quanto riguarda il primo aspetto, occorre preliminarmente chiarire che si parla di servizi e di prestatori di servizi «analoghi» («*like*») se essi sono «in un rapporto di concorrenza gli uni con gli altri» («*in a competitive relationship with each other*») [19].

Al fine di semplificare l'accertamento del suddetto requisito, vige una vera e propria «presunzione di analogia» («*presumption of likeness*») dei servizi e dei prestatori di servizi là dove una misura preveda una distinzione basata esclusivamente sull'origine («*exclusively on origin*») [20]. Non è però questo il caso. La normativa UE prevede sì, attraverso lo strumento della decisione di adeguatezza, una differenza di trattamento fra i vari Stati terzi destinatari dei dati personali, e quindi, adottando una diversa prospettiva, una differenza di trattamento fra i vari Stati terzi di origine dei servizi o dei prestatori. Tuttavia, tale distinzione non è basata esclusivamente sull'origine, ma su altri fattori: in particolare, come si è visto, sull'adeguatezza o meno del livello di protezione dei dati personali che il Paese extra-UE in questione garantisce, che a propria volta dipende da un gran numero di circostanze. Si tratta, piuttosto, di una differenza di trattamento «inestricabilmente connessa a tale origine» («*inextricably linked to such origin*»), caso in cui la presunzione di analogia tra i servizi o tra i prestatori non può operare [21].

A questo punto, al fine di stabilire se il requisito della «*likeness*» sia integrato oppure no, occorrerà effettuare un'analisi più dettagliata del rapporto di concorrenza («*competitive relationship*») sussistente tra i servizi, o i fornitori, in gioco: sarà dunque una valutazione caso per caso [22], che potrà portare a risultati differenti. Ovviamente, là dove l'accertamento dovesse dare esito negativo, l'indagine si interromperebbe: senza analogia, non vi sarà alcuna violazione della CNPF. Ma tale requisito potrebbe anche essere ritenuto presente: si pensi molto

---

[19] Sul punto v.: WTO, *China – Certain Measures Affecting Electronic Payment Services. Report of the Panel*, 16 luglio 2012, WT/DS413/R, § 7.700, in base a cui: «*[…] These provisions further suggest that like services are services that are in a competitive relationship with each other (or would be if they were allowed to be supplied in a particular market) […]*»; WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Panel*, 30 settembre 2015, WT/DS453/R, § 7.159, in base a cui: «*[…] in China – Electronic Payment Services […] the panel concluded that "like services are services that are in a competitive relationship with each other (or would be if they were allowed to be supplied in a particular market)" […]*»; e § 7.160, in base a cui: «*[…] we see no obstacle to using the same likeness interpretation as that used by the panel in China – Electronic Payment Services […]*»; WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body*, cit., § 6.25, in base a cui: «*[…] we consider that the concept of "likeness" of services and service suppliers under Articles II:1 and XVII:1 of the GATS is concerned with the competitive relationship of services and service suppliers […]*».

[20] WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body*, cit., § 6.38, in base a cui: «*[…] where a measure provides for a distinction based exclusively on origin […] "likeness" can be presumed […]*».

[21] *Ibid*., §§ 6.55-6.56.

[22] Sul punto v.: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 29.

banalmente al caso di un motore di ricerca australiano, che sarebbe ragionevolmente considerato in un rapporto di concorrenza, e quindi analogo, rispetto a un motore di ricerca statunitense (l'Australia, giova ricordarlo, non è coperta da una decisione di adeguatezza, mentre gli USA sono attualmente destinatari del *Data Privacy Framework*). La finalità dei motori di ricerca è infatti quella di trovare informazioni su Internet, indipendentemente da quale sia il Paese di origine degli stessi; le loro proprietà e la loro natura non variano, in conseguenza della loro nazionalità, in una misura tale da negare l'analogia sussistente tra i medesimi [23].

Sempre in tema di «*likeness*», c'è un argomento che merita di essere preso in considerazione. Si potrebbe infatti affermare che, nel valutare i servizi *online*, i consumatori tengano in debita considerazione il livello di tutela della *privacy* e di protezione dei dati personali garantito dagli stessi. Ciò potrebbe rappresentare una caratteristica rilevante nella valutazione del rapporto di concorrenza, facendo venir meno l'analogia, altrimenti sussistente, tra un servizio proveniente da un Paese extra-UE che offre una protezione «adeguata» e un servizio proveniente da uno Stato terzo che non fornisce le stesse garanzie. Come ulteriore conseguenza, la CNPF risulterebbe rispettata, senza necessità di ulteriori verifiche. L'argomento appena esposto, tuttavia, non appare convincente: alcuni studi dimostrano infatti come i consumatori tendano a comportarsi irrazionalmente e che le loro scelte in merito ai servizi *online* non sono necessariamente influenzate dal livello di tutela loro garantito [24]; questo fenomeno viene definito, non a caso, «*privacy paradox*». Perciò, è possibile concludere che la tutela della *privacy* e la protezione dei dati non devono essere considerati alla stregua di fattori che possono incidere sull'esito del giudizio di «analogia» tra due servizi, o prestatori [25].

Nel caso in cui i servizi, o prestatori, fossero analoghi, sarebbe dunque necessario passare alla seconda fase dell'indagine. Ci si dovrebbe cioè chiedere se sia presente una misura UE che accorda un «trattamento meno favorevole», ovverosia che modifica le condizioni di concorrenza a svantaggio di servizi o prestatori di servizi analoghi (per l'appunto) di qualsiasi altro membro [26]. Giova puntualizzare che una simile discriminazione può essere *de jure* – quando

---

[23] Su tale esempio v.: C.L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, in *Melbourne Journal of International Law*, 2011, Volume 12, Numero 1, pp. 1-36, spec. p. 15.

[24] Sul punto v.: K. Irion-G. Luchetta, *Online Personal Data Processing and the EU Data Protection Reform*, Centre for European Policy Studies, Bruxelles, 2013, p. 35.

[25] Sul punto, v.: S. Yakovleva-K. Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 2016, Volume 2, Numero 2, pp. 191-208, spec. p. 204; K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 30; F. Velli, *op. cit.*, p. 885.

[26] WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body*, cit., § 6.129, in base a cui: «*[…] a measure accords less favourable treatment if it modifies the conditions of competition to the detriment of like services or service suppliers of any other Member*».

la misura è formalmente discriminatoria – ma anche solamente *de facto*: ciò si verifica quando una misura, pur non essendo formalmente discriminatoria, all'atto della concreta applicazione comporta un differente trattamento fra servizi o prestatori di servizi di origini diverse, alterando le condizioni concorrenziali. Entrambe le casistiche sono quindi coperte dal divieto[27].

Appare chiaro *ictu oculi* che i prestatori operanti in quegli Stati extra-UE che sono destinatari di una decisione di adeguatezza sono in una posizione di vantaggio, dal momento che beneficiano in modo automatico e illimitato del diritto di ricevere i dati personali trasferiti dall'Unione europea, i quali a loro volta sono fondamentali per la fornitura dei servizi. È invece più gravosa la posizione dei prestatori di quei Paesi terzi che non hanno ottenuto una decisione di adeguatezza: per ricevere dati personali dall'UE, essi sono costretti ad avvalersi dei meccanismi alternativi del Capo V GDPR, che, come già visto, presentano limiti e comportano oneri. Di conseguenza, anche se non siamo di fronte a un trattamento esplicitamente discriminatorio, la disciplina dell'Unione in materia di *personal data flows* comporta un trattamento preferenziale a beneficio dei servizi e prestatori di determinati Stati[28].

La previsione da parte dell'UE di un regime di maggior favore per alcuni Paesi, come noto, è tutt'altro che immotivata: l'obiettivo è infatti quello di impedire che il livello di protezione dei dati personali assicurato nell'Unione dal Regolamento (UE) 2016/679 non sia compromesso mediante il trasferimento di tali dati fuori dai confini europei. Tale *ratio*, tuttavia, non incide in alcun modo sulla qualificazione del trattamento come «meno favorevole»: non vi è infatti alcun elemento all'interno dell'art. II GATS che dia rilievo agli «obiettivi ed effetti» («*aims and effects*») di una misura nella valutazione circa la compatibilità della stessa con tale disposizione[29].

Di conseguenza, è possibile concludere che la disciplina UE in materia di flussi di dati personali accorda ai servizi e prestatori di alcuni membri dell'OMC un trattamento meno favorevole rispetto a quello accordato a servizi e prestatori «analoghi» di altri Stati (segnatamente, quelli beneficiari di decisioni di adegua-

---

[27] WTO, *European Communities – Regime for the Importation, Sale and Distribution of Bananas. Report of the Appellate Body*, cit., § 234, in base a cui: «*For these reasons, we conclude that "treatment no less favourable" in Article II:1 of the GATS should be interpreted to include* de facto*, as well as* de jure*, discrimination* […]». In dottrina, sul punto, v. *inter alios*: C. DORDI, *op. cit.*, p. 167; sulla vicenda «*EC – Bananas III*», invece, v. *inter alios*: S.A.B. SCHROPP-D. PALMETER, *Commentary on the Appellate Body Report in EC–Bananas III (Article 21.5): waiver-thin, or lock, stock, and metric ton?*, in *World Trade Review*, 2010, Volume 9, Numero 1, pp. 7-57.

[28] In tal senso v., *inter alios*: C.L. REYES, *op. cit.*, p. 16; K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 30; F. VELLI, *op. cit.*, p. 885.

[29] WTO, *European Communities – Regime for the Importation, Sale and Distribution of Bananas. Report of the Appellate Body*, cit., § 241, in base a cui: «*We see no specific authority either in Article II or in Article XVII of the GATS for the proposition that the "aims and effects" of a measure are in any way relevant in determining whether that measure is inconsistent with those provisions […]*».

tezza). Ragionevolmente, nell'ambito di una controversia instaurata di fronte ai competenti organi dell'Organizzazione mondiale del commercio, sarebbe dunque ravvisata una violazione della CNPF dell'art. II GATS, quantomeno *prima facie*. A questo punto, si tratterebbe quindi di andare a verificare se la stessa possa essere giustificata attraverso una delle eccezioni espressamente previste dallo stesso Accordo generale sugli scambi di servizi[30]. Ci si occuperà di questo aspetto a breve, dopo aver valutato la compatibilità della normativa dell'Unione anche con gli altri obblighi del GATS.

1.2. *Gli altri obblighi generali: le norme in materia di trasparenza e quelle sulla regolamentazione interna*

Oltre alla CNPF, il GATS contiene altri obblighi generali, tra cui specialmente le norme in materia di «trasparenza» («*transparency*») e di «regolamentazione interna» («*domestic regulation*»).

Le prime, disciplinate dall'art. III GATS, non creano particolari problemi: imponendo esse obblighi di pubblicazione, comunicazione e risposta a richieste di informazioni, non si vede come possano essere violate dalla disciplina in questione[31].

Più complesso il discorso in materia di regolamentazione interna, di cui all'art. VI GATS: tale disposizione tende a evitare che gli Stati membri dell'OMC possano perseguire obiettivi protezionistici, limitando espressamente o rendendo in via di fatto inefficaci le disposizioni del GATS non solo mediante l'emanazione di misure interne intrinsecamente discriminatorie, ma anche attraverso l'applicazione discriminatoria di misure che formalmente non lo sono[32]. Nell'ambito di tale articolo, assume poi particolare rilievo il par. 1, il quale, a onor del vero, si applica esclusivamente con riguardo a quei settori oggetto degli «impegni spe-

---

[30] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 30.

[31] WTO, *General Agreement on Trade in Services*, cit., art. III («*Transparency*»). In dottrina, sul punto, v. *inter alios*: C. DORDI, *op. cit.*, p. 168.

[32] La disposizione in questione costituisce una novità rispetto al GATT ed è dovuta alla particolare importanza rivestita dalle disposizioni nazionali in materia di servizi. Esse, in alcuni casi, sono finalizzate a tutelare il fruitore, che spesso non ha elementi per poter valutare la qualità del servizio offerto fino al momento del godimento della prestazione (c.d. «asimmetria informativa»): si pensi, ad esempio, che la tutela del paziente di un servizio sanitario è assicurata, di norma, mediante requisiti professionali di accesso alla professione di medico, oltre a obblighi di trasparenza e di corretta informazione. In altre situazioni, invece, sono funzionali alla promozione di interessi di carattere generale: è il caso, ad esempio, della concessione di autorizzazioni al trasporto pubblico di persone, condizionate all'impegno del beneficiario di coprire specifiche aree remote del Paese (che probabilmente non potranno generare profitti) o dell'obbligo, per le istituzioni finanziarie, di destinare una quota del denaro versato dai correntisti a fondi prudenziali a tutela dei creditori. Tuttavia, tali disposizioni nazionali possono influenzare, e limitare, gli scambi internazionali in misura ancora maggiore di quanto non avvenga per le merci.

cifici» (di cui si dirà a breve): nei settori in questione, la disposizione oggetto di analisi prevede che tutte le «misure di applicazione generale» concernenti gli scambi di servizi debbano essere «amministrate in modo ragionevole, obiettivo e imparziale»[33].

Il suddetto art. VI.1 GATS merita considerazione per il fatto che la legislazione UE in materia di dati personali rientra indubbiamente nella categoria delle «misure di applicazione generale». Queste ultime, citando certa giurisprudenza degli organi dell'OMC, sono misure che incidono su «un numero non identificato di operatori economici» («*an unidentified number of economic operators*»)[34] e che si applicano a «una serie di situazioni o casi, piuttosto che essere limitate nel loro ambito di applicazione» («*a range of situations or cases, rather than being limited in their scope of application*»)[35]. Si tratta di condizioni chiaramente soddisfatte dalla normativa in questione: essa non è limitata nel suo ambito di applicazione, ma al contrario concerne tutti i trattamenti e trasferimenti di dati personali, coprendo così «una serie di situazioni o casi». Pur riferendosi non a tutti i dati, ma solo a quelli personali, la disciplina in esame dà di questi ultimi una definizione molto ampia: il «*range of situations or cases*» a cui essa si applica non risulta dunque essere significativamente limitato. Essa incide inoltre su un numero non identificato di operatori economici, circostanze che la rendono senza dubbio sussumibile tra le «misure di applicazione generale»[36].

Come si è detto, in relazione alle misure di cui sopra, l'art. VI.1 GATS prescrive un obbligo di correttezza procedurale nella loro amministrazione, che deve essere contraddistinta da ragionevolezza, obiettività e imparzialità. Se è vero che la legislazione UE in quanto tale non potrà certo porsi in contrasto con un simile obbligo, è anche vero che risulta impossibile escludere che vi siano state o che vi potranno essere violazioni dell'art. VI.1 GATS consistenti in un'*applicazione* di tale disciplina non ragionevole, obiettiva o imparziale[37]. In particolare, a parere di alcuni, oggetto di contestazione sotto questo profilo potrebbe essere

---

[33] WTO, *General Agreement on Trade in Services*, cit., art. VI («*Domestic Regulation*»), par. 1.

[34] Sul punto v.: WTO, *United States – Restrictions on Imports of Cotton and Man-Made Fibre Underwear. Report of the Panel*, 8 Novembre 1996, WT/DS24/R, § 7.65, in base a cui: «*[…] However, to the extent that the restraint affects an unidentified number of economic operators, including domestic and foreign producers, we find it to be a measure of general application*».

[35] Sul punto v.: WTO, *European Communities – Selected Customs Matters. Report of the Panel*, 16 giugno 2006, WT/DS315/R, § 7.116, in base a cui: «*[…] The Panel understands that, therefore, the "[l]aws, regulations, judicial decisions and administrative rulings of general application" […] are laws, regulations, judicial decisions and administrative rulings that apply to a range of situations or cases, rather than being limited in their scope of application […]*».

[36] Sul punto v.: C.L. Reyes, *op. cit.*, pp. 17-19. V. anche: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 31.

[37] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 31, secondo cui: «*[…] While – at the level of its application – it is impossible to conclude that there never was and never will be a violation of GATS Article VI.1, this would not affect EU data protection law as such […]*».

soprattutto la prassi applicativa della Commissione europea nell'adozione delle decisioni di adeguatezza: l'accertamento compiuto da tale istituzione non si basa esclusivamente su considerazioni di carattere giuridico, ma a volte è influenzato anche da valutazioni di natura squisitamente politica ed economica. L'approccio della Commissione, come autorevolmente sostenuto, finisce dunque per non essere sempre ragionevole, obiettivo e imparziale [38], e in quanto tale si espone al rischio di essere contestato ai sensi dell'art. VI.1 GATS [39].

Al contrario, risulta assai difficile configurare violazioni dall'art. VI.2 GATS, che impone ai membri dell'OMC di istituire o mantenere organi imparziali competenti a verificare la legittimità delle decisioni amministrative concernenti gli scambi di servizi (la normativa in esame non va certo a inficiare il rispetto di un simile obbligo) [40], nonché violazioni dei paragrafi 3, 4 e 5 dello stesso articolo: questi ultimi riguardano ipotesi in cui la fornitura di servizi è subordinata a obblighi in materia di autorizzazioni [41], requisiti o licenze, oppure a norme tecniche [42]; ma nel caso di specie ciò non avviene, ragion per cui le citate disposizioni non risultano chiamate in causa [43].

In definitiva, per quanto riguarda gli obblighi generali del GATS, ci si occuperà della necessità di dover giustificare eventuali violazioni non solo della clausola della nazione più favorita, ma anche dell'art. VI in materia di «regolamentazione interna», ancorché limitatamente a quanto prescritto dal suo par. 1.

---

[38] Sul punto v., *inter alios*: C. KUNER, *Developing an Adequate Legal Framework for International Data Transfers*, in S. GUTWIRTH-Y. POULLET-P. DE HERT-C. DE TERWANGNE-S. NOUWT (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 263-273, spec. p. 271, secondo cui le decisioni di adeguatezza «*are far from always being objective and logical […]*».

[39] In tal senso v.: S. YAKOVLEVA-K. IRION, *The Best of Both Worlds?*, cit., pp. 205-206. V. anche C.L. REYES, *op. cit.*, pp. 18-20; F. VELLI, *op. cit.*, p. 886.

[40] WTO, *General Agreement on Trade in Services*, cit., art. VI («*Domestic Regulation*»), par. 2.

[41] *Ibid.*, par. 3.

[42] Sul punto v., *inter alios*, P. PICONE-A. LIGUSTRO, *op cit.*, p. 383.

[43] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 31, secondo cui la disciplina UE in materia di dati personali «*[…] does not trigger paragraphs 2, 3, 4 and 5 of GATS Article VI because it does not mount authorisation, qualification or licensing requirements, nor can it be considered a technical standard […]*». A onor del vero, è stato sostenuto che le regole in materia di trasferimenti di dati verso Paesi extra-UE potessero violare anche i paragrafi 3 e 4 dell'art. VI GATS; in tal senso v.: C.L. REYES, *op. cit.*, pp. 18-20. Tale argomento è stato però puntualmente confutato; in tal senso v.: S. YAKOVLEVA-K. IRION, *The Best of Both Worlds?*, cit., p. 205, secondo cui: «*[…] Some literature claims that the rules on the transfer of personal data to third countries violate GATS Articles VI:3 and VI:4(b). This is doubtful because the provision of Article VI:3 concerns authorisation requirements, of which the relevant rules, when considered as a whole, are not an example. Neither can they be qualified as qualification requirements and procedures, technical standards and licensing requirements, which are regulated by GATS Article VI:4 […]*».

1.3. *Gli impegni specifici: le norme in materia di trattamento nazionale e accesso al mercato*

Oltre agli obblighi generali, il GATS contiene anche alcuni «impegni specifici» (poc'anzi citati). La loro caratteristica è quella di vincolare non tutti i membri, ma solo quelli che hanno manifestato la volontà di liberalizzare ulteriormente determinate categorie di servizi, indicandole nelle proprie «liste di impegni specifici» («*schedules of specific commitments*»). Le *schedules* assumono dunque una posizione assolutamente centrale nel sistema del GATS: solo facendo riferimento a esse è possibile comprendere il reale grado di liberalizzazione che un Paese ha inteso concedere a un certo servizio [44].

Prima di svolgere un'indagine sulla compatibilità della disciplina UE sui trasferimenti di dati personali con i suddetti impegni specifici, occorre dunque verificare quali sono i settori in cui l'UE ha assunto simili impegni, e accertare se fra tali settori ne figurano alcuni in cui hanno luogo flussi oltrefrontiera di dati personali. Se così non fosse, l'indagine sul punto si interromperebbe immediatamente, non potendo certo configurarsi una violazione di obblighi che non sono mai stati assunti.

Tuttavia, facendo riferimento alla lista di impegni specifici dell'Unione, ovvero la «*European Union Schedule of Specific Commitments*» del 2019 [45], che ha sostituito una serie di liste precedenti [46] e che è stata poi integrata nel

---

[44] Sul punto v., *inter alios*, P. Picone-A. Ligustro, *op cit.*, p. 375.

[45] WTO, *European Union Schedule of Specific Commitments*, 7 maggio 2019, GATS/SC/157.

[46] WTO, *The EU-25 Consolidated Schedule. Communication from the Secretariat*, 7 maggio 2019, S/L/430, in base a cui: «*[…] The EU-25 consolidated Schedule is now reproduced in document GATS/SC/157 which replaces the following documents: - Schedule of Specific Commitments of the European Communities and its Member States (doc. GATS/SC/31 of 15 April 1994); - Schedule of Specific Commitments of the European Communities and its Member States, Supplement 2 (doc. GATS/SC/31/Suppl.2 of 28 July 1995); - Schedule of Specific Commitments of the European Communities and its Member States, Supplement 3 (doc. GATS/SC/31/Suppl.3 of 11 April 1997); - Schedule of Specific Commitments of the European Communities and its Member States, Supplement 4, Revision (doc. GATS/SC/31/Suppl.4/Rev.1 of 18 November 1999). - Schedule of Specific Commitments of the Czech Republic (doc. GATS/SC/26 of 15 April 1994); - Schedule of Specific Commitments of the Czech Republic, Supplement 2 (doc. GATS/SC/26/Suppl.2 of 11 April 1997); - Schedule of Specific Commitments of the Czech Republic, Supplement 3 (doc. GATS/SC/26/Suppl.3 of 26 February 1998); - Schedule of Specific Commitments of Estonia (doc. GATS/SC/127 of 5 October 1999); - Schedule of Specific Commitments of Cyprus (doc. GATS/SC/25 of 15 April 1994); - Schedule of Specific Commitments of Cyprus, Supplement 1 (doc. GATS/SC/25/Suppl.1 of 23 February 1998); - Schedule of Specific Commitments of Cyprus, Supplement 2, Revision (doc. GATS/SC/25/Suppl.2/Rev.1 of 18 November 1999); - Schedule of Specific Commitments of Latvia (doc. GATS/SC/126 of 22 April 1999); - Schedule of Specific Commitments of Lithuania (doc. GATS/SC/133 of 21 December 2001); - Schedule of Specific Commitments of Hungary (doc. GATS/SC/40 of 15 April 1994); - Schedule of Specific Commitments of Hungary, Supplement 2 (doc. GATS/SC/40/Suppl.2 of 11 April 1997); - Schedule of Specific Commitments of Hungary, Supplement 3 (doc. GATS/SC/40/Suppl.3 of 26 February 1998); - Schedule of Specific Commitments of Malta (doc. GATS/SC/54 of 15 April 1994); - Schedule of Specific Commitments*

2024 [47], ci si rende conto che l'UE ha effettivamente assunto impegni specifici in settori che implicano il trattamento (e il trasferimento) di dati personali. Fra questi si possono menzionare: nell'ambito dei «*Business Services*» (punto II.1 della *Schedule*) [48], i «*Computer and Related Services*» (II.1.B) [49], tra cui ancor più in particolare i «*Data Processing Services*» (II.1.B.c) [50], i «*Data Base Services*» (II.1.B.d) [51] e gli «*Other Computer Services*» (II.1.B.e) [52]; nell'ambito dei «*Communication Services*» (punto II.2 della *Schedule*) [53], i «*Telecommunications Services*» (II.2.C) [54]; nell'ambito dei «*Financial Services*» (punto II.7 della *Schedule*) [55], gli «*Insurance and Insurance-Related Services*» (II.7.A) [56] e i «*Banking and Other Financial Services*» (II.7.B) [57]; nell'ambito dei «*Tourism and Travel Related Services*» (punto II.9 della *Schedule*) [58], i «*Travel Agencies and Tour Operators Services*» (II.9.B) [59]; nell'ambito dei «*Transport Services*» (punto II.11 della *Schedule*) [60], il «*Computer Reservation System*» (II.11.C.d) [61].

---

of Malta, Supplement 1 (doc. GATS/SC/54/Suppl.1 of 26 February 1998); - Schedule of Specific Commitments of Austria (doc. GATS/SC/7 of 15 April 1994); - Schedule of Specific Commitments of Poland (doc. GATS/SC/71 of 15 April 1994); - Schedule of Specific Commitments of Poland, Supplement 2 (doc. GATS/SC/71/Suppl.2 of 11 April 1997); - Schedule of Specific Commitments of Poland, Supplement 3 (doc. GATS/SC/71/Suppl.3 of 26 February 1998); - Schedule of Specific Commitments of Slovenia (doc. GATS/SC/99 of 30 August 1995); - Schedule of Specific Commitments of Slovenia, Supplement 1 (doc. GATS/SC/99/Suppl.1 of 26 February 1998); - Schedule of Specific Commitments of the Slovak Republic (doc. GATS/SC/77 of 15 April 1994); - Schedule of Specific Commitments of the Slovak Republic, Supplement 2 (doc. GATS/SC/77/Suppl.2 of 11 April 1997); - Schedule of Specific Commitments of the Slovak Republic, Supplement 3 (doc. GATS/SC/77/Suppl.3 of 26 February 1998); - Schedule of Specific Commitments of Finland (doc. GATS/SC/33 of 15 April 1994) and - Schedule of Specific Commitments of Sweden (doc. GATS/SC/82 of 15 April 1994)».

[47] WTO, *European Union Schedule of Specific Commitments. Supplement 1*, 27 febbraio 2024, GATS/SC/157/Suppl.1.

[48] WTO, *European Union Schedule of Specific Commitments*, cit., pp. 24-95.

[49] *Ibid*., pp. 58-64.

[50] *Ibid*., pp. 61-62.

[51] *Ibid*., pp. 62-63.

[52] *Ibid*., p. 64.

[53] *Ibid*., pp. 96-98.

[54] *Ibid*., pp. 97-98. I «*Telecommunications Services*» sono definiti, in tale sede, come segue: «*All services consisting of the transmission and reception of signals by any electromagnetic means, excluding broadcasting*».

[55] *Ibid*., pp. 118-157.

[56] *Ibid*., pp. 118-127 e pp. 142-148.

[57] *Ibid*., pp. 127-140 e pp. 149-157.

[58] *Ibid*., pp. 164-167.

[59] *Ibid*., pp. 165-166.

[60] *Ibid*., pp. 172-191.

[61] *Ibid*., pp. 180-181.

In questi settori l'UE ha dunque assunto impegni specifici, prevedendo altresì una serie di eccezioni agli stessi, la maggior parte delle quali non riguarda però il trattamento di dati personali [62].

È stato quindi accertato che l'Unione risulta vincolata da impegni specifici anche in settori in cui hanno luogo trattamenti e trasferimenti di dati personali. Resta ora da capire se la disciplina UE in materia di *personal data flows* può astrattamente porsi in contrasto con tali obblighi, i quali devono essere pertanto esaminati.

Tra gli impegni specifici, occorre innanzitutto analizzare il «*trattamento nazionale*» («*national treatment*»), disciplinato dall'art. XVII GATS. Ai sensi di quest'ultimo, un membro OMC ha l'obbligo (ovviamente in riferimento ai servizi inclusi nella propria lista) di accordare ai servizi e ai prestatori di servizi stranieri un trattamento non meno favorevole di quello accordato ad analoghi servizi e fornitori nazionali [63]. L'obbligo di non discriminazione può essere adempiuto prevedendo per i servizi e i fornitori stranieri sia un trattamento «formalmente identico», sia uno «formalmente diverso» rispetto a quello accordato ad analoghi servizi e prestatori di servizi nazionali, purché sia altrettanto favorevole [64]. Un trattamento «formalmente identico» o «formalmente diverso» è considerato meno favorevole qualora esso modifichi le condizioni della concorrenza a favore di servizi o fornitori di servizi del membro rispetto ad analoghi servizi o fornitori di servizi di un altro membro [65]. In buona sostanza, risultano vietate espressamente non solo le discriminazioni *de jure*, ma anche quelle *de facto* [66].

In ragione di quanto sopra, le verifiche da compiere, allo scopo di accertare la presenza di una violazione di tale obbligo da parte della disciplina UE in materia

---

[62] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 28.

[63] WTO, *General Agreement on Trade in Services*, cit., art. XVII («*National Treatment*»), par. 1.

[64] *Ibid*., par. 2.

[65] *Ibid*., par. 3.

[66] L'esplicito divieto delle discriminazioni *de facto* assume particolare rilevanza nel settore terziario, dove i regimi restrittivi non hanno per oggetto tanto i servizi, quanto soprattutto i prestatori. In tale settore, ad esempio, una discriminazione *de jure* potrebbe essere rappresentata da una norma nazionale che preveda un privilegio nell'assegnazione delle frequenze di trasmissione televisive ai fornitori nazionali di servizi audiovisivi a scapito dei fornitori stranieri. Sempre a titolo esemplificativo, saremmo invece di fronte a una discriminazione *de facto* in presenza di una norma nazionale che stabilisca il requisito della residenza ai fini dell'ottenimento di una licenza che abiliti alla prestazione di un determinato servizio: la norma, pur trattando indistintamente i prestatori stranieri e quelli nazionali da un punto di vista formale, di fatto offrirebbe un trattamento meno favorevole ai prestatori stranieri. In dottrina, sul punto, v.: C. Dordi, *op. cit.*, pp. 179-180. Un altro caso di discriminazione *de facto* potrebbe essere quello in cui uno Stato preveda che la consegna di una determinata certificazione o autorizzazione, indispensabile per la fornitura di un servizio sul suo mercato, possa essere fatta solo nelle mani di una persona fisica. Ciò comporterebbe, per i fornitori stranieri, l'onere di sostenere un viaggio all'estero, che sarebbe evitabile semplicemente attraverso la spedizione del documento. In dottrina, sul punto, v.: P. Picone-A. Ligustro, *op cit.*, p. 376.

di flussi di dati personali, finiscono per essere simili a quelle precedentemente analizzate in relazione alla CNPF. Per prima cosa, sarà ancora una volta necessario valutare caso per caso se sussista il requisito della «analogia» tra servizi o tra prestatori di servizi (valutazione che procederà nello stesso modo esposto poc'anzi) [67]. In secondo luogo, là dove l'analogia vi fosse, ci si dovrebbe chiedere se la disciplina in questione accordi un trattamento meno favorevole («*less favourable treatment*») ai servizi o prestatori stranieri, modificando le condizioni di concorrenza a vantaggio di quelli nazionali (analoghi, per l'appunto). E a tal riguardo, appare chiaro che i prestatori di Stati extra-UE che non sono destinatari di una decisione di adeguatezza sono in una posizione di svantaggio rispetto a quelli domestici, dal momento che per ricevere dall'UE i dati personali a loro necessari sono costretti a ricorrere agli onerosi e intrinsecamente limitati meccanismi alternativi del Capo V GDPR; tutto ciò, ovviamente, modifica le condizioni di concorrenza a favore dei servizi e dei fornitori dell'UE (nonché del SEE) [68]. Ancora una volta, gli «obiettivi ed effetti» («*aims and effects*») della misura non incideranno in alcun modo sulla qualificazione del trattamento come «meno favorevole» [69]. I competenti organi dell'OMC potrebbero quindi ritenere che la disciplina UE in esame accordi a servizi e prestatori di servizi stranieri (segnatamente, quelli di Stati extra-UE non beneficiari di decisioni di adeguatezza) un trattamento meno favorevole rispetto a quello accordato a servizi e prestatori domestici «analoghi». Potrebbero dunque ravvisare una violazione dell'art. XVII GATS, quantomeno *prima facie* (restando ovviamente ferma la possibilità di giustificare tale misura, come si vedrà).

Un altro impegno specifico presente nel GATS è poi quello dell'«accesso al mercato» («*market access*»), enunciato all'art. XVI, il quale impedisce ai membri dell'OMC di opporre ostacoli ingiustificati alla fornitura di servizi da parte di prestatori stranieri sul proprio mercato [70]: in particolare, il par. 2 dell'articolo

---

[67] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 33. Sul punto, v. anche: S. YAKOVLEVA-K. IRION, *The Best of Both Worlds?*, cit., p. 204. F. VELLI, *op. cit.*, p. 887.

[68] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., pp. 32-33; F. VELLI, *op. cit.*, p. 886. Sul punto, v. anche: S. YAKOVLEVA-K. IRION, *The Best of Both Worlds?*, cit., p. 204.

[69] WTO, *European Communities – Regime for the Importation, Sale and Distribution of Bananas. Report of the Appellate Body*, cit., § 241, in base a cui: «*We see no specific authority either in Article II or in Article XVII of the GATS for the proposition that the "aims and effects" of a measure are in any way relevant in determining whether that measure is inconsistent with those provisions […]*».

[70] Secondo certa dottrina, l'obbligo in questione rappresenterebbe un indubbio punto di forza del GATS: tale accordo non si accontenta di promuovere, attraverso le analizzate norme sul trattamento della nazione più favorita e sul trattamento nazionale, regimi interni che siano semplicemente non discriminatori, ma richiede positivamente l'apertura dei mercati nazionali agli operatori stranieri. Sul punto v.: B. HOEKMAN, *Services and Intellectual Property Rights*, in S.M. COLLINS, B.P. BOSWORTH (a cura di), *The New GATT: Implications for the United States*, Brookings, Washington, 1994.

in questione individua sei categorie di misure vietate, cinque delle quali riguardano forme diverse di restrizioni quantitative [71].

Orbene, a parere della dottrina le norme legislative dell'UE in materia di flussi transfrontalieri di dati personali non possono essere considerate alla stregua di restrizioni quantitative: esse, infatti, non fissano limiti né al numero dei prestatori di servizi, né al valore complessivo delle transazioni, né al numero complessivo di imprese di servizi o alla produzione totale di servizi, né al numero totale di persone fisiche che possono essere impiegate in un particolare settore o da un prestatore, né alla partecipazione di capitale estero; non ricadono, cioè, in nessuna delle ipotesi dell'art. XVI.2, lettere a), b), c), d), f). Tali norme non impongono neppure forme specifiche di personalità giuridica o di organizzazione dell'impresa per la prestazione di servizi, unica proibizione dell'elenco dell'art. XVI.2 che non riguarda restrizioni quantitative, contenuta alla lettera e). Di conseguenza, le norme UE in questione non ricadrebbero nel divieto dell'art. XVI GATS [72].

Vi potrebbe essere però un'eccezione: il caso in cui vi fosse una sospensione totale dei trasferimenti di dati personali verso uno Stato extra-UE. Una simile situazione, in verità, non si è mai verificata, neppure in seguito all'annullamento delle decisioni di adeguatezza adottate nei confronti degli USA, dal momento che è sempre e comunque rimasto possibile il ricorso ai meccanismi di trasferimento alternativi. Là dove però simili sospensioni avessero luogo, saremmo in presenza di contingenti numerici con limite zero («*zero quota*»), ovvero particolari forme di restrizioni quantitative vietate proprio dalle norme in materia di accesso al mercato; segnatamente, dall'art. XVI.2.a, che proibisce le limitazioni del numero dei prestatori di servizi [73], e dall'art. XVI.2.c, che vieta le limitazioni del numero complessivo di imprese di servizi o della produzione totale di servizi [74]. Sorgereb-

---

[71] WTO, *General Agreement on Trade in Services*, cit., art. XVI («*Market Access*»). Sul punto v., *inter alios*: P. Picone-A. Ligustro, *op cit.*, p. 377. V. anche: C. Dordi, *op. cit.*, pp. 175-176.

[72] S. Yakovleva-K. Irion, *The Best of Both Worlds?*, cit., p. 204, secondo cui: «*[…] EU rules on the transfer of personal data to third countries, on their face, do not appear to fall under any of the banned market access limitations under GATS Article XVI:2 […]*». Sul punto, v. anche: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 31.

[73] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit., § 238, in base a cui: «*For the above reasons, we are of the view that limitations amounting to a zero quota are quantitative limitations and fall within the scope of Article XVI:2(a)*».

[74] *Ibid.*, § 251, in base a cui: «*In this case, the measures at issue, by prohibiting the supply of services in respect of which a market access commitment has been taken, amount to a "zero quota" on service operations or output with respect to such services. As such, they fall within the scope of Article XVI:2(c)*»; § 252, in base a cui: «*For all of these reasons, we uphold the Panel's finding, in paragraph 6.355 of the Panel Report, that a measure prohibiting the supply of certain services where specific commitments have been undertaken is a limitation: … within the meaning of Article XVI:2(c) because it totally prevents the services operations and/or service output through one or more or all means of delivery that are included in mode 1. In other words, such a ban results in a "zero quota" on one or more or all means of delivery include in mode 1*».

be dunque, pure in questo caso, la necessità di giustificare la misura. È tuttavia doveroso precisare che, oltre a essere quella appena descritta un'ipotesi quasi esclusivamente teorica, si tratterebbe ancora di una volta di una violazione a livello applicativo e non legislativo [75].

Riepilogando, per quanto riguarda gli impegni specifici del GATS, ci si preoccuperà della necessità di dover giustificare eventuali violazioni *prima facie* soprattutto dell'art. XVII sul trattamento nazionale, ma anche dell'art. XVI in materia di accesso al mercato (sebbene un contrasto con quest'ultima disposizione sia più difficilmente configurabile). Tutto ciò, come è ovvio che sia, vale solo in relazione ai settori dove tali impegni specifici siano stati assunti.

2. *Le difficoltà nel giustificare le violazioni* prima facie *del GATS.*

Si è appena visto come le norme di diritto dell'Unione europea in materia di flussi di dati personali verso Stati extra-UE, o l'applicazione delle stesse, possano porsi in contrasto con svariati obblighi sanciti all'interno del *General Agreement on Trade in Services*: nello specifico, la clausola della nazione più favorita, la regolamentazione interna (ancorché con esclusivo riferimento all'art. VI.1), il trattamento nazionale, l'accesso al mercato (pur essendo questa un'ipotesi remota).

Tuttavia, come è già stato detto, là dove sia presente una violazione *prima facie* del GATS è possibile, a determinate condizioni, giustificarla attraverso le clausole di eccezione contenute nello stesso accordo. Resta dunque da vedere se tali clausole risultano utilizzabili in relazione alla disciplina in questione, circostanza che la metterebbe al riparo da una pronuncia sfavorevole da parte degli organi dell'OMC.

---

[75] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 32, secondo cui: «*[…] Provided a situation would arise that dictates a full suspension of the rules on transfer of personal data to a certain third country, this could amount to a market access restriction contrary to GATS Article XVI.1 and the finding of a "zero quota" under GATS Article XVI.2(a) and (c). This measure – again not at the level of legislation – would require justification and would therefore be submitted to the general exceptions of GATS Article XIV […]*»; S. YAKOVLEVA-K. IRION, *The Best of Both Worlds?*, cit., pp. 204-205, secondo cui: «*[…] In the literature it is argued that the default prohibition on the transfer of personal data to third countries with inadequate protection effectively constitutes a 'zero quota' violating GATS Article XVI:2(a) and (c)*», ma, in ragione della presenza dei meccanismi alternativi: «*[…] a finding of GATS inconsistent 'zero quota' market access barriers can hardly be made […]*»; F. VELLI, *op. cit.*, p. 887, secondo cui: «*[…] the only situation that could result in such an automatic market restriction would be if there were a full suspension of the rules on the transfer of personal data to a third country. This has never happened in practice so far, not even after the annulment of Safe Harbour, but an interruption of data transfers might amount to a market access restriction contrary to Art. XVI:1 GATS and to a zero quota under Art. XVI:2, let. a) and c), GATS […]*».

2.1. *L'integrazione economica*

Per prima cosa, occorre partire dall'«integrazione economica» («*economic integration*») dell'art. V, che nel rispetto di determinate condizioni permette agli Stati di concludere accordi che liberalizzino gli scambi di servizi tra le sole parti contraenti, senza incorrere per tale fatto in violazioni degli obblighi del GATS[76].

Orbene, il mercato interno dell'UE/SEE rappresenta senza alcun dubbio una forma di integrazione economica regionale ai sensi dell'art. V del GATS, come è stato notificato da parte delle Comunità europee agli altri membri dell'OMC già con un documento del 1998[77].

Risultano infatti rispettate le condizioni fissate dalla disposizione in esame. In particolare, per poter essere sussumibile nell'art. V GATS, un accordo di integrazione deve riguardare un numero sostanziale di settori, coinvolgendo almeno tendenzialmente la maggior parte degli scambi di servizi tra i suoi membri, e non può escludere *a priori* determinate modalità di fornitura dei servizi dai benefici dell'integrazione stessa. Inoltre, l'integrazione deve comportare l'eliminazione di ogni discriminazione tra servizi resi da un fornitore nazionale e servizi similari provenienti da altri Paesi (obiettivo perseguito anche mediante una clausola di «*stand-still*», che vieta l'introduzione di misure discriminatorie nuove o più severe rispetto a quelle esistenti al momento dell'entrata in vigore dell'accordo)[78].

Tali requisiti sono indubbiamente presenti nell'UE: come si legge nel menzionato documento del 1998, nell'ambito della stessa l'integrazione copre tutti i settori e le attività di servizi, e le misure sui servizi si applicano a tutte le modalità di fornitura[79]; in aggiunta, come è ben noto, fin dalle sue origini la Comunità europea è stata costruita sul principio fondamentale della non-discriminazione riguardante tutti gli scambi intra-comunitari fra Stati membri: vi è infatti un divieto generale di discriminazione sulla base della nazionalità e sono poi previsti divieti di discriminazione più specifici in particolari ambiti, segnatamente il diritto di stabilimento e la fornitura di servizi[80].

Inoltre, l'UE rispetta anche la condizione, stabilita dall'art. V.4 GATS, in

---

[76] WTO, *General Agreement on Trade in Services*, cit., art. V («*Economic Integration*»).

[77] WTO, *Establishment of the European Union, Services. Communication from the European Communities and their Member States*, 24 aprile 1998, WT/REG39/1. Tale documento è stato proprio adottato «*[f]ollowing the request to examine the European Communities and their twelve Member States under Article V of the GATS […]*», come si legge a p. 1.

[78] Sul punto v., *inter alios*: P. PICONE-A. LIGUSTRO, *op cit.*, p. 372.

[79] WTO, *Establishment of the European Union, Services. Communication from the European Communities and their Member States*, cit., p. 4, secondo cui: «*[…] In the EC the integration covers all services sectors and activities. The measures on services apply to all modes of supply […]*».

[80] *Ibid.*, p. 5, secondo cui: «*[…] The EC is built upon the fundamental principle of non-discrimination for all intra-Community trade among Member States. There is a general prohibition of discrimination on grounds of nationality […]. In addition […] more specific prohibitions of discrimination for particular areas, notably on the right of establishment and supply of services […]*».

base a cui l'integrazione deve essere finalizzata a facilitare gli scambi tra le parti contraenti piuttosto che all'innalzamento delle barriere esistenti nei confronti dei membri non aderenti all'integrazione stessa (disposizione volta a evitare la costituzione dei cosiddetti «*stumbling blocks*», cioè di accordi che, più che porre in essere un'integrazione regionale, sono in realtà diretti ad adottare un atteggiamento protezionistico verso l'esterno) [81]. Come si legge sempre nel citato documento del 1998, infatti, nessuna disposizione dell'accordo innalza il livello delle restrizioni agli scambi di servizi nei confronti di qualsiasi altro membro dell'OMC [82].

Avendo appurato che l'UE rappresenta un'integrazione economica *ex* art. V GATS, è possibile affermare che tale disposizione costituirebbe la primissima difesa nel caso in cui la disciplina in materia di dati personali fosse accusata di accordare un trattamento meno favorevole ai servizi o ai prestatori di servizi di un membro dell'OMC, non facente però parte dell'Unione, rispetto a quello accordato ai servizi o prestatori analoghi di uno Stato UE [83]. Come ben evidenziato, il GDPR prevede infatti un regime di libera circolazione dei dati personali all'interno dell'UE, mentre affinché abbiano luogo trasferimenti al di fuori della stessa è necessario il rispetto dei requisiti del Capo V: ciò comporta indubbiamente una posizione di vantaggio per i prestatori operanti nell'Unione, che beneficiano in modo incondizionato del diritto di ricevere da altri Paesi UE i dati personali necessari per la fornitura dei loro servizi, rispetto a quelli analoghi di Stati terzi. Tuttavia, a parere di rilevante dottrina, là dove un Paese extra-UE contestasse, ad esempio, una violazione della CNPF in ragione di quanto esposto, difficilmente tale contestazione potrebbe trovare accoglimento: l'art. V GATS fornirebbe una pronta giustificazione proprio per casi come questo [84].

La norma in esame, tuttavia, non potrebbe offrire alcun aiuto là dove venisse contestata un'altra ipotesi di violazione della CNPF: quella, teorizzata in precedenza, del trattamento meno favorevole accordato ai servizi o prestatori di servizi di quei membri OMC (extra-UE) che non hanno ottenuto una decisione di adeguatezza, rispetto a quello accordato ai servizi o prestatori analoghi di quei membri OMC (sempre extra-UE) che invece beneficiano di una simile misura.

---

[81] Sul punto v., *inter alios*: P. PICONE-A. LIGUSTRO, *op cit.*, pp. 372-373.

[82] WTO, *Establishment of the European Union, Services. Communication from the European Communities and their Member States*, cit., p. 7, secondo cui: «*[…] No provisions in the Agreement raise the level of restrictions on trade in services for any other WTO Member […]*».

[83] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 33, secondo cui: «*[…] This provision […] would likely be the first line of defence for the EU if an EU measure were found to accord less favourable treatment to a WTO Member State as compared to an EU Member State […]*».

[84] F. VELLI, *op. cit.*, p. 888, secondo cui: «*[…] Art. V GATS could be deemed a first justification in case of a breach of the MFN obligation […]*». V. anche: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 34, secondo cui: «*[…] A third country outside the EU/EEA, even if treated less favourably than a Member State of the EU/EEA, is unlikely to successfully invoke MFN […] of the GATS […]*».

2.2. *Le eccezioni generali*

Per quanto riguarda tutte le eventuali violazioni degli obblighi del GATS che, per loro natura, non possono essere giustificate attraverso l'art. V sull'integrazione economica, vi è però un'altra possibilità: quella di ricorrere alle «eccezioni generali» («*general exceptions*») dell'art. XIV, le quali costituiscono espressione del diritto dei membri di regolamentare («*right to regulate*») la fornitura di servizi nei rispettivi territori, al fine di rispettare gli obiettivi di politica nazionale (come enunciato nel Preambolo del GATS medesimo) [85].

Il testo della disposizione in esame prevede, dopo un «cappello» («*chapeau*») introduttivo, un elenco di eccezioni identificate con varie lettere [86]. Affinché essa possa essere invocata, come chiarito dagli organi dell'OMC, occorre *in primis* accertare che la misura di cui trattasi rientri nell'ambito di applicazione di una delle cause di giustificazione contenute nelle lettere dalla a) alla e) dell'articolo; in caso di esito positivo di tale accertamento, si rende necessaria una valutazione della compatibilità con il «cappello» introduttivo di cui sopra: quest'ultimo, infatti, richiede che l'applicazione delle misure eccezionalmente consentite non causi «discriminazioni arbitrarie o ingiustificate tra Paesi dove vigono condizioni analoghe», né produca «restrizioni dissimulate agli scambi di servizi». La verifica appena descritta prende il nome di «analisi a due livelli» («*two-tier analysis*») [87].

Per quanto riguarda più nel dettaglio le misure giustificabili *ex* art. XIV GATS, nell'elenco figurano *inter alia* le misure necessarie a salvaguardare la morale pubblica o a mantenere l'ordine pubblico (art. XIV.a), nonché le misure necessarie ai fini della tutela della vita o della salute delle persone, e del mondo animale o vegetale (art. XIV.b). Figura altresì un'ipotesi di grande interesse ai nostri fini: quella delle misure necessarie per garantire l'osservanza di leggi e regolamenti non incompatibili con le disposizioni del GATS («*necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement*»), ivi compresi quelli relativi alla tutela della *privacy* delle persone fisiche in relazione all'elaborazione e alla diffusione di dati personali («*protection of the privacy of individuals in relation to the processing and dissemination of personal data*»), nonché alla protezione della riservatezza di registri e documenti contabili di persone fisiche (art. XIV.c.ii).

---

[85] Sul punto v., *inter alios*: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 34.

[86] WTO, *General Agreement on Trade in Services*, cit., art. XIV («*General Exceptions*»).

[87] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit., § 292, in base a cui: «*Article XIV of the GATS, like Article XX of the GATT 1994, contemplates a "two-tier analysis" of a measure that a Member seeks to justify under that provision. A panel should first determine whether the challenged measure falls within the scope of one of the paragraphs of Article XIV […] Where the challenged measure has been found to fall within one of the paragraphs of Article XIV, a panel should then consider whether that measure satisfies the requirements of the chapeau of Article XIV*».

Da una prima lettura, l'ultima disposizione citata parrebbe in grado di risolvere ogni problema e di mettere la normativa UE sui flussi transfrontalieri di dati personali al riparo da tutte le contestazioni precedentemente ipotizzate. Tuttavia, da un'analisi più attenta della norma, nonché delle pronunce degli organi dell'OMC in materia di «*general exceptions*», emerge un quadro meno tranquillizzante: come si dirà a breve, là dove venisse avviata in seno all'Organizzazione mondiale del commercio una controversia finalizzata a mettere in discussione la compatibilità col GATS della disciplina UE sui *personal data flows*, l'Unione potrebbe avere rilevanti difficoltà a giustificare quest'ultima attraverso l'art. XIV.c.ii.

Per motivare una simile affermazione, si rende indispensabile svolgere, in riferimento al caso in esame, quella «analisi a due livelli» di cui si è detto sopra. Innanzitutto, occorre quindi accertare la presenza dei requisiti richiesti da una delle lettere – dalla a) alla e) – dell'art. XIV GATS, soffermandosi segnatamente sulla lettera c), numero ii), che si è visto essere l'ipotesi più pertinente ai fini della presente trattazione.

Gli organi dell'OMC hanno chiarito che per poter ritenere applicabile una delle opzioni della lettera c) dell'art. XIV – e quindi anche quella del numero ii) – è necessario svolgere un accertamento ulteriormente suddiviso in tre fasi. *In primis*, serve che la misura da giustificare sia pensata per «garantire l'osservanza» («*secure compliance*») di leggi e regolamenti, relativi, nel caso specifico del numero ii), alla tutela della *privacy* delle persone fisiche in relazione all'elaborazione e alla diffusione di dati personali. In seconda battuta, tali leggi e regolamenti devono essere «non incompatibili» («*not inconsistent*») con le disposizioni del GATS. In ultima istanza, la misura in esame deve essere «necessaria» («*necessary*») per garantire l'osservanza di tali leggi e regolamenti [88]. Da mettere in evidenza, inoltre, che l'onere della prova circa la sussistenza di tali condizioni grava sul membro OMC convenuto [89].

Nel caso in esame, l'Unione europea riuscirebbe con buona probabilità a dimostrare la presenza delle prime due condizioni. Come ricorda anche il più volte menzionato Considerando 101 del Regolamento (UE) 2016/679, le regole in materia di trasferimenti di dati personali fuori dall'UE sono finalizzate ad

[88] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Panel*, cit., § 6.563, in base a cui: «*Pursuant to the text of Article XIV(c), in determining whether a challenged measure is provisionally justified under that Article, three elements must be demonstrated by the Member who invokes Article XIV(c), namely: (a) the measure for which justification is claimed must "secure compliance" with other laws or regulations; (b) those other "laws or regulations" must not be inconsistent with the WTO Agreement; and (c) the measure for which justification is claimed must be "necessary" to secure compliance with those other laws or regulations*».

[89] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 35. Più in generale, sull'onere della prova nell'Organizzazione mondiale del commercio, v. *inter alios*: F. Martines, *L'onere della prova nell'Organizzazione Mondiale del Commercio e valori del sistema*, Maggioli, Rimini, 2012.

assicurare che il livello di tutela delle persone fisiche accordato nell'Unione dallo stesso Regolamento non sia compromesso; detto in altri termini, ciò vuol dire proprio che siamo in presenza di misure pensate per «garantire l'osservanza» delle norme del GDPR in materia di protezione dei dati personali, tra cui, a titolo esemplificativo, i principi applicabili al trattamento [90], nonché i diritti delle persone interessate [91]. È inoltre chiaro che le norme appena citate siano «non incompatibili» con le disposizioni del GATS, dal momento che esse non discriminano in alcun modo tra servizi o prestatori di servizi (possono essere le misure che richiedono giustificazione a farlo, ma non le norme alla cui osservanza tali misure sono preordinate) [92].

Molto meno scontata, tuttavia, è la circostanza che l'UE riesca a dimostrare la «necessità» di tali misure. Come emerge dalle pronunce degli organi dell'OMC, è tanto più probabile che una misura superi il «test di necessità» quanto più è meritevole l'interesse che essa persegue [93], quanto più essa contribuisce alla realizzazione di tale interesse [94], e quanto meno essa è restrittiva per gli scambi internazionali [95]. Appare dunque chiaro che, per valutare se la misura è o meno necessaria, occorrerà svolgere un processo di «ponderazione e bilanciamento di una serie di fattori» («*a process of weighing and balancing a series of factors*») [96]

---

[90] Ai sensi dell'art. 5 del Regolamento (UE) 2016/679, tali principi sono: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione.

[91] Tra questi, ai sensi del Capo III del Regolamento (UE) 2016/679, figurano *inter alia*: il diritto di accesso (art. 15), il diritto di rettifica (art. 16), il diritto alla cancellazione (art. 17), il diritto di limitazione di trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), il diritto di opposizione (art. 21).

[92] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 36. V. anche: F. Velli, *op. cit.*, p. 889.

[93] WTO, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef. Report of the Appellate Body*, 11 dicembre 2000, WT/DS161/AB/R, WT/DS169/AB/R, § 162, in base a cui: «*[…] The more vital or important those common interests or values are, the easier it would be to accept as "necessary" a measure designed as an enforcement instrument*».

[94] *Ibid*., § 163, in base a cui: «*There are other aspects of the enforcement measure to be considered in evaluating that measure as "necessary". One is the extent to which the measure contributes to the realization of the end pursued, the securing of compliance with the law or regulation at issue. The greater the contribution, the more easily a measure might be considered to be "necessary" […]*». In tal senso v. anche: WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Panel*, cit., § 7.685.

[95] WTO, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef. Report of the Appellate Body*, cit., § 163, in base a cui: «*[…] Another aspect is the extent to which the compliance measure produces restrictive effects […]. A measure with a relatively slight impact […] might more easily be considered as "necessary" than a measure with intense or broader restrictive effects*». In tal senso v. anche: WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Panel*, cit., § 7.727.

[96] WTO, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef. Report of the Appellate Body*, cit., § 163: «*In sum, determination of whether a measure, which is not "indis-*

che può variare sensibilmente e che, alla luce del margine di discrezionalità di cui godono gli organi dell'OMC, può portare a risultati difficilmente pronosticabili [97].

In particolare, proprio per quanto riguarda la loro «necessità», le regole in materia di flussi di dati personali verso Paesi extra-UE presentano alcuni punti deboli che possono rendere assolutamente incerto l'esito del giudizio. Nello specifico, il fatto che ben due decisioni di adeguatezza (entrambe adottate nei confronti degli Stati Uniti) siano state prima fortemente contestate nella loro effettività e poi addirittura annullate dalla Corte di giustizia, non deporrebbe certo a favore di un'eventuale linea difensiva dell'Unione. Ciò, infatti, potrebbe portare ad affermare che le decisioni di adeguatezza non riescono ad assicurare che il livello di protezione dei dati personali garantito nell'UE dal GDPR non sia compromesso: verrebbe così messo in serio dubbio il reale contributo che le misure in esame forniscono alla realizzazione dell'obiettivo perseguito, elemento che invece è fondamentale per addivenire a un giudizio di «necessità» delle stesse [98].

Inoltre, occorre considerare un'altra eventualità: il membro OMC che rivestisse il ruolo di attore potrebbe anche cercare di dimostrare che era «ragionevolmente disponibile» («*reasonably available*») un'alternativa meno restrittiva rispetto alla misura in questione (in questo caso, l'onere della prova non graverebbe dunque sul membro convenuto) [99]. Una simile contestazione potrebbe anche essere ritenuta fondata: confrontando la disciplina sui trasferimenti oltrefrontiera dei dati dell'Unione europea con altre adottate a livello internazionale, ci si rende facilmente conto di come la prima sia senz'altro quella che richiede lo standard di protezione più elevato e, di conseguenza, anche quella che incide in modo più negativo sugli scambi di servizi [100]. Al contrario, come evidenziato a suo tempo nella presente trattazione, vi sono discipline strutturate diversamente che sono ben più sensibili alle esigenze di carattere economico e commerciale: in particolare, le Linee guida dell'OCSE, che adottano un approccio «dal basso verso l'alto» (si prende le mosse da una situazione in cui non solo i flussi sono

---

pensable", may nevertheless be "necessary" within the contemplation of Article XX(d), involves in every case a process of weighing and balancing a series of factors which prominently include the contribution made by the compliance measure to the enforcement of the law or regulation at issue, the importance of the common interests or values protected by that law or regulation, and the accompanying impact of the law or regulation […]». In tal senso v. anche: WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit., § 305; WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Panel*, cit., § 7.659.

[97] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 37.

[98] *Ibid.*.

[99] WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit., § 308 ss..

[100] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 37.

consentiti, ma addirittura vi è un divieto di ostacolarli; limitare i flussi e incrementare il livello di protezione dei dati è invece possibile soltanto in presenza di determinate condizioni); ma un altro esempio può essere rappresentato dal sistema APEC [101]. Orbene, là dove gli organi dell'OMC si convincessero che tali discipline, oltre a incidere in misura minore sugli scambi, riescano comunque a raggiungere i medesimi risultati, la normativa UE sui *personal data flows* finirebbe inevitabilmente per non superare il «test di necessità» [102].

Ma anche là dove il «test di necessità» dovesse essere superato, la «*two-tier analysis*» non sarebbe certo conclusa: mancherebbe il secondo livello della stessa, ovvero la valutazione circa la sussistenza delle condizioni sancite nel «cappello» («*chapeau*») introduttivo dell'art. XIV GATS. Esso, lo si è anticipato, richiede che l'applicazione delle misure eccezionalmente consentite non causi «discriminazioni arbitrarie o ingiustificate tra Paesi dove vigono condizioni analoghe» («*arbitrary or unjustifiable discrimination between countries where like conditions prevail*»), né produca «restrizioni dissimulate agli scambi di servizi» («*disguised restriction on trade in services*»). La sua funzione, in buona sostanza, è quella di impedire un abuso o un uso improprio del diritto di un membro di invocare le eccezioni elencate nelle lettere dalla a) alla e) dell'articolo [103]. Quanto invece alla sua interpretazione, certe pronunce degli organi OMC hanno finito per declinare lo standard da esso richiesto in termini di «coerenza» («*consistency*») delle misure contestate [104]: conseguentemente, qualora una normativa presenti elementi di «ambiguità» («*ambiguity*»), le condizioni richieste dal cappello non possono ritenersi integrate [105].

In ragione di quanto esposto, anche il fatto che l'Unione europea riesca a dimostrare che siano rispettati tutti i requisiti del «*chapeau*» dell'art. XIV GATS è tutt'altro che automatico. In particolare, una critica assai fondata potrebbe essere quella riguardante le decisioni di adeguatezza parziali o settoriali, precedentemente trattate, la cui esistenza crea significativi problemi: in presenza di Stati extra-UE i cui ordinamenti non assicurano, quantomeno nella loro interezza, un livello di protezione adeguato (cioè, «sostanzialmente equivalente» a quello dell'Unione), in alcuni casi – Canada, Israele, Giappone, Regno Unito, Repubblica di Corea, Stati Uniti – si è fatto uno sforzo per addivenire a soluzioni creative e adottare decisioni che coprissero almeno parte di tali ordinamenti;

---

[101] S. YAKOVLEVA-K. IRION, *Pitching trade against privacy: reconciling EU governance of personal data flows with external trade*, in *International Data Privacy Law*, 2020, Volume 10, Numero 3, pp. 201-221, spec. pp. 211-212. V. anche: F. VELLI, *op. cit.*, p. 889.

[102] K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 37; S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 212.

[103] Sul punto v., *inter alia*: WTO, *Argentina – Measures Relating to Trade in Goods and Services. Report of the Panel*, cit., § 7.743.

[104] Sul punto v., *inter alia*: WTO, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body*, cit., § 351.

[105] *Ibid.*, § 368 e § 369.

in altri casi – si pensi, banalmente, a quello dell'Australia – non è stata invece adottata alcuna decisione di adeguatezza, con conseguente pregiudizio per i servizi e i prestatori dei Paesi interessati, costretti ad avvalersi degli onerosi e intrinsecamente limitati meccanismi alternativi del Capo V GDPR.

Non solo. L'adozione di simili decisioni settoriali nei confronti di ordinamenti che non sono «adeguati» nella loro interezza stride anche, anzi ancor di più, con la possibilità che non vengano adottate decisioni di adeguatezza di alcun tipo pur in presenza di Stati che assicurano un livello di protezione «sostanzialmente equivalente» a quello dell'UE. Si è visto come, ad esempio, il Gruppo di lavoro «Articolo 29» abbia adottato un parere in cui si è espresso in modo sostanzialmente favorevole circa l'adozione di una decisione di adeguatezza nei confronti del Principato di Monaco [106]; tuttavia, una simile decisione non è stata ancora adottata, circostanza che rende tale Paese a tutti gli effetti «non adeguato» [107]. Occorre ricordare che il Principato di Monaco non è membro dell'OMC; là dove però una situazione come quella appena descritta si verificasse nei confronti di uno Stato che invece ne fa parte, i servizi e prestatori di tale Paese – «adeguato» nella sostanza, ma non formalmente riconosciuto come tale dalla Commissione europea – sarebbero posti in una posizione sfavorevole del tutto ingiustificata ai sensi del diritto dell'Organizzazione.

Gli organi dell'OMC potrebbero quindi ritenere che la prassi applicativa della Commissione nell'adozione delle decisioni di adeguatezza sia «incoerente», causando «discriminazioni arbitrarie o ingiustificate tra Paesi dove vigono condizioni analoghe» [108]. Ciò comporterebbe, automaticamente, il mancato rispetto delle condizioni richieste dal cappello dell'art. XIV GATS, e come ulteriore conseguenza l'impossibilità di giustificare una qualsiasi violazione dell'Accordo stesso.

È dunque possibile affermare che là dove fosse ravvisata la presenza di una violazione delle prescrizioni del GATS da parte delle regole in materia di trasferimenti di dati personali fuori dall'UE, l'Unione stessa non potrebbe far eccessivo affidamento sull'eccezione generale dell'art. XIV.c.ii: tanti sono gli elementi che devono essere presenti (la necessità, le condizioni del «*chapeau*») e tanti sono i punti deboli della disciplina in questione. Inoltre, circostanza ancor più importante quantomeno sul piano pratico, gli organi dell'OMC hanno dimostrato nel corso del tempo di svolgere una valutazione estremamente rigorosa circa la sussistenza dei requisiti richiesti dalle «*general exceptions*» (sia quelle dell'art. XIV GATS, che quelle dell'art. XX GATT, disposizione corrispondente), così rigorosa da rendere quasi proibitivo il ricorso alle stesse.

---

[106] UE, Gruppo di lavoro «Articolo 29», *Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco*, 19 luglio 2012, WP 198.

[107] C. KUNER, *Article 45. Transfers on the basis of an adequacy decision*, in C. KUNER-L.A. BYGRAVE-C. DOCKSEY (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 771-796, spec. p. 777.

[108] Sul punto, v: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 38; F. VELLI, *op. cit.*, p. 889.

Basti pensare che nel 2015 il sistema di risoluzione delle controversie dell'OMC è stato criticato per il fatto che, su ben 44 casi in cui erano state invocate le eccezioni generali, soltanto in uno di essi tale invocazione aveva avuto successo [109].

In definitiva, l'intera analisi sul punto si può concludere con le considerazioni seguenti: l'approccio proprio del diritto OMC, che dà grande importanza alle esigenze dell'espansione del commercio internazionale, diverge sensibilmente da quello assai restrittivo che caratterizza la disciplina UE in materia di flussi di dati personali verso Paesi terzi. Ciò implica che quest'ultima possa porsi in contrasto con svariati obblighi presenti nel GATS: clausola della nazione più favorita, regolamentazione interna (con esclusivo riferimento all'art. VI.1), trattamento nazionale, accesso al mercato (ipotesi remota). Inoltre, nel caso in cui vi fosse una procedura di fronte agli organi OMC, tali violazioni sarebbero per varie ragioni molto difficili da giustificare. L'Unione europea rischierebbe quindi di incorrere in una pronuncia sfavorevole, con tutte le conseguenze negative da essa derivanti, come la possibile adozione di contromisure commerciali [110].

[109] CITIZEN.ORG, *Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded*, 19 agosto 2015, reperibile al seguente link: *https://www.citizen.org/article/only-one-of-44-attempts-to-use-the-wtos-general-exception-to-only-one-of-44-attempts-to-use-the-gatt-article-xx-gats-article-xiv-general-exception-has-ever/* (ultimo accesso in data 31 dicembre 2024). Sul punto v. anche: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 34; F. VELLI, *op. cit.*, p. 889.

[110] WTO, *Annex 2 to the Agreement Establishing the World Trade Organization – Understanding on rules and procedures governing the settlement of disputes*, Marrakesh, 15 aprile 1994. Le contromisure commerciali adottate dalla parte vincitrice possono anche colpire settori diversi da quelli implicati nel contenzioso: si parla di «ritorsioni incrociate» o «*cross retaliation*». In dottrina, sul punto, v. *inter alios*: F. MARRELLA, *op. cit.*, p. 709.

CAPITOLO II

GLI IMPEGNI, INSERITI IN ACCORDI INTERNAZIONALI DI NATURA COMMERCIALE DELL'UE, VOLTI A CONSENTIRE I FLUSSI DI DATI

SOMMARIO: 1. Gli impegni al trasferimento di dati contenuti in strumenti multilaterali facenti parte del *corpus* normativo dell'OMC. – 1.1. L'«*Understanding on Commitments in Financial Services*». – 1.2. L'«*Annex on Telecommunications*». – 2. Gli impegni al trasferimento di dati contenuti in accordi bilaterali di natura (anche solo parzialmente) commerciale conclusi dall'UE con Stati terzi. – 2.1. Il *Comprehensive Economic and Trade Agreement* (CETA) con il Canada. – 2.2. Alcuni accordi meno recenti: l'Accordo di libero scambio con la Corea del Sud e l'Accordo commerciale con Colombia, Perù ed Ecuador. – 2.3. Alcuni accordi meno recenti: gli Accordi di Associazione con l'America centrale e con l'Ucraina *(segue)*. – 2.4. Alcuni accordi più recenti: l'*Economic Partnership Agreement* (EPA) con il Giappone. – 2.5. Alcuni accordi più recenti: gli Accordi di libero scambio con la Repubblica di Singapore e con la Repubblica socialista del Vietnam *(segue).* – 3. Le criticità degli impegni al trasferimento di dati, e delle disposizioni finalizzate a controbilanciarli, negli accordi commerciali dell'UE. – 3.1. Le criticità derivanti dalla semplice presenza di previsioni in materia di dati personali negli accordi commerciali dell'UE. – 3.2. Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: alcuni miglioramenti. – 3.3. Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: problematiche perduranti *(segue)*. – 3.4. Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: la nozione di «adeguatezza» e il ruolo degli organismi sovranazionali di risoluzione delle controversie *(segue)*.

L'analisi non può però arrestarsi al rapporto tra l'attuale disciplina UE in materia di flussi e gli obblighi, contenuti nel diritto dell'OMC, concernenti in generale la liberalizzazione dei servizi. Occorre occuparsi altresì del rapporto tra la normativa UE e certe disposizioni – inserite in alcuni degli accordi internazionali di natura (esclusivamente o anche solo parzialmente) commerciale conclusi dall'Unione – che rappresentano dei veri e propri impegni al trasferimento dei dati, anche denominati «*data flows commitments*». Tali impegni, chiaramente finalizzati a incentivare i flussi di dati personali in ragione della grande importanza che essi rivestono nell'ambito del commercio globale, sono poi controbilanciati da previsioni finalizzate alla salvaguardia della *privacy* e del diritto alla protezione dei dati personali, altrimenti dette «*data protection provisions*».

Per prima cosa, sarà dunque essenziale passare in rassegna simili impegni: si partirà da quelli contenuti in strumenti più risalenti, aventi natura multilaterale e facenti parte a loro volta del *corpus* normativo dell'OMC, e si arriverà poi a quelli inseriti in accordi più recenti, che hanno invece carattere bilaterale e sono conclusi dall'UE al di fuori del quadro giuridico dell'OMC.

Dopo una simile analisi, sarà finalmente possibile interrogarsi sul rapporto tra la disciplina UE in materia di trasferimenti oltrefrontiera di dati personali e le previsioni sui flussi inserite negli appena menzionati strumenti. In particolare, ci si dovrà chiedere se, nella prospettiva del diritto UE, la semplice presenza o la concreta formulazione di disposizioni di tal genere in accordi internazionali che vincolano l'Unione sollevi o meno delle criticità. Nel caso, occorrerà pure domandarsi se vi siano stati dei miglioramenti tra i più risalenti degli articoli in questione e quelli più recenti.

Anche la presente parte di trattazione, specularmente alla precedente, avrà quindi l'obiettivo di comprendere se vi possano essere difficoltà nel coordinare la disciplina UE in esame con impegni commerciali assunti dall'Unione a livello internazionale; e ancora una volta, in caso siano configurabili incompatibilità, si dovranno capire le possibili conseguenze in cui può incorrere l'UE.

1. *Gli impegni al trasferimento di dati contenuti in strumenti multilaterali facenti parte del* corpus *normativo dell'OMC*

1.1. *L'«*Understanding on Commitments in Financial Services»

Come anticipato, è opportuno prendere le mosse dai *data flows commitments* contenuti negli strumenti più risalenti, aventi natura multilaterale e facenti parte del diritto dell'Organizzazione mondiale del commercio.

Tra questi, innanzitutto, figura l'Intesa sugli impegni nel settore dei servizi finanziari o «*Understanding on Commitments in Financial Services*» del 1994 [1]. Si tratta di uno standard elevato di impegni nel settore dei servizi finanziari, che prevede in tale ambito una liberalizzazione ancora più ampia di quella richiesta dalle norme del GATS [2]. L'Intesa non ha valore giuridico vincolante, ecce-

[1] WTO, *Understanding on Commitments in Financial Services*, Marrakesh, 15 aprile 1994. Sul punto v. la pagina del sito dell'OMC dedicata ai «*Financial services*», consultabile al seguente link: *https://www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm* (ultimo accesso in data 31 dicembre 2024).

[2] Department of Finance of Canada, *The General Agreement on Trade in Services. The Financial Services Sector*, dicembre 1995, p. 6, secondo cui: «*[…] the Understanding on Commitments in Financial Services is a voluntary "high" standard of commitments in the financial services sector. It encompasses broader liberalization commitments than those required under the general provisions of the GATS* […]».

zion fatta per quei membri che su base volontaria fanno riferimento alla stessa nell'individuazione dei loro impegni in materia di servizi finanziari [3]. Come chiarito nel Preambolo di tale strumento, i membri hanno dunque la facoltà di assumere nel settore impegni specifici sulla base di un'impostazione alternativa rispetto a quella del GATS [4].

Sul punto, merita di essere sottolineato che non tutti, ma numerosi Stati dell'UE hanno assunto i loro impegni, in relazione ai servizi finanziari, proprio ai sensi delle disposizioni dell'*Understanding* [5].

La previsione dell'Intesa che assume particolare rilievo ai fini della presente trattazione è l'art. B.8, dedicato proprio a «*Transfers of Information and Processing of Information*», il quale risulta suddiviso in due parti. La prima rappresenta un vero e proprio impegno al trasferimento di dati personali: in capo ai membri, infatti, è posto il divieto di adottare misure che impediscano la trasmissione di informazioni là dove essa risulti necessaria per lo svolgimento dell'attività ordinaria di un fornitore di servizi finanziari. La seconda parte, invece, contiene una clausola derogatoria (anche detta «*carve-out clause*»): in base alla stessa, infatti, nessun elemento della disposizione in esame limita il diritto dei membri di proteggere i dati personali e la *privacy*, sempreché tale diritto non sia utilizzato per eludere le previsioni del GATS [6].

Occorre puntualizzare che l'*Understanding* risulta essere cronologicamente antecedente non solo al Regolamento (UE) 2016/679, ma anche alla Direttiva 95/46/CE: nel 1994, l'Unione europea non era dotata di alcuna legislazione in materia di protezione dei dati personali. Ciò non toglie che, come anticipato e

---

[3] C. RAGHAVAN, *Financial Services, the WTO and Initiatives for Global Financial Reform*, in J.K. SUNDARAM (a cura di), *Reforming the International Financial System for Development*, Columbia University Press, New York, pp. 218-242, secondo cui: «*[…] The Understanding, as an alternative approach or modality for scheduling commitments, did not form part of the agreement and had no legal value, except perhaps for those who explicitly or implicitly referenced the Understanding in scheduling their financial services commitments […]*».

[4] In base al Preambolo dell'*Understanding on Commitments in Financial Services*: «*Participants in the Uruguay Round have been enabled to take on specific commitments with respect to financial services under the General Agreement on Trade in Services (hereinafter referred to as the "Agreement") on the basis of an alternative approach to that covered by the provisions of Part III of the Agreement […]*» (la «*Part III*» del GATS è quella dedicata agli «*Specific Commitments*»).

[5] WTO, *European Union Schedule of Specific Commitments*, cit., p. 118, in base a cui: «*[…] Part of the EC (AT, BE, CZ, DK, DE, ES, FI, FR, EL, HU, IT, IE, LU, NL, PT, SE, SK […]) undertakes commitments on Financial Services in accordance with the provisions of the "Understanding on Commitments in Financial Services" (the Understanding). […] Commitments on Financial Services of the other part of the EC (CY, EE, LV, LT, MT, PL, SI) are not based on the Understanding […]*».

[6] WTO, *Understanding on Commitments in Financial Services*, cit., art. B.8. In dottrina, sul punto, v. *inter alios*: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 42; S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, in *World Trade Review*, Luglio 2018, Volume 17, Numero 3, pp. 477-508, spec. p. 492 ss.; S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 209 ss..

come soprattutto si vedrà in seguito, possano esistere delle criticità legate sia alla semplice presenza nell'Intesa di una disposizione come l'art. B.8, che alla concreta formulazione di tale articolo, nonché possibili difficoltà di coordinamento tra lo stesso e la disciplina UE in materia di dati personali.

Prima di proseguire nella trattazione, si coglie l'occasione per precisare anche un'altra circostanza. L'articolo appena esaminato concerne i flussi di dati in un ambito specifico, ovvero quello dei servizi finanziari. Si vedrà in seguito come pure altre delle previsioni che verranno analizzate nel proseguo concernano proprio i trasferimenti di informazioni nel medesimo contesto. Ciò, tuttavia, non deve sorprendere. Il settore dei servizi finanziari è, da un lato, uno dei più rilevanti per l'economia digitale [7]; dall'altro, è anche uno di quelli che presenta maggiori problematicità: alcuni sondaggi dimostrano che il pubblico è particolarmente preoccupato dal trattamento dei dati personali di natura finanziaria; molte persone hanno la percezione del fatto che le transazioni finanziarie col tempo stiano diventando sempre più tracciabili e tendono a ritenere che la protezione delle informazioni riservate e la sicurezza delle transazioni non siano garantite a sufficienza [8].

1.2. *L'«*Annex on Telecommunications»

Merita di essere preso in considerazione anche un altro strumento multilaterale facente parte del *corpus* normativo dell'OMC, ovverosia l'Allegato sulle telecomunicazioni o «*Annex on Telecommunications*»; a differenza dell'Intesa, che ha una collocazione autonoma, l'*Annex* rientra a tutti gli effetti tra gli allegati del GATS [9]. Il suo obiettivo è esplicitato all'art. 1, in base a cui, alla luce della specificità del settore delle telecomunicazioni, i membri hanno voluto approfondire le disposizioni dell'Accordo generale sugli scambi di servizi per quanto concerne le misure riguardanti l'accesso a reti e servizi pubblici di trasporto di telecomunicazioni e il loro utilizzo; pertanto l'Allegato contiene note e disposizioni aggiuntive rispetto al GATS [10].

L'art. 3 chiarisce poi che con «telecomunicazioni» si intende la trasmissione e la ricezione di segnali attraverso mezzi elettromagnetici [11]; la medesima disposizione definisce pure altre rilevanti nozioni, quali quelle di «servizi pubblici

---

[7] Sul punto v.: M. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, in *University of California Davis Law Review*, 2017, Volume 51, pp. 65-132, spec. p. 83.

[8] A. Sousa De Jesus, *Data Protection in EU Financial Services*, ECRI Research Report No. 6, April 2004, spec. p. 4.

[9] WTO, *General Agreement on Trade in Services*, cit., *Annex on Telecommunications*.

[10] WTO, *General Agreement on Trade in Services*, cit., *Annex on Telecommunications*, art. 1 («*Objectives*»).

[11] *Ibid*., art. 3 («*Definitions*»), lett. a).

di trasporto di telecomunicazioni» [12] e di «reti pubbliche di trasporto di telecomunicazioni» [13].

Si tratta di un ambito per cui valgono considerazioni indubbiamente simili a quelle svolte poc'anzi per i servizi finanziari: quello delle telecomunicazioni è uno dei settori più significativi per l'economia digitale [14], in cui i dati vengono utilizzati in modo intensivo [15]; ma proprio per questo solleva anche importanti esigenze di tutela.

Giungendo quindi alle disposizioni dell'*Annex* più rilevanti ai fini della presente trattazione, esse sono senz'altro le lettere c) e d) dell'art. 5, in cui è possibile riscontrare una struttura simile a quella della previsione precedentemente analizzata. Da un lato, la lettera c) dell'art. 5 obbliga i membri ad assicurare che i fornitori di servizi di qualsiasi altro membro possano utilizzare le reti e i servizi pubblici di trasporto di telecomunicazioni per la circolazione di informazioni a livello nazionale e oltre confine, nonché per l'accesso a informazioni contenute in *database* o comunque conservate in forma leggibile dalla macchina. Dall'altro lato, la lettera d) contiene una clausola di deroga finalizzata a controbilanciare l'impegno appena descritto: un membro può infatti adottare le misure necessarie al fine di garantire la sicurezza e la riservatezza dei messaggi, fermo restando l'obbligo di non applicare tali misure secondo modalità che costituirebbero un mezzo di discriminazione arbitraria o ingiustificata, ovvero una restrizione dissimulata allo scambio di servizi [16].

Le problematiche che ne derivano sono simili a quelle sommariamente anticipate in relazione all'*Understanding on Commitments in Financial Services*, che verranno meglio analizzate più avanti.

---

[12] *Ibid.*, lett. b).

[13] *Ibid.*, lett. c).

[14] Sul punto v.: M. BURRI, *op. cit.*, p. 83.

[15] Sul punto v., *inter alios*: E. VAN DER MAREL, *Disentangling the Flows of Data: Inside or Outside the Multinational Company?*, ECIPE OCCASIONAL PAPER No. 7, 2015, p. 2.

[16] WTO, *General Agreement on Trade in Services*, cit., *Annex on Telecommunications*, art. 5 («*Access to and use of Public Telecommunications Transport Networks and Services*»), lett. c) e lett. d). In dottrina, sul punto, v. *inter alios*: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 43; S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 492 ss.; S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 209 ss.

2. *Gli impegni al trasferimento di dati contenuti in accordi bilaterali di natura (anche solo parzialmente) commerciale conclusi dall'UE con Stati terzi*

Si giunge a questo punto all'esame di previsioni sui flussi e sulla protezione dei dati personali che sono cronologicamente successive rispetto a quelle analizzate poc'anzi e che sono invece contenute in trattati di tipo bilaterale non facenti parte del diritto dell'OMC: ci si riferisce agli accordi di libero scambio, o *Free Trade Agreements* (FTA), e più in generale agli accordi bilaterali di natura (anche solo parzialmente) commerciale conclusi dall'Unione europea con Stati terzi.

Come noto, l'UE ha iniziato a fare un massiccio ricorso agli FTA nei primi anni del nuovo millennio, anche alla luce di difficoltà all'epoca emerse nell'ambito del sistema commerciale multilaterale[17]. Nel 2006, in un'importante Comunicazione dal titolo «Europa globale – Competere nel mondo – Un contributo alla strategia per la crescita e l'occupazione dell'UE»[18], la Commissione europea affermava che gli accordi di libero scambio potevano prendere le mosse dalle regole dell'OMC per andare oltre e procedere più celermente al fine di promuovere l'apertura e l'integrazione, affrontando tematiche che non erano ancora pronte per una discussione multilaterale: tra queste, gli investimenti, gli appalti pubblici, la concorrenza, altre questioni regolamentari e l'applicazione dei diritti di proprietà intellettuale, ma non solo[19].

Nel 2015, con la Comunicazione «Commercio per tutti – Verso una politica commerciale e di investimento più responsabile»[20], la stessa Commissione ha poi fatto un bilancio parziale di tale «ambizioso programma bilaterale», integrativo dell'impegno dell'Unione in seno all'OMC, che ha portato l'UE a concludere o iniziare a negoziare accordi bilaterali di libero scambio con partner commerciali

---

[17] Sul punto v., *inter alios*: S. Woolcock, *European Union policy towards Free Trade Agreements*, ECIPE WORKING PAPER No. 3, 2007; I. Bosse-Platière-C. Rapoport, *Negotiating and implementing EU free trade agreements in an uncertain environment*, in I. Bosse-Platière-C. Rapoport (a cura di), *The Conclusion and Implementation of EU Free Trade Agreements. Constitutional Challenges*, Edward Elgar Publishing, Cheltenham, 2019, pp. 1-21.

[18] UE, Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, *Europa globale – Competere nel mondo – Un contributo alla strategia per la crescita e l'occupazione dell'UE*, 4 ottobre 2006, COM/2006/0567 def..

[19] *Ibid*., § 4.2.ii. In dottrina, sul punto, v. *inter alios*: L. Pasquali, *Il contributo dell'accordo UE – Mercosur alla governance internazionale dell'ambiente*, in *Nomos*, Volume 20, Numero 3, 2020, pp. 179-200; L. Pasquali, *The EU-MERCOSUR Agreement as Source of Development of Specific Global Norms and Standards*, in C. García Segura-J. Ibáñez-P. Pareja (a cura di), *Actores Regionales y Normas Globales: la Unión Europea y los BRICS como Actores Normativos*, Tirant lo Blanch, Valencia, 2021, pp. 131-142.

[20] UE, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Commercio per tutti – Verso una politica commerciale e di investimento più responsabile*, 14 ottobre 2015, COM/2015/0497 final.

di tutti i continenti: se dieci anni prima gli FTA in vigore rappresentavano meno del 25% degli scambi dell'Unione, nel 2015 erano invece giunti a costituire più di un terzo del commercio dell'UE, e sarebbero arrivati fino a due terzi qualora tutti i negoziati in corso fossero terminati con successo [21].

L'agenda commerciale bilaterale dell'Unione europea è stata portata avanti anche in tempi più recenti, come ricordato sempre dalla Commissione nelle proprie numerose Relazioni sull'attuazione degli accordi commerciali [22]. Nella Relazione del 2024, ad esempio, viene descritta una rete di ben 42 accordi commerciali con 74 partner, gli scambi con i quali hanno rappresentato nel 2023 il 45,8% del commercio estero dell'UE (2.300 miliardi di euro) [23].

Fatta una simile premessa occorre chiarire che in questa sede, esattamente come quando si è passata in rassegna la normativa dell'OMC, rilevano in particolar modo le norme di tali accordi in materia di scambi di servizi: tra di esse non solo sono presenti alcuni degli obblighi chiave già esaminati parlando del GATS, come il trattamento nazionale, la clausola della nazione più favorita e l'accesso al mercato, ma in numerosi casi è anche possibile trovare dei veri e propri impegni al trasferimento oltrefrontiera di dati personali. Tali «*data flows commitments*», inseriti nei capitoli relativi ad alcuni dei settori più rilevanti per l'economia digitale (ad esempio, i servizi finanziari e quelli di telecomunicazione), sono accompagnati da previsioni finalizzate alla tutela della *privacy* e del diritto alla protezione dei dati personali, sulla falsariga di quanto già visto per l'*Understanding on Commitments in Financial Services* e per l'*Annex on Telecommunications*. E ovviamente, anche in riferimento a simili disposizioni, si pongono questioni analoghe a quelle già parzialmente anticipate, che verranno però approfondite nel proseguo. Per meglio comprendere di cosa si sta parlando, è

---

[21] *Ibid*., § 1.2.

[22] Sul punto v., *inter alia*: UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione degli accordi di libero scambio 1° gennaio 2018 – 31 dicembre 2018*, 14 ottobre 2019, COM/2019/455 final; UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione degli accordi commerciali dell'UE 1° gennaio 2019 – 31 dicembre 2019*, 12 novembre 2020, COM/2020/705 final; UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione e sull'applicazione degli accordi commerciali dell'UE*, 27 ottobre 2021, COM/2021/654 final; UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione e sull'applicazione degli accordi commerciali dell'UE*, 11 ottobre 2022, COM/2022/730 final; UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione e sull'applicazione degli accordi commerciali dell'UE*, 15 novembre 2023, COM/2023/740 final; UE, Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sull'attuazione e sull'applicazione della politica commerciale dell'UE*, 3 dicembre 2024, COM/2024/385 final.

[23] UE, Relazione della Commissione *sull'attuazione e sull'applicazione degli accordi commerciali dell'UE*, 3 dicembre 2024, cit. § I.1.

opportuno passare prima in rassegna alcuni dei principali accordi bilaterali di natura (anche solo parzialmente) commerciale di cui l'UE è parte, al fine di analizzare puntualmente le più significative tra le previsioni di tal genere.

Giova, preliminarmente, una premessa di carattere metodologico: nelle pagine che seguono, ci si focalizzerà sul CETA con il Canada (illustrato per primo per la sua importanza e notorietà); su alcuni accordi più risalenti, come quelli con Corea del Sud, Colombia-Perù-Ecuador, America Centrale e Ucraina; nonché su alcuni accordi successivi, come quelli con Giappone, Singapore e Vietnam. Lo studio di alcuni accordi ancor più recenti, come quelli con Nuova Zelanda e Regno Unito, nonché di alcune modifiche apportate agli accordi precedenti (in particolare, a quello con il Giappone), sarà invece demandato a una parte poco successiva della presente trattazione: tali strumenti contengono infatti disposizioni di tipologia sensibilmente differente, di cui si dirà meglio più avanti.

2.1. *Il* Comprehensive Economic and Trade Agreement *(CETA) con il Canada*

Innanzitutto, come anticipato, si prenderà in esame l'Accordo economico e commerciale globale o *Comprehensive Economic and Trade Agreement* tra l'Unione europea e i suoi Stati membri, da una parte, e il Canada, dall'altra parte, meglio conosciuto come CETA[24]. Si partirà da qui per la sua notevole rilevanza: molte delle riflessioni che verranno svolte a proposito del CETA risulteranno applicabili anche agli accordi che saranno presi in considerazione nel proseguo e non verranno quindi ripetute.

Al termine di un lungo *iter* di negoziazioni iniziato nel 2009, il *Comprehensive Economic and Trade Agreement* è stato ufficialmente siglato da UE e Canada in data 30 ottobre 2016, ed è poi entrato provvisoriamente in vigore il 21 settembre 2017[25]. Quanto al contenuto, le sue disposizioni sono suddivise in ben 30 Capi,

---

[24] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, 30 ottobre 2016, GU L 11, 14 gennaio 2017, pp. 23-1079.

[25] Come noto, la necessità di ricorrere all'applicazione provvisoria è una conseguenza della natura «mista» dell'accordo in questione, espressione che sta a significare che le materie in esso disciplinate rientrano in parte nella competenza dell'Unione e in parte in quella degli Stati membri. La soluzione adottata in questi casi, e avallata anche dalla giurisprudenza della Corte di giustizia, è quella di una partecipazione al trattato anche dei singoli Paesi dell'UE, che procedono a negoziarlo e ratificarlo congiuntamente alle istituzioni dell'Unione e conformemente alle rispettive procedure costituzionali (in dottrina, sugli accordi misti, v. *inter alios*: R. Adam-A. Tizzano, *Manuale di diritto dell'Unione europea. Quarta edizione*, Giappichelli, Torino, 2024, pp. 903-905). Ciò può comportare, tuttavia, una notevole dilazione dei tempi di entrata in vigore di un accordo internazionale: proprio per questo si fa uso dello strumento dell'entrata in vigore a titolo provvisorio. Esso è in grado di dare un'adeguata risposta alle esigenze politiche ed economiche di applicazione immediata degli accordi, senza violare le norme di diritto internazionale sulla conclusione dei trattati: tale possibilità è infatti contemplata tanto dall'art. 25 della Convenzione di Vienna sul diritto dei trattati del 1969, quanto dall'art. 218, par. 5, del TFUE.

e sono altresì presenti numerosi allegati [26]. Per semplificare, si può affermare che tale accordo si occupa di sette aspetti fondamentali, ovvero: lo scambio di merci; lo scambio di servizi; gli appalti pubblici; gli investimenti; la proprietà intellettuale; lo sviluppo sostenibile; le imprese più piccole [27].

Vi sono anche norme in materia di risoluzione delle controversie. Il Capo 29 dell'accordo si occupa di quelle che possono sorgere tra UE e Canada circa l'interpretazione e l'applicazione dell'accordo [28], stabilendo un procedimento al termine del quale può essere financo riconosciuto alla parte richiedente il diritto di sospendere gli obblighi o ricevere una compensazione [29].

All'interno del Capo 8 sugli «Investimenti» [30], e più precisamente nella Sezione F [31], sono invece collocate previsioni normative in materia di «Risoluzione delle controversie tra investitori e Stati in materia di investimenti». Esse contemplano la possibilità per gli investitori di una parte di avanzare ricorsi direttamente davanti a organismi internazionali istituiti *ad hoc* per ottenere il risarcimento dei danni subiti, a opera della parte presso cui hanno effettuato un investimento, per violazioni dell'accordo CETA: in questi casi, si utilizzano le espressioni [32] «procedura ISDS», ovvero «*Investor-State Dispute Settlement*» («risoluzione delle controversie investitore-Stato») [33], e «ICS», ovvero «*Investment Court System*» («sistema giurisdizionale per gli investimenti») [34]. Tale soluzione è stata fortemente contestata, poiché da alcuni ritenuta in contrasto con i trattati UE, e nel 2017 il Regno del Belgio ha domandato alla Corte di giustizia un parere sul punto [35]. Tuttavia la Corte, abbandonando la rigidità che aveva contraddi-

---

[26] Per una panoramica completa dei vari Capi e Allegati del CETA, si veda la pagina del sito della Commissione europea dedicata a «CETA capitolo per capitolo», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/canada/eu-canada-agreement/ceta-chapter-chapter_en?prefLang=it&etrans=it* (ultimo accesso in data 31 dicembre 2024).

[27] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «*CETA overview – The 7 main parts of the agreement*», consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/en/country-assets/tradoc_156056.pdf* (ultimo accesso in data 31 dicembre 2024).

[28] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., artt. 29.1-29.19.

[29] *Ibid*., art. 29.14 («Misure correttive temporanee in caso di mancata esecuzione»).

[30] *Ibid*., artt. 8.1-8.45.

[31] *Ibid*., artt. 8.18-8.45.

[32] Tali espressioni, a onor del vero, non sono perfettamente sinonimiche, ma non è questa la sede per occuparsene. In dottrina, sul punto, v. *inter alios*: A. Algostino, *ISDS (Investor-State Dispute Settlement), il cuore di tenebra della global economic governance e il costituzionalismo*, in *Costituzionalismo.it*, 2016, Numero 1, pp. 103-174, spec. p. 158, secondo cui, semplificando, l'ICS può essere ritenuto una particolare declinazione dell'ISDS.

[33] UE, Corte di giustizia, Parere del 30 aprile 2019, 1/17, ECLI:EU:C:2019:341, § 5.

[34] *Ibid*., § 8.

[35] Il Regno del Belgio, nello specifico, sosteneva l'incompatibilità della procedura ISDS con il principio della competenza esclusiva della Corte a fornire un'interpretazione definitiva del diritto

stinto la propria precedente giurisprudenza relativa a casi simili [36], nel Parere 1/17 dell'aprile 2019 ha concluso che il Capo 8, Sezione F, dell'Accordo CETA è «compatibile con il diritto primario dell'Unione» [37]. Una soluzione che, va evidenziato, è stata destinataria di innumerevoli critiche, sul piano tanto giuridico quanto politico: il Giudice di Lussemburgo, ad esempio, è stato accusato di aver dato il via libera a una serie di accordi «trita-norme», grazie ai quali le multinazionali «possono agire in giudizio nei confronti dei governi nazionali e della stessa UE, ogni qualvolta ritengano che una legislazione arrechi disturbo ai loro affari» [38]. Occorre però precisare che gli articoli del CETA dedicati alla risoluzione delle controversie tra investitori e Stati in materia di investimenti non formano oggetto di applicazione provvisoria [39]; nel momento in cui si scrive, dunque, la procedura ISDS non è in vigore.

Tornando alla disciplina di diritto materiale contenuta nel CETA, come anticipato, le norme che indubbiamente rilevano in misura maggiore ai fini della presente trattazione sono quelle dedicate agli scambi di servizi, la cui liberalizzazione è innanzitutto perseguita, come nel GATS, attraverso ben noti obblighi fondamentali quali il trattamento nazionale [40], la clausola della nazione più

UE, il cui rispetto sarebbe necessario per assicurare l'autonomia dell'ordinamento giuridico dell'Unione (sul punto v. UE, Corte di giustizia, Parere 1/17, cit., §§ 46-47). Il Belgio si è così rivolto alla Corte di giustizia con una domanda di parere *ex* art. 218, par. 11, TFUE, in base a cui: «[…] 11. Uno Stato membro, il Parlamento europeo, il Consiglio o la Commissione possono domandare il parere della Corte di giustizia circa la compatibilità di un accordo previsto con i trattati. In caso di parere negativo della Corte, l'accordo previsto non può entrare in vigore, salvo modifiche dello stesso o revisione dei trattati».

[36] In particolare v.: UE, Corte di giustizia, sentenza del 6 marzo 2018, C-284/16, *Slowakische Republik contro Achmea BV*, ECLI:EU:C:2018:158.

[37] UE, Corte di giustizia, Parere 1/17, cit., § 245. La conclusione della Corte è motivata dal fatto che il Tribunale CETA può ben avere la competenza a interpretare e applicare le disposizioni dell'accordo alla luce delle norme e dei principi di diritto internazionale applicabili tra le parti; non potrebbe invece interpretare o applicare le disposizioni del diritto dell'Unione diverse da quelle del CETA, ma tale circostanza non si verifica (UE, Corte di giustizia, Parere 1/17, cit., § 118). Infatti, il Tribunale può solo, entro certi margini, interpretare incidentalmente il diritto UE o comunque tenerne conto, ma non in modo definitivo: è dunque salvo il principio della competenza esclusiva del Giudice di Lussemburgo a fornire un'interpretazione definitiva di tale diritto. In dottrina, sul punto, v. *inter alios*: P. Mengozzi, *Il parere 1/17 della Corte di giustizia UE sul Trattato CETA e il principio di autonomia del diritto UE*, in *Studi sull'integrazione europea*, 2020, Volume XV, Numero 2, pp. 323-338.

[38] D. Dongo-S. Bergamini, *CETA, via libera della Corte di Giustizia al 'trita-norme' a servizio delle 'Corporation'*, in *Greatitalianfoodtrade.it*, 6 maggio 2019.

[39] UE, Decisione (UE) 2017/38 del Consiglio *relativa all'applicazione provvisoria dell'accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, 28 ottobre 2016, GU L 11, 14 gennaio 2017, pp. 1080-1081, art. 1, par. 1, lett. a).

[40] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 9.3 («Trattamento nazionale»).

favorita [41], l'accesso al mercato [42]. Ancor più nello specifico, però, interessano le norme sui «Servizi finanziari», a cui è dedicato il Capo 13 [43], nonché quelle sulle «Telecomunicazioni», a cui è dedicato il Capo 15 [44]. È proprio qui che troviamo disposizioni simili a quelle precedentemente incontrate nell'*Understanding* e nell'*Annex*, in cui da un lato ci si impegna ad assicurare il libero flusso delle informazioni, mentre dall'altro si predispongono garanzie a protezione dei dati personali. Il tutto, però, non senza che ne derivino alcune criticità.

Prendendo le mosse dal Capo 13 del CETA, riguardante i «Servizi finanziari» [45], esso ha la funzione di consentire agli enti finanziari e agli investitori

---

[41] *Ibid*., art. 9.5 («Trattamento della nazione più favorita»).

[42] *Ibid*., art. 9.6 («Accesso al mercato»).

[43] *Ibid*., artt. 13.1-13.21.

[44] *Ibid*., artt. 15.1-15.15.

[45] La nozione di «servizi finanziari» e altre importanti nozioni come quelle di «prestatore di servizi finanziari transfrontalieri di una parte», «prestazione transfrontaliera di servizi finanziari o scambi transfrontalieri di servizi finanziari» ed «ente finanziario», sono puntualmente definite dall'art. 13.1 («Definizioni») del CETA. In particolare, in base a tale disposizione: «Ai fini del presente capo si intende per: prestatore di servizi finanziari transfrontalieri di una parte, qualunque persona di una parte che presta servizi finanziari nel territorio di tale parte e che presta o intende prestare servizi finanziari a livello transfrontaliero; prestazione transfrontaliera di servizi finanziari o scambi transfrontalieri di servizi finanziari, la prestazione di servizi finanziari: a) dal territorio di una parte nel territorio dell'altra parte; oppure b) nel territorio di una parte ad opera di una persona di tale parte a una persona dell'altra parte; ma non comprende la prestazione di servizi nel territorio di una parte ad opera di un investimento in tale territorio; ente finanziario, un prestatore che svolge una o più operazioni definite come servizi finanziari nel presente articolo, qualora il prestatore sia regolamentato o soggetto a supervisione in relazione alla prestazione di tali servizi in qualità di ente finanziario a norma della legislazione della parte nel cui territorio è situato, comprese le succursali situate nel territorio della parte facenti capo a tale prestatore di servizi finanziari avente la propria sede nel territorio dell'altra parte; […] servizio finanziario, qualunque servizio di carattere finanziario, compresi i servizi assicurativi e connessi, i servizi bancari e altri servizi finanziari (esclusa l'assicurazione), nonché i servizi ausiliari e accessori a un servizio di carattere finanziario. I servizi finanziari comprendono le seguenti attività: a) servizi assicurativi e connessi: i) assicurazione diretta (ivi compresa la coassicurazione): A) ramo vita; oppure B) ramo danni; ii) riassicurazione e retrocessione; iii) intermediazione assicurativa (ad esempio attività di broker e di agenzia); oppure iv) servizi accessori del settore assicurativo, quali consulenza, calcolo attuariale, valutazione del rischio e liquidazione sinistri; e b) servizi bancari e altri servizi finanziari (esclusa l'assicurazione): i) accettazione dal pubblico di depositi e altri fondi rimborsabili; ii) prestiti di qualsiasi tipo, ivi compresi crediti al consumo, crediti ipotecari, factoring e finanziamenti di operazioni commerciali; iii) leasing finanziario; iv) tutti i servizi relativi ai pagamenti e ai trasferimenti di denaro, compresi carte di credito, di addebito e di prelievo, traveller's cheques e bonifici bancari; v) garanzie e impegni; vi) operazioni per conto proprio o per conto della clientela in borsa, sul mercato ristretto o altrove, relative a: A) strumenti del mercato monetario (ivi compresi assegni, cambiali o certificati di deposito); B) valuta estera; C) prodotti derivati, ivi compresi contratti a termine e opzioni; D) strumenti relativi a tassi di cambio e d'interesse, inclusi swap e contratti a termine del tipo forward rate agreement; E) valori mobiliari; oppure F) altri strumenti negoziabili e altre attività finanziarie, compresi i lingotti; vii) partecipazione all'emissione di qualsiasi genere di titoli, compresi la sottoscrizione e il collocamento in qualità di agente (in forma pubblica o privata) nonché la prestazione di servizi

dell'UE e del Canada di beneficiare di condizioni di accesso eque e paritarie ai rispettivi mercati, applicando però disposizioni conformi alle norme prudenziali e regolamentari in vigore nell'UE e nel Canada [46]. Qui è possibile trovare una previsione di indiscutibile interesse ai nostri fini: si tratta dell'art. 13.15, dedicato a «Trasmissione e trattamento di informazioni». Ai sensi del par. 1, ciascuna parte autorizza gli enti finanziari o i prestatori di servizi finanziari transfrontalieri dell'altra parte a trasmettere informazioni, in entrata e in uscita dal suo territorio, ai fini del loro trattamento, se quest'ultimo è necessario per il normale esercizio dell'attività dei suddetti enti o prestatori: siamo dunque in presenza di un vero e proprio *data flows commitment*, attraverso il quale ciascuna parte si obbliga a consentire il flusso di determinate informazioni verso l'altra. Il par. 2 ha invece la funzione di controbilanciare tale impegno: si prevede infatti che ciascuna parte mantenga in vigore le opportune misure di salvaguardia a tutela della vita privata (nella versione Inglese: «*Each Party shall maintain adequate safeguards to protect privacy*»), in particolare in relazione alla trasmissione dei dati personali; si aggiunge inoltre che, là dove si trasferiscano oltrefrontiera dati personali, tale flusso deve avvenire ai sensi della pertinente normativa della parte da cui esso ha avuto origine [47].

Si può ora passare al Capo 15, dedicato alle «Telecomunicazioni» [48], nel quale

---

connessi; viii) servizi di intermediazione nel mercato monetario; ix) gestione patrimoniale, ad esempio gestione di cassa o di portafoglio, tutte le forme di gestione di investimenti collettivi, fondi pensione, servizi di custodia, di deposito e amministrazione fiduciaria; x) servizi di liquidazione e compensazione relativi ad attività finanziarie, ivi compresi titoli, prodotti derivati e altri strumenti negoziabili; xi) fornitura e trasmissione di informazioni finanziarie, nonché elaborazione di dati finanziari e relativo software; oppure xii) servizi finanziari di consulenza, intermediazione e altri servizi finanziari accessori, relativi a tutte le attività elencate ai precedenti punti da i) a xi), ivi comprese referenze bancarie e informazioni commerciali, ricerche e consulenze in merito a investimenti e portafogli e consulenze su acquisizioni, ristrutturazioni e strategie aziendali […]».

[46] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «CETA capitolo per capitolo», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/canada/eu-canada-agreement/ceta-chapter-chapter_en?prefLang=it&etrans=it* (ultimo accesso in data 31 dicembre 2024). In dottrina, v. *inter alios*: L. Mulas, *Il Comprehensive Economic and Trade Agreement (CETA): tra liberalizzazione e regolamentazione prudenziale*, in *Diritto comunitario e degli scambi internazionali*, 2020, Numero 2, pp. 415-449, spec. p. 419.

[47] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 13.15 («Trasmissione e trattamento di informazioni»). In dottrina, sul punto, v. *inter alios*: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 43; S. Yakovleva-K. Irion, *Pitching trade against privacy*, cit., p. 214.

[48] La nozione di «servizi di telecomunicazioni» e altre importanti nozioni come quelle di «rete pubblica di trasporto di telecomunicazioni» e di «servizio pubblico di trasporto di telecomunicazioni», sono puntualmente definite dall'art. 15.1 («Definizioni») del CETA. In particolare, in base a tale disposizione: «Ai fini del presente capo si intende per: […] rete pubblica di trasporto di telecomunicazioni, le infrastrutture pubbliche di telecomunicazioni che rendono possibili le telecomunicazioni tra punti terminali definiti di una rete; servizio pubblico di trasporto di teleco-

UE e Canada si impegnano a dare alle imprese della controparte condizioni di accesso eque e non discriminatorie alle reti e ai servizi di telecomunicazioni, nonché a garantire la concorrenza nel mercato in questione, pur sempre nel rispetto di alcuni diritti dei clienti[49]. In tale sede, la disposizione che assume il maggior rilievo ai fini della presente trattazione è l'art. 15.3, segnatamente i suoi paragrafi 3 e 4. Ancora una volta, il primo dei due paragrafi citati (il par. 3) contiene un *data flows commitment*, dal momento che obbliga sia il Canada che l'UE ad assicurare che le imprese dell'altra parte possano utilizzare le reti e i servizi pubblici di trasporto di telecomunicazioni per trasmettere informazioni non solo nel proprio territorio, ma anche oltre i propri confini. L'altro paragrafo (il par. 4) è invece finalizzato a controbilanciare tale disposizione: si prevede infatti che le parti adottino, in deroga al paragrafo 3, misure appropriate per tutelare «la sicurezza e la riservatezza», nonché la «vita privata» (nella versione Inglese, «*privacy*») degli utenti[50].

Sul punto, occorre però fare due precisazioni: innanzitutto, questo avviene «in applicazione dell'articolo 28.3» del CETA, disposizione inserita nel Capo 28 sulle «Eccezioni» e dedicata in particolare alle «Eccezioni generali»: ancor più nello specifico, il suo par. 2 riporta un contenuto assai simile a quello del già esaminato art. XIV del GATS in materia di «*General Exceptions*» e consente quindi di giustificare alcune misure che *prima facie* rappresenterebbero una violazione di determinate norme dell'accordo CETA, purché ricorrano le condizioni che sono già state esaminate parlando per l'appunto del GATS[51]. In secondo luogo, lo stesso art. 15.3, par. 4, del CETA sancisce l'obbligo di non applicare le misure a tutela di sicurezza, riservatezza, vita privata in un modo che rappresenti una «discriminazione arbitraria o ingiustificata» oppure una «restrizione dissimulata agli scambi»[52].

---

municazioni, qualunque servizio di trasporto di telecomunicazioni che una parte, espressamente o di fatto, richiede sia offerto al pubblico in generale, e che comporti la trasmissione in tempo reale di informazioni fornite dal cliente tra due o più punti senza che intervengano cambiamenti nella forma o nel contenuto dell'informazione del cliente da un punto all'altro. Tale servizio può comprendere, tra l'altro, i servizi di telefonia vocale, i servizi di trasmissione dati a commutazione di pacchetto, i servizi di trasmissione dati a commutazione di circuito, i servizi di telex, i servizi telegrafici, i servizi di fax, i servizi relativi a circuiti privati affittati e i servizi e sistemi di comunicazione mobile e personale; […] servizi di telecomunicazioni, tutti i servizi relativi alla trasmissione e alla ricezione di segnali con mezzi elettromagnetici, esclusa l'attività economica consistente nella fornitura di contenuti per mezzo di telecomunicazioni […]».

[49] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «CETA capitolo per capitolo», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/canada/eu-canada-agreement/ceta-chapter-chapter_en?prefLang=it&etrans=it* (ultimo accesso in data 31 dicembre 2024).

[50] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 15.3 («Accesso a reti o servizi pubblici di trasporto di telecomunicazioni e relativo uso»).

[51] *Ibid*., art. 28.3 («Eccezioni generali»).

[52] Sull'art. 15.3 del CETA v., *inter alios*: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., pp. 43-44. S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 493.

Si tornerà a breve su disposizioni come l'art. 13.15 e l'art. 15.3 del CETA: si metteranno in risalto le somiglianze, ma anche le differenze, rispetto alle previsioni in materia di dati contenute in strumenti più risalenti, come l'*Understanding on Commitments in Financial Services* e l'*Annex on Telecommunications* del GATS. Ci si chiederà inoltre se le problematiche che caratterizzano le une siano proprie anche delle altre. Questo tuttavia non prima di aver esaminato, a titolo esemplificativo e senza alcuna pretesa di esaustività, anche altri accordi commerciali conclusi dall'Unione europea, al fine di riscontrare se anche in questi siano presenti disposizioni analoghe a quelle appena trattate. Per essi, come già accennato, valgono molte delle considerazioni già svolte per il CETA, che non verranno dunque replicate.

2.2. *Alcuni accordi meno recenti: l'Accordo di libero scambio con la Corea del Sud e l'Accordo commerciale con Colombia, Perù ed Ecuador*

Per prima cosa, si analizzeranno le previsioni che incidono sui flussi di dati personali e sulla protezione degli stessi in due accordi, di natura prettamente commerciale, meno recenti rispetto al CETA. Il primo è il *Free Trade Agreement* tra l'UE e i suoi Stati membri, da una parte, e la Corea del Sud, dall'altra parte (talvolta detto «EUKOR»)[53], firmato il 6 ottobre 2010, divenuto provvisoriamente applicabile dal 1° luglio 2011 ed entrato formalmente in vigore il 13 dicembre 2015[54]. Il secondo è l'Accordo commerciale tra l'UE e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra parte[55], firmato in data 26 giugno 2012 ed entrato in vigore in via provvisoria con il Perù dal 1° marzo 2013, con la Colombia dal 1° agosto 2013, nonché con l'Ecuador – che nel 2016 ha aderito a tale strumento[56] – dal 1° gennaio 2017; tale Accordo è poi entrato definitivamente in vigore in data 1° novembre 2024[57].

---

[53] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, 6 ottobre 2010, GU L 127, 14 maggio 2011, pp. 6-1343.

[54] Per una panoramica del contenuto dell'accordo di libero scambio tra UE e Corea del Sud, si veda la pagina del sito della Commissione europea dedicata a «*EU-South Korea Free Trade Agreement – A Quick Reading Guide*», consultabile al seguente link: *https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/871d9750-97a7-412f-a52a-fbf92422cafe/details* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – South Korea*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/south-korea/* (ultimo accesso in data 31 dicembre 2024).

[55] UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, 26 giugno 2012, GU L 354, 21 dicembre 2012, pp. 3-2607.

[56] UE, *Protocollo di adesione dell'accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra, per tener conto dell'adesione dell'Ecuador*, 11 novembre 2016, GU L 356, 24 dicembre 2016, pp. 3-1456.

[57] Per una panoramica del contenuto dell'Accordo commerciale con Colombia, Perù ed Ecuador si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile

I due accordi vanno a disciplinare varie materie già menzionate in riferimento al CETA [58] e contengono anch'essi meccanismi per la «Risoluzione delle controversie» tra le parti circa l'interpretazione e l'applicazione dei due accordi, che possono portare parte attrice a ricevere un indennizzo o sospendere i propri obblighi [59].

Per entrambi gli accordi, tuttavia, interessano in questa sede specialmente le disposizioni in materia di servizi [60], tra cui figurano non solo i già conosciuti obblighi chiave [61], ma anche, in ciascuno dei due strumenti, una disposizione sul «Trattamento dei dati» nell'ambito dei «Servizi finanziari»: si tratta per l'EUKOR dell'art. 7.43 [62], mentre per l'accordo con Colombia, Perù ed Ecuador dell'art. 157 [63].

Esse si presentano come due disposizioni estremamente simili tra di loro (con una struttura piuttosto vicina a quella dell'art 13.15 del CETA). In entrambi i

---

al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/accordo-commerciale-ue-colombia-peru-ecuador* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Andean Community*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/regions/andean-community/* (ultimo accesso in data 31 dicembre 2024); sull'entrata in vigore dell'accordo, si veda invece la pagina del sito del Consiglio europeo e del Consiglio dell'Unione europea dedicata a «*EU-Andean Countries: Council greenlights the conclusion of the trade agreement with Colombia, Peru and Ecuador*», consultabile al seguente link: *https://www.consilium.europa.eu/en/press/press-releases/2024/10/14/eu-andean-countries-council-greenlights-the-conclusion-of-the-trade-agreement-with-colombia-peru-and-ecuador/#:~:text=The%20Trade%20Agreement%20with%20Colombia%20and%20Peru%2C%20and%20the%20referred,force%20on%201%20November%202024* (ultimo accesso in data 31 dicembre 2024).

[58] L'accordo con la Corea del Sud e l'accordo con Colombia, Perù ed Ecuador, composti rispettivamente di 15 Capi e 14 Titoli, disciplinano infatti materie come lo scambio di merci, lo scambio di servizi, gli appalti pubblici, la proprietà intellettuale, lo sviluppo sostenibile.

[59] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., Capo 14 («Risoluzione delle controversie»), i.e. artt. 14.1-14.20; UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., Titolo XII («Risoluzione delle controversie»), i.e. artt. 298-323.

[60] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., Capo 7 («Commercio di servizi, stabilimento e commercio elettronico»), i.e. artt. 7.1-7.50; UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., Titolo IV («Scambi di servizi, stabilimento e commercio elettronico»), i.e. artt. 107-167.

[61] Per l'accesso al mercato v.: UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.5; UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., art. 119. Per il trattamento nazionale v.: UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.6; UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., art. 120. Per il trattamento della nazione più favorita v.: UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.8.

[62] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.43 («Trattamento dei dati»).

[63] UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., art. 157 («Trattamento dei dati»).

casi, da un lato, è sancito un impegno al trasferimento dei dati nel settore dei servizi finanziari: in tale ambito, ciascuna parte si obbliga a consentire il flusso di determinate informazioni verso l'altra [64]. Dall'altro lato si cerca di controbilanciare tale *data flows commitment* [65]: ciascuna parte, infatti, adotta le opportune misure di salvaguardia (nelle versioni inglesi dei due accordi, «*adequate safeguards*») a tutela della vita privata («*privacy*»), in particolare in relazione al trasferimento dei dati personali [66]. Tuttavia, diversamente da come avviene nel CETA (che, lo si ripete, è successivo), gli articoli nell'EUKOR e nell'accordo con Colombia-Perù-Ecuador non prevedono che, là dove si trasmettano oltrefrontiera dati personali, tale flusso debba avvenire ai sensi della pertinente normativa della parte da cui esso ha avuto origine.

2.3. *Alcuni accordi meno recenti: gli Accordi di Associazione con l'America centrale e con l'Ucraina* (segue)

Si vuole ora riscontrare la presenza di disposizioni simili a quelle poc'anzi esaminate anche in una specifica categoria di accordi: quella degli «Accordi di associazione» [67]. In particolare, se ne prenderanno in considerazione due

---

[64] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.43, lett. a); UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., art. 157, par. 1.

[65] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.43, lett. b); UE, *Accordo commerciale tra l'Unione europea e i suoi Stati membri, da una parte, e la Colombia e il Perù, dall'altra*, cit., art. 157, par. 2.

[66] Sull'art. 7.43 dell'Accordo di libero scambio tra UE e Corea del Sud v., *inter alios*: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 494; F. VELLI, *op. cit.*, p. 890; Sull'art. 157 dell'Accordo commerciale dell'UE con Colombia, Perù ed Ecuador v., *inter alios*: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 494.

[67] La possibilità per l'UE di concludere Accordi di associazione è prevista dall'art. 217 TFUE. Comprendere nei dettagli l'effettiva identità di tale categoria di accordi non è però particolarmente agevole. Le «azioni in comune» e le «procedure particolari» a cui fa riferimento l'art. 217 TFUE sono effettivamente riscontrabili negli accordi di associazione finora conclusi dall'UE: si possono infatti trovare organi paritetici, sotto il nome di «Consigli di associazione», che hanno il compito di assicurare, spesso con l'ausilio di altri organi sussidiari come i «Comitati di associazione», la corretta gestione dell'accordo e un quadro di consultazione tra le parti contraenti; essi sono presenti pure nell'accordo con l'America centrale (rispettivamente, articoli 4 e 7) e in quello con l'Ucraina (rispettivamente, articoli 461 e 464). Tuttavia, anche una gran parte degli accordi commerciali dell'Unione prevede forme più o meno ampie di istituzionalizzazione: l'elemento che differenzia gli Accordi di associazione da tutti gli altri trattati dell'UE deve dunque essere cercato altrove. Esso non può neppure essere rappresentato dall'ampiezza dei contenuti che tali accordi possono assumere: sebbene sia vero che spesso simili strumenti vanno a disciplinare molteplici settori, è anche vero che sono altresì configurabili pure Accordi di associazione caratterizzati da una dimensione quasi esclusivamente commerciale; la struttura e i contenuti possono dunque

(anch'essi antecedenti rispetto al CETA). Il primo è quello tra l'UE e i suoi Stati membri, da una parte, e l'America centrale, dall'altra [68], firmato il 29 giugno 2012 e – dopo una lunga fase in cui parte dello stesso è stata applicata provvisoriamente [69] – entrato in vigore nel 2024 (si ricorda che la nozione di «America centrale» ricomprende le Repubbliche di Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua e Panama) [70]. Il secondo è quello tra l'UE e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra [71], firmato nel 2014 e (anche in questo caso dopo un periodo in cui parte del medesimo ha trovato applicazione provvisoria) entrato definitivamente in vigore il 1° settembre 2017 [72].

Come noto, gli accordi di tal genere concretamente conclusi dall'UE sono solitamente contraddistinti dalla presenza di organi paritetici che producono

---

essere variabili. In definitiva, per trovare l'elemento caratteristico degli Accordi di associazione è forse più opportuno porre l'accento sulle loro finalità, come del resto ha fatto anche la Corte di giustizia: essi, infatti, hanno lo scopo di creare «vincoli particolari e privilegiati con uno Stato terzo il quale deve, almeno in parte, partecipare al regime comunitario» (in particolare v.: UE, Corte di giustizia, sentenza del 30 settembre 1987, 12/86, *Meryem Demirel contro Comune di Schwäbisch Gmünd*, ECLI:EU:C:1987:400). Ciò che rileva maggiormente, dunque, è il tipo di rapporto che l'Unione stabilisce con la controparte e non l'atto giuridico per mezzo del quale esso è posto in essere. In dottrina, in tal senso, v.: R. ADAM-A. TIZZANO, *op. cit.*, pp. 898-900.

[68] UE, *Accordo che istituisce un'associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'America centrale, dall'altra*, 29 giugno 2012, GU L 346, 15 dicembre 2012, pp. 3-2621.

[69] Ai sensi dell'art. 353 («Entrata in vigore»), par. 4, dell'Accordo che istituisce un'associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'America centrale, dall'altra, la sua Parte IV («Commercio») è stata applicata in via provvisoria dal 1° agosto 2013 con Honduras, Nicaragua e Panama, dal 1° ottobre 2013 con Costa Rica ed El Salvador e dal 1° dicembre 2013 con il Guatemala.

[70] Per una panoramica del contenuto dell'Accordo di associazione tra l'UE e i suoi Stati membri, da una parte, e l'America centrale, dall'altra parte, si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/accordo-di-associazione-ue-america-centrale* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Central America*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/regions/central-america/* (ultimo accesso in data 31 dicembre 2024); sull'entrata in vigore dell'accordo, si veda invece la pagina del sito dell'EEAS dedicata a «*EU-Central America agreement enters into force*», consultabile al seguente link: *https://www.eeas.europa.eu/delegations/guatemala/eu-central-america-agreement-enters-force_en?s=187* (ultimo accesso in data 31 dicembre 2024).

[71] UE, *Accordo di associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra*, 21 marzo e 27 giugno 2014, GU L 161, 29 maggio 2014, pp. 3-2137.

[72] Per una panoramica del contenuto dell'Accordo di associazione tra l'UE e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra parte, si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/zona-di-libero-scambio-globale-e-approfondita-ue-ucraina* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Ukraine*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/ukraine/* (ultimo accesso in data 31 dicembre 2024).

atti, nonché da una notevole estensione delle materie in essi trattate, che hanno carattere non solo commerciale, ma anche politico [73]. Simili caratteristiche possono essere rinvenute in entrambi gli accordi che ci si propone qui di analizzare, soprattutto nell'Accordo di associazione con l'Ucraina: esso è infatti funzionale ad avvicinare progressivamente tale Stato all'Unione europea, promuovendo legami politici più profondi, vincoli economici più forti, nonché il rispetto di valori comuni; tutto ciò, sia ai fini della Politica europea di vicinato (PEV) [74], che nella prospettiva di una possibile futura ammissione dell'Ucraina all'UE [75].

I due accordi vanno dunque a disciplinare un novero di materie ben più ampio rispetto ai trattati di natura esclusivamente commerciale [76]. Ai nostri fini, tuttavia, è necessario addentrarsi ancora una volta tra le norme in tema di commercio (che peraltro, nell'accordo con l'America centrale, sono state per oltre un decennio le uniche in vigore, in quanto oggetto di applicazione provvisoria) [77]. Tali norme regolamentano i settori tipici dei trattati commerciali [78], tra cui gli scambi di servizi.

In riferimento a quest'ultimo ambito, oltre ai noti obblighi chiave [79], sono

---

[73] Sul punto v., *inter alios*: A. Converti, *Istituzioni di diritto dell'Unione europea*, Halley, Macerata, 2003, pp. 361-364.

[74] Sulla Politica europea di vicinato (PEV), si veda la pagina del sito del Parlamento europeo ad essa dedicata, consultabile al seguente link: *https://www.europarl.europa.eu/factsheets/it/sheet/170/politica-europea-di-vicinato* (ultimo accesso in data 31 dicembre 2024).

[75] Sul punto v., *inter alios*: M. Evola, *The EU-Ukraine Association Agreement between the European Neighbourhood Policy and admission*, in *Il Diritto dell'Unione europea*, 2015, Numero 1, pp. 199-236.

[76] L'Accordo di associazione con l'America centrale è costruito su tre pilastri: quello del «Dialogo politico» (Parte II, i.e. artt. 12-23), fondato sulla democrazia, lo Stato di diritto e i diritti umani (v. art. 13, par. 2); quello della «Cooperazione» (Parte III, i.e. artt. 24-76), il cui obiettivo è sostenere l'attuazione dell'accordo in modo da realizzare un partenariato efficace tra le due regioni facilitando l'accesso a risorse, meccanismi, strumenti e procedure (v. art. 24, par. 1); e infine quello del «Commercio» (Parte IV, i.e. artt. 77-351). L'Accordo di associazione con l'Ucraina contiene invece norme sulle seguenti materie: «Dialogo politico e riforme, associazione politica, cooperazione e convergenza in materia di politica estera e di sicurezza» (Titolo II, i.e. artt. 4-13); «Giustizia, libertà e sicurezza» (Titolo III, i.e. artt. 14-24); «Scambi e questioni commerciali» (Titolo IV, i.e. artt. 25-336); «Cooperazione economica e settoriale» (Titolo V, i.e. artt. 337-452); «Cooperazione finanziaria e disposizioni antifrode» (Titolo VI, i.e. artt. 453-459).

[77] UE, *Accordo che istituisce un'associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'America centrale, dall'altra*, cit., Parte IV («Commercio»), i.e. artt. 77-351; UE, *Accordo di associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra*, cit., Titolo IV («Scambi e questioni commerciali»), i.e. artt. 25-336.

[78] Negli Accordi di Associazione con l'America centrale e con l'Ucraina, le norme in materia commerciale regolamentano settori quali gli scambi di merci, gli scambi di servizi, gli appalti pubblici, la proprietà intellettuale, lo sviluppo sostenibile, nonché la risoluzione delle controversie tra le parti. Su quest'ultimo punto viene dettata una disciplina simile a quelle precedentemente prese in considerazione nella trattazione, la quale (giova precisarlo) è finalizzata a risolvere le controversie concernenti l'interpretazione o l'applicazione delle sole norme in materia commerciale.

[79] Per l'accesso al mercato v.: UE, *Accordo che istituisce un'associazione tra l'Unione europea*

dettate anche disposizioni dedicate al «Trattamento dei dati» nel settore dei servizi finanziari: per l'accordo con l'America centrale l'art. 198 [80] e per l'accordo con l'Ucraina l'art. 129 [81]. Essi risultano non solo assai simili all'art. 13.15 del CETA, ma soprattutto quasi perfettamente sovrapponibili ai corrispondenti articoli dell'EUKOR e dell'Accordo commerciale con Colombia, Perù ed Ecuador, alla cui trattazione si fa dunque integralmente rinvio [82].

La presenza di *data flows commitments*, accompagnati da previsioni a tutela dei dati personali e della *privacy*, è dunque riscontrabile non solo in trattati dell'UE di natura esclusivamente commerciale, ma pure in accordi aventi portata ben più ampia come gli Accordi di associazione (anche se, ovviamente, tali impegni sono sempre collocati tra gli articoli dedicati al commercio). Le disposizioni contenute negli accordi di tal genere, inoltre, risultano tra loro assai omogenee, nonostante siano profondamente differenti sia le controparti dell'Unione che il tipo di rapporto che si intende instaurare con le medesime (come si è detto, l'Accordo di associazione con l'Ucraina è pensato anche nell'ottica di un'eventuale ammissione della medesima all'UE, riflessione ovviamente non applicabile all'Accordo con gli Stati dell'America centrale).

2.4. *Alcuni accordi più recenti: l'*Economic Partnership Agreement *(EPA) con il Giappone*

Dopo aver preso in considerazione alcuni strumenti meno recenti (di natura esclusivamente o parzialmente commerciale) e aver rinvenuto in essi disposizioni incidenti sia sui flussi che sulla protezione dei dati personali, si tratta a questo punto di verificare se norme analoghe siano altresì rintracciabili nei più recenti accordi dell'Unione europea, successivi anche al CETA. La risposta, lo si anticipa, è affermativa: rispetto alla maggior parte delle previsioni esaminate finora, si potranno notare alcune differenze nella formulazione (mentre, lo si è visto, gli articoli contenuti nell'EUKOR, nell'accordo con Colombia-Perù-Ecuador, nell'accordo con l'America centrale e nell'accordo con l'Ucraina sono presso-

---

e i suoi Stati membri, da una parte, e l'America centrale, dall'altra, cit., art. 170; UE, *Accordo di associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra*, cit., art. 93. Per il trattamento nazionale v.: UE, *Accordo che istituisce un'associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'America centrale, dall'altra*, cit., art. 171; UE, *Accordo di associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra*, cit., art. 94.

[80] UE, *Accordo che istituisce un'associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'America centrale, dall'altra*, cit., art. 198 («Trattamento dei dati»).

[81] UE, *Accordo di associazione tra l'Unione europea e i suoi Stati membri, da una parte, e l'Ucraina, dall'altra*, cit., art. 129 («Trattamento dei dati»).

[82] Sull'art. 198 dell'Accordo di associazione tra UE e America centrale v., *inter alios*: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 494.

ché identici tra loro); nonostante ciò, tuttavia, si tratta della stessa tipologia di disposizioni, riguardanti i medesimi settori presi in considerazione fino a questo momento: in particolare, i servizi finanziari e i servizi di telecomunicazione.

Il primo che si prenderà in considerazione, fra tali trattati più recenti, è l'Accordo tra l'Unione europea e il Giappone per un partenariato economico, meglio noto come *Economic Partnership Agreement* (EPA) [83], firmato il 17 luglio 2018 ed entrato in vigore il 1° febbraio 2019 [84]. Esso disciplina vari settori, in gran parte coincidenti rispetto a quelli dei trattati commerciali finora presi in considerazione [85], tra cui ancora una volta i servizi. Nel relativo Capo, insieme alle consuete norme su accesso al mercato [86], trattamento nazionale [87] e trattamento della nazione più favorita [88], figurava originariamente anche l'art. 8.63, in materia di «Trasmissione e trattamento di informazioni» nell'ambito dei servizi finanziari. Al suo interno, da un lato, le parti si impegnavano a non impedire determinati flussi di informazioni nel settore dei servizi finanziari [89]; dall'altro, tale previsione veniva controbilanciata, ribadendo il diritto di UE e Giappone di proteggere i dati personali, la vita privata e la riservatezza, purché tale diritto non fosse utilizzato con la finalità di eludere certe disposizioni dell'accordo (tra cui, ad esempio, quelle sugli scambi transfrontalieri di servizi) [90]. Se dunque, come anticipato, la formulazione letterale dell'art. 8.63 differiva parzialmente da quella delle disposizioni degli accordi precedentemente analizzati, lo stesso non poteva dirsi della sua struttura, né della sua funzione [91]. Tuttavia, a onor del vero, nel momento in cui si scrive l'art. 8.63 non fa più parte dell'EPA: viene infatti integralmente rimosso dall'art. 5 del successivo accordo sui flussi tran-

[83] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, 17 luglio 2018, GU L 330, 27 dicembre 2018, pp. 3-899.

[84] Per una panoramica del contenuto dell'Accordo tra l'UE e il Giappone per un partenariato economico, si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/accordo-di-partenariato-economico-ue-giappone* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Japan*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/japan/* (ultimo accesso in data 31 dicembre 2024).

[85] Tra i principali settori disciplinati dall'EPA col Giappone figurano gli scambi di merci, gli scambi di servizi, la liberalizzazione degli investimenti, gli appalti pubblici, la proprietà intellettuale, lo sviluppo sostenibile, nonché la risoluzione delle controversie tra le parti su tali materie.

[86] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 8.15.

[87] *Ibid*., art. 8.16.

[88] *Ibid*., art. 8.17.

[89] *Ibid*., art. 8.63 («Trasmissione e trattamento di informazioni»), par. 1.

[90] *Ibid*., art. 8.63 («Trasmissione e trattamento di informazioni»), par. 2.

[91] Sul "vecchio" art. 8.63 dell'Accordo tra l'UE e il Giappone per un partenariato economico v., *inter alios*: M. Bartl-K. Irion, *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, University of Amsterdam, Amsterdam, 2017, pp. 4-5.

sfrontalieri di dati concluso tra UE e Giappone il 23 ottobre 2023 [92], di cui la Commissione europea ha annunciato l'entrata in vigore in data 1° luglio 2024 [93]. In luogo di tale articolo, figurano ora disposizioni che verranno prese in considerazione nel proseguo, poiché di tipologia assai differente.

Del testo originale dell'EPA, permane invece un altro articolo su cui si vuole portare l'attenzione, collocato sempre tra le norme dedicate ai servizi, ma in questo caso a quelli di telecomunicazione: si tratta dell'art. 8.44. In questo caso, il paragone può essere indubbiamente instaurato con l'art. 15.3 CETA, riguardante anch'esso i servizi di telecomunicazione. Infatti, da un lato, l'art. 8.44 dell'EPA contiene un impegno al trasferimento dei dati: sia il Giappone che l'UE sono infatti obbligati a garantire che i prestatori di servizi dell'altra parte possano utilizzare le reti e i servizi pubblici di trasporto di telecomunicazioni per la circolazione di informazioni non solo nel proprio territorio, ma anche oltre i propri confini [94]. Dall'altro lato, si può invece notare una previsione secondo cui le parti possono adottare le misure necessarie a garantire la sicurezza e la riservatezza; tuttavia, tali misure non devono essere applicate in una forma che costituisca una «discriminazione arbitraria o ingiustificata» o una «restrizione dissimulata» degli scambi [95], proprio come nel menzionato accordo col Canada [96]. L'art. 8.44 dell'EPA non ha subito alcuna abrogazione né modifica a opera del più recente accordo sui flussi transfrontalieri di dati tra UE e Giappone.

2.5. *Alcuni accordi più recenti: gli Accordi di libero scambio con la Repubblica di Singapore e con la Repubblica socialista del Vietnam* (segue)

Gli ultimi due accordi che verranno presi in considerazione, perlomeno in questa fase della trattazione, sono l'Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore [97], firmato il 19 ottobre 2018 ed entrato

---

[92] Sul punto, v. la pagina del sito della Commissione europea dedicata a «Dialogo economico ad alto livello UE-Giappone: storico accordo sui flussi transfrontalieri di dati», consultabile al seguente link: *https://ec.europa.eu/commission/presscorner/detail/it/ip_23_5378* (ultimo accesso in data 31 dicembre 2024).

[93] Sul punto, v. la pagina del sito della Commissione europea dedicata a «*EU-Japan deal on data flows enters into force*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/news/eu-japan-deal-data-flows-enters-force-2024-07-01_en* (ultimo accesso in data 31 dicembre 2024).

[94] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 8.44 («Accesso e uso»), par. 3.

[95] *Ibid*., art. 8.44 («Accesso e uso»), par. 4.

[96] Sull'art. 8.44 dell'Accordo tra l'UE e il Giappone per un partenariato economico v., *inter alios*: M. Bartl-K. Irion, *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, cit., pp. 5-6.

[97] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, 19 ottobre 2018, GU L 294, 14 novembre 2019, pp. 3-755.

in vigore il 21 novembre 2019 [98], e l'Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam [99], firmato il 30 giugno 2019 ed entrato in vigore il 1° agosto 2020 [100]. Entrambi si occupano di materie in gran parte coincidenti rispetto a quelle degli strumenti visti fin qui.

Ancora una volta, è opportuno evidenziare la presenza di disposizioni in materia di «Trattamento dei dati» nell'ambito dei servizi finanziari: l'art. 8.54 del FTA con Singapore [101] e l'art. 8.45 di quello col Vietnam [102]. Si tratta di articoli piuttosto simili a quelli riscontrati nei meno recenti accordi dell'UE visti fin qui: ci si riferisce quindi alle disposizioni contenute nell'EUKOR, nell'Accordo commerciale con Colombia-Perù-Ecuador, nell'Accordo di associazione con l'America centrale e in quello con l'Ucraina, alla cui trattazione si fa dunque rinvio. Vi sono però anche alcune variazioni nelle formulazioni, ad esempio il fatto che le «garanzie adeguate» a tutela della vita privata e dei dati personali – che servono a controbilanciare i *data flows commitments* – non devono però essere utilizzate per eludere gli accordi in questione [103]: da questo punto di vista, il paragone più immediato risulta essere dunque quello con il "vecchio" art. 8.63 dell'EPA con il Giappone [104].

Infine, passando ai servizi di telecomunicazione, entrambi gli accordi includono disposizioni simili a quelle del CETA e dell'EPA: da un lato, sono pre-

---

[98] Per una panoramica del contenuto dell'Accordo di libero scambio tra l'UE e la Repubblica di Singapore, si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/accordo-di-libero-scambio-ue-singapore* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Singapore*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/singapore/* (ultimo accesso in data 31 dicembre 2024).

[99] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, 30 giugno 2019, GU L 186, 12 giugno 2020, pp. 3-1400.

[100] Per una panoramica del contenuto dell'Accordo di libero scambio tra l'UE e il Vietnam, si veda la pagina del sito della Commissione europea ad esso dedicata, consultabile al seguente link: *https://trade.ec.europa.eu/access-to-markets/it/content/accordo-di-libero-scambio-ue-vietnam* (ultimo accesso in data 31 dicembre 2024); si veda anche la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Vietnam*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/* (ultimo accesso in data 31 dicembre 2024).

[101] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 8.54 («Trattamento dei dati»).

[102] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 8.45 («Trattamento dei dati»).

[103] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 8.54, par. 2; UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 8.45, par 1 e par. 3.

[104] Con particolare riferimento all'art. 8.54 dell'Accordo di libero scambio tra UE e Repubblica di Singapore v., *inter alios*: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 494.

senti impegni a consentire la circolazione di informazioni nel suddetto settore [105]; dall'altro, figurano previsioni a tutela della «riservatezza» [106], il cui scopo è quello di controbilanciare tali impegni, ma comunque senza che ciò determini «restrizioni degli scambi di servizi» [107].

3. *Le criticità degli impegni al trasferimento di dati, e delle disposizioni finalizzate a controbilanciarli, negli accordi commerciali dell'UE*

Attraverso l'indagine fin qui condotta è stato possibile riscontrare la presenza di disposizioni che incidono sui flussi di dati personali e sulla protezione degli stessi all'interno di vari tipi di accordi dell'UE di natura (esclusivamente o anche solo parzialmente) commerciale: alcuni, più risalenti, recanti carattere multilaterale e facenti parte del *corpus* normativo dell'OMC; altri, più recenti, aventi invece natura bilaterale e conclusi dall'UE al di fuori del quadro giuridico dell'OMC.

Gli articoli di cui sopra, nonostante alcune differenze tra loro, presentano praticamente sempre la stessa struttura: da un lato, stabiliscono un *data flows commitment*, impegnano cioè ciascuna parte, in certi settori come i servizi finanziari o quelli di telecomunicazione, a consentire il flusso di determinate informazioni verso l'altra parte; dall'altro lato, contengono una previsione a tutela dei dati personali e della *privacy*, finalizzata dunque a controbilanciare il precedente impegno.

Come si è rapidamente accennato, però, tali disposizioni non sono esenti da criticità. Alcune di esse riguardano la loro semplice presenza all'interno dei citati accordi: non è infatti per nulla chiaro se, e fino a che punto, la Commissione europea sia autorizzata a negoziare, negli accordi commerciali tra l'UE e Stati terzi, previsioni che possano incidere sulla protezione dei dati e sulla *privacy*. Altre delle summenzionate criticità riguardano invece la concreta formulazione delle previsioni analizzate finora: sebbene da questo punto di vista gli articoli contenuti negli accordi bilaterali dell'UE rappresentino un passo in avanti rispetto a quelli dell'*Understanding* e dell'*Annex*, vi sono ancora rilevanti motivi per

---

[105] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 8.26 («Accesso a reti e servizi pubblici di telecomunicazioni e relativo utilizzo»), par. 3; UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 8.31 («Accesso a reti e servizi pubblici di telecomunicazione e relativo uso»), par. 3.

[106] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 8.27 («Riservatezza delle informazioni»); UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 8.36 («Riservatezza delle informazioni»).

[107] Con particolare riferimento all'art. 8.27 dell'Accordo di libero scambio tra UE e Repubblica di Singapore v., *inter alios*: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 493.

ritenere che tutte le disposizioni fin qui esaminate non forniscano una tutela sufficiente ai dati personali e alla *privacy*. Ancora una volta, inoltre, si finirà per mettere in evidenza un problema di coordinamento tra la disciplina dell'Unione europea in materia di dati personali e la regolamentazione contenuta nei trattati internazionali conclusi dalla stessa UE in ambito commerciale: osservando l'una si pone il concreto rischio di disattendere l'altra e viceversa.

Di tutte le circostanze appena anticipate, si darà una spiegazione più approfondita nelle pagine che seguono.

3.1. *Le criticità derivanti dalla semplice presenza di previsioni in materia di dati personali negli accordi commerciali dell'UE*

Per prima cosa, si analizzeranno le problematiche connesse alla semplice presenza, nei trattati commerciali dell'UE, di disposizioni che possano incidere sui flussi di dati personali e sulla loro protezione.

Come noto, il compito di negoziare i trattati commerciali spetta alla Commissione europea; all'interno di quest'ultima, ancor più nello specifico, si occupa della materia la Direzione generale «Commercio», altrimenti nota come DG TRADE, responsabile della politica per il commercio con i Paesi del resto del mondo [108].

La Commissione, tuttavia, porta avanti i negoziati nel rispetto dei mandati con cui il Consiglio impartisce le necessarie direttive [109], che includono gli obiettivi

[108] Sulla Direzione generale «Commercio», si veda la pagina del sito della Commissione europea ad essa dedicata, consultabile al seguente link: *https://ec.europa.eu/info/departments/trade_it* (ultimo accesso in data 31 dicembre 2024).

[109] La procedura per la negoziazione e la conclusione di accordi commerciali da parte dell'Unione europea è disciplinata specialmente da due articoli collocati nella «Parte quinta» del TFUE, quella dedicata all'«Azione esterna dell'Unione»: l'art. 207 e l'art. 218. Quest'ultimo detta una «procedura unica» per tutti i tipi di accordi internazionali stipulabili dall'Unione. Vi sono poi altre previsioni del medesimo trattato che, in riferimento ad alcune materie specifiche, prevedono delle varianti a tale procedura: tra di esse figura l'altro articolo menzionato, il 207, dedicato proprio alla stipulazione degli accordi commerciali. Dal combinato disposto delle due summenzionate previsioni, si evince quanto segue: la procedura prende le mosse da un'iniziativa della Commissione europea, che può infatti presentare una raccomandazione al Consiglio affinché questo la autorizzi all'avvio dei negoziati con lo Stato terzo (o gli Stati terzi). A queste due istituzioni, Consiglio e Commissione, spetterà il compito di adoperarsi durante tutta la procedura affinché gli accordi negoziati siano compatibili con le politiche e norme interne dell'Unione. I negoziati sono condotti dalla Commissione in consultazione con un Comitato speciale, designato dal Consiglio per assisterla e composto da rappresentanti degli Stati membri. La Commissione, inoltre, porta avanti i negoziati nel quadro delle direttive che il Consiglio può impartirle. Riferisce altresì periodicamente al Comitato speciale e al Parlamento europeo sui progressi dei negoziati. È poi il Consiglio, su proposta della Commissione, ad adottare una decisione che autorizza la firma dell'accordo e, se del caso, la sua applicazione provvisoria prima dell'entrata in vigore. Quanto alla conclusione formale del trattato, anche la decisione di procedere alla stessa da parte dell'Unione è presa, su proposta della Commissione, dal Consiglio previa approvazione del Parlamento europeo.

e l'ambito dei negoziati medesimi, nonché eventuali limiti di tempo [110].

Si può prendere a questo punto come esempio il mandato indirizzato dal Consiglio alla Commissione in merito alla negoziazione del CETA tra UE e Canada [111]. Tale mandato, risalente al 2009, ma reso pubblico solo nel 2015, contiene riferimenti a svariati settori [112]. Tuttavia, non è possibile rinvenire nel documento previsioni che facciano riferimento alla tutela della *privacy* o alla protezione dei dati personali; queste ultime non risultano dunque affatto menzionate all'interno del mandato [113]. Analoghe considerazioni, inoltre, possono essere svolte anche per i mandati di negoziato relativi agli altri accordi commerciali visti fin qui [114].

In verità, nei mandati stessi sono anche presenti delle formule che consentono un certo grado di flessibilità [115]. Ma l'incertezza rimane: come affermato nel 2015 anche dall'allora Garante europeo della protezione dei dati, Giovanni Buttarelli, di fronte ai membri delle Commissioni del Parlamento europeo per il commercio internazionale (INTA) e per le libertà civili, la giustizia e gli affari interni (LIBE), il testo dei mandati non rende completamente chiaro fino a che punto la Commissione avesse il mandato di negoziare previsioni che potessero avere effetto sulla protezione dei dati [116].

Si precisa che gli accordi misti devono essere conclusi contemporaneamente anche dagli Stati membri; rimane però fermo che gli atti formali che contraddistinguono l'*iter* di negoziazione e conclusione dell'accordo da parte dell'Unione seguiranno le regole appena ricordate. In dottrina, sulla procedura per la negoziazione e la conclusione degli accordi internazionali dell'Unione (ivi compresi quelli commerciali), v. *inter alios*: R. ADAM-A. TIZZANO, *op. cit.*, pp. 905-914.

[110] Sul «mandato di negoziato» v. anche la pagina del sito del Consiglio europeo e del Consiglio dell'Unione europea dedicata agli «Accordi commerciali dell'UE», consultabile al seguente link: *https://www.consilium.europa.eu/it/policies/trade-policy/trade-agreements/* (ultimo accesso in data 31 dicembre 2024).

[111] UE, Consiglio dell'Unione europea, *Documento 9036/09*, 24 aprile 2009, reso pubblico il 15 dicembre 2015.

[112] A titolo puramente esemplificativo, il Titolo 7 del mandato prevede che: «L'accordo comprenderà norme volte a garantire un'adeguata ed efficace tutela e applicazione dei diritti di proprietà intellettuale» (§ 32); ma ci sono cenni anche ad altri interessi pubblici, come la tutela e salvaguardia dell'ambiente, il lavoro e la cultura (§ 5 ss.).

[113] Sulla mancata menzione della *privacy* e della protezione dei dati personali all'interno del mandato del Consiglio alla Commissione relativo alla negoziazione del CETA tra UE e Canada, v. *inter alios*: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 21.

[114] Ad esempio, il mandato del Consiglio alla Commissione relativo alla negoziazione dell'EPA tra UE e Giappone: UE, Consiglio dell'Unione europea, *Documento 15864/12*, 29 novembre 2012, reso pubblico il 14 settembre 2017; sulla mancata menzione della *privacy* e della protezione dei dati personali all'interno di tale mandato, v. *inter alios*: S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 217.

[115] Riprendendo come esempio il mandato riguardante il CETA, il Titolo 12 prevede che: «L'accordo potrà comprendere norme relative ad altri settori connessi alle relazioni economiche qualora nel corso dei negoziati entrambe le parti esprimano un interesse in tal senso» (§ 41).

[116] UE, Garante europeo della protezione dei dati, *Trade agreements and data flows. Joint*

L'assenza di qualunque riferimento alla *privacy* e alla protezione dei dati personali all'interno dei mandati di negoziato appena presi in considerazione è tutto fuorché una casualità o una dimenticanza. Si tratta, al contrario, di una circostanza figlia di precise considerazioni di tipo politico, presenti già da tempo, ma ulteriormente esplicitate nel 2014 dall'allora candidato alla carica di Presidente della Commissione europea, Jean-Claude Juncker. Quest'ultimo, nei suoi «Orientamenti politici per la prossima Commissione europea», affermava quanto segue: «Da Presidente della Commissione sarò tuttavia anche inequivocabile nell'indisponibilità a immolare sull'altare del libero scambio le norme europee in materia di […] protezione dei dati […]. Da Presidente della Commissione, saranno per me non negoziabili […]» valori tra cui «[…] la protezione dei dati personali degli europei […]» [117]. E sono proprio tali parole di Juncker ad essere state citate, un anno più tardi, nel menzionato intervento di Buttarelli, a sostegno dell'affermazione secondo cui sembra che non vi sia alcuno specifico mandato a negoziare i diritti alla *privacy* e alla protezione dei dati personali negli accordi commerciali [118].

Ci si domanda, dunque, quale sia il corretto approccio da seguire. La risposta

---

hearing of the INTA and LIBE committees, European Parliament, 16 giugno 2015, p. 2, secondo cui: «*[…] the text of mandate is not fully clear as to what extent the Commission has the mandate to negotiate provisions that may have an effect on data protection […]*». A onor del vero, nel citato passaggio, il Garante Giovanni Buttarelli non si stava riferendo ad accordi menzionati nella presente trattazione, bensì al Partenariato transatlantico su commercio e investimenti o *Transatlantic Trade and Investment Partnership* (TTIP) tra l'UE e gli USA, e all'Accordo sugli scambi di servizi o *Trade in Services Agreement* (TiSA), di carattere multilaterale; entrambi gli accordi non sono poi stati conclusi. Le considerazioni di Buttarelli, tuttavia, possono essere estese anche ai mandati di negoziato di cui si è parlato fin qui, che presentano caratteristiche analoghe.

[117] J.C. Juncker, *Un nuovo inizio per l'Europa. Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico – Orientamenti politici per la prossima Commissione europea*, Strasburgo, 15 luglio 2014, § 6. Si coglie l'occasione per precisare che le necessità, da un lato, di favorire i flussi di dati e, dall'altro, di garantire la *privacy* e la protezione dei dati personali hanno trovato menzione anche negli «Orientamenti politici» delle due Commissioni presiedute da Ursula von der Leyen; sul punto v.: U. Von Der Leyen, *Un'Unione più ambiziosa. Il mio programma per l'Europa – Orientamenti politici per la prossima Commissione europea 2019-2024*, 2019, § 3, secondo cui: «[…] dobbiamo trovare una nostra strada europea, che consenta di equilibrare il flusso e l'ampio uso dei dati tutelando al contempo alti livelli di privacy, sicurezza, protezione e norme etiche. Con il regolamento generale sulla protezione dei dati siamo già su questa strada, e molti paesi hanno seguito il nostro esempio […]»; U. Von Der Leyen, *La scelta dell'Europa – Orientamenti politici per la prossima Commissione europea 2024-2029*, Strasburgo, 18 luglio 2024, p. 12, secondo cui: «[…] intendiamo presentare una strategia europea per l'Unione dei dati. La strategia si fonderà sulle norme vigenti in materia di dati per garantire un quadro giuridico semplificato, chiaro e coerente che consenta alle imprese e alle amministrazioni pubbliche di condividere i dati senza soluzione di continuità e su vasta scala, rispettando nel contempo elevati standard di tutela della vita privata e di sicurezza […]».

[118] UE, Garante europeo della protezione dei dati, *Trade agreements and data flows*, cit., p. 2, secondo cui: «*[…] Commission President Juncker has repeatedly made clear that fundamental rights, such as the rights to privacy and to the protection of personal data are in his view not negotiable. And indeed, it seems there is no specific mandate to negotiate these rights […]*».

è fornita, in realtà, proprio dalla Commissione europea nell'ormai nota Comunicazione del 2017 «Scambio e protezione dei dati personali in un mondo globalizzato», in cui si afferma con chiarezza che, in linea di principio, «il dialogo con i paesi terzi in materia di protezione dei dati e i negoziati commerciali devono seguire percorsi separati» [119]. Per consentire i flussi di dati personali verso uno Stato extra-UE, sarà dunque opportuno cercare di addivenire a una decisione di adeguatezza nei suoi confronti, in assenza della quale si renderà comunque necessario il ricorso agli altri meccanismi del Capo V GDPR (le garanzie adeguate o le deroghe in specifiche situazioni); in mancanza anche di questi, lo si ricorda, il trasferimento non sarà consentito. Al contrario, i profili in questione dovranno rimanere fuori dai negoziati commerciali, poiché, come ricordato anche nella stessa Comunicazione, «negli accordi commerciali la protezione dei dati personali non è negoziabile» [120]. Giova precisare che tale approccio non è descritto solo nel documento appena citato, ma è stato sancito – sempre dalla Commissione europea – anche in altre occasioni [121]; la sua validità è stata, altresì, sostenuta pure in tempi recenti da rilevante dottrina [122].

In conclusione, si può ribadire che la Commissione, in qualità di negoziatore dell'Unione europea, non aveva alcun mandato a trattare sullo standard di protezione dei dati offerto dalla stessa UE nell'ambito dei negoziati commerciali con Stati terzi [123]. Tuttavia, è innegabile che gli accordi commerciali presi in considerazione finora, contenendo veri e propri impegni al trasferimento di informazioni, a loro volta corredati da norme su *data protection* e *privacy*, finiscano inevitabilmente per incidere sulla capacità dell'Unione di assicurare un elevato livello di protezione ai dati personali degli individui, entrando in rotta di collisione con la disciplina legislativa dell'UE in materia [124]. Come si è già

---

[119] UE, Comunicazione della Commissione europea al Parlamento europeo e al Consiglio, *Scambio e protezione dei dati personali in un mondo globalizzato*, 10 gennaio 2017, COM/2017/07 final, § 3.1.

[120] *Ibid*., § 3.

[121] Ad esempio v.: UE, Comunicazione della Commissione, *Commercio per tutti – Verso una politica commerciale e di investimento più responsabile*, cit., § 2.1.2., secondo cui: «[…] La Commissione è impegnata ad assicurare che i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali dei cittadini dell'UE siano pienamente garantiti da un solido quadro giuridico in materia di protezione dei dati. Le norme in materia di trattamento dei dati personali non formano oggetto dei negoziati né sono interessate dagli accordi commerciali […]».

[122] Sul punto v., *inter alios*: K. Irion-M.E. Kaminski-S. Yakovleva, *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, in *University of Chicago Law Review Online*, 2023, p. 20, secondo cui: «*[…] Efforts to place data privacy into international trade law would result in an unconstructive relationship […]*».

[123] Sul punto v. anche: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 56, secondo cui: «*EU negotiators have no mandate to bargain over EU data protection standards in trade negotiations*».

[124] S. Yakovleva-K. Irion, *Pitching trade against privacy*, cit., p. 217, secondo cui: «*[…] trade*

anticipato, dunque, è possibile affermare che la semplice presenza negli accordi commerciali di previsioni come quelle puntualmente analizzate fin qui possa essere considerato un elemento problematico in quanto tale, non essendo affatto chiaro in che misura le istituzioni dell'UE fossero legittimate a inserirle.

3.2. *Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: alcuni miglioramenti*

Alle perplessità appena esposte, se ne aggiungono poi altre, legate più prettamente a come le disposizioni sui flussi e sulla protezione dei dati personali sono formulate.

Da questo punto di vista, è preliminarmente necessario evidenziare che, rispetto agli articoli contenuti nell'*Understanding on Commitments in Financial Services* e nell'*Annex on Telecommunications*, quelli inseriti negli accordi commerciali bilaterali dell'UE rappresentano un indubbio passo in avanti. La ragione non riguarda tanto la formulazione dei *data flows commitments*, che nei vari strumenti presi in considerazione rimane fondamentalmente costante, bensì quella delle previsioni a tutela della *privacy* e dei dati personali. Si vuole infatti far notare che queste ultime, sia nell'*Understanding* che nell'*Annex*, sono formulate come delle eccezioni rispetto alla regola generale [125]. Ciò significa che ciascuna parte ha semplicemente una facoltà di adottare misure a protezione della *privacy* e dei dati personali, non certo un obbligo.

Inoltre, la regola generale rimane quella dell'impegno a consentire determinati flussi transfrontalieri di dati, a cui per l'appunto si può derogare ma solo in presenza di condizioni piuttosto stringenti. Nel caso dell'*Understanding*, è previsto che il diritto in questione non possa essere utilizzato per eludere le previsioni del GATS [126]; in quello dell'*Annex*, invece, è addirittura richiesto un doppio livello di condizioni: in primo luogo le misure eccezionalmente consentite devono essere «necessarie» («*necessary*») alla realizzazione dell'interesse perseguito; in seconda battuta, esse non devono essere applicate secondo modalità che costituirebbero un mezzo di discriminazione arbitraria o ingiustificata, ovvero una restrizione dissimulata allo scambio di servizi [127]. Nel caso dell'*Annex,* in particolare, è dunque richiesta un'«analisi a due livelli» («*two-tier analysis*») analoga a quella prevista dal già ampiamente analizzato art. XIV GATS: da un lato, il medesimo «test di necessità»; dall'altro lato, gli stessi identici requisiti del «*chapeau*». Si può ben

---

deals, however, are affecting the EU's ability to afford a high level of protection for individual's personal data and may clash with […] the strengthened EU legislation».

[125] WTO, *Understanding on Commitments in Financial Services*, cit., art. B.8; WTO, *General Agreement on Trade in Services*, *Annex on Telecommunications*, cit., art. 5, lett. d).

[126] WTO, *Understanding on Commitments in Financial Services*, cit., art. B.8.

[127] WTO, *General Agreement on Trade in Services*, *Annex on Telecommunications*, cit., art. 5, lett. d).

ricordare come, già a proposito di tale disposizione dell'Accordo generale sugli scambi di servizi, sia stata evidenziata la grande difficoltà di rispettarne tutte le condizioni e dunque di avvalersi dell'eccezione ivi stabilita. Valendo per l'art. 5, lett. d), dell'*Annex* considerazioni corrispondenti, si può dunque comprendere senza fatica quanto stretta sia la portata di tale previsione derogatoria e di conseguenza anche la possibilità di adottare misure a tutela della riservatezza [128].

Al contrario, come si è già detto, gli articoli contenuti negli accordi commerciali bilaterali conclusi dall'Unione europea in epoca successiva, e in particolare nei loro capitoli dedicati ai servizi finanziari e di telecomunicazione, appaiono indubbiamente più evoluti e più sensibili nei confronti delle esigenze della *privacy* e della *data protection*. Qui è infatti possibile rilevare come le disposizioni finalizzate a controbilanciare i *data flows commitments* siano non delle eccezioni a degli obblighi di portata più generale, ma a loro volta degli obblighi positivi di adottare o mantenere garanzie adeguate alla tutela degli interessi in questione. Lo si può rilevare nel CETA [129], in accordi più risalenti come l'EUKOR [130] (ma non solo) [131], nonché in trattati più recenti come quelli con Singapore [132] e Vietnam [133].

Negli accordi bilaterali in esame è quindi possibile riscontrare non un obbligo di natura commerciale e un'eccezione al libero scambio, il cui utilizzo sarebbe

---

[128] Sulle criticità dell'art. B.8 dell'*Understanding on Commitments in Financial Services* e dell'art. 5, lett. d), dell'*Annex on Telecommunications* v.: S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., pp. 492-495. Sull'art. B.8 dell'*Understanding on Commitments in Financial Services* v. anche: A. WESSEL, *Broken data protection in EU trade agreements*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 22 settembre 2016, par. 4.

[129] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 13.15, par. 2; art. 15.3, par. 4. In dottrina, sul punto, v. *inter alios*: A. WESSEL, *CETA will harm our privacy*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 15 aprile 2016; A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 3; S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., pp. 493-495; F. VELLI, *op. cit.*, pp. 890-891.

[130] UE, *Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra*, cit., art. 7.43, lett. b). In dottrina, sul punto, v. *inter alios*: A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 2; F. VELLI, *op. cit.*, p. 890.

[131] Formule pressoché analoghe a quella presente nell'EUKOR possono essere rinvenute nell'art 157, par. 2, dell'Accordo commerciale con Colombia, Perù ed Ecuador; nell'art. 198, par. 2, dell'Accordo di associazione con l'America centrale; nonché nell'art. 129, par. 2, dell'Accordo di associazione con l'Ucraina.

[132] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 8.54, par. 2, e art. 8.27. In dottrina, sul punto, v. *inter alios*: A. WESSEL, *EU-Singapore Trade Agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 19 aprile 2018.

[133] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 8.45, par. 1, e art. 8.36. In dottrina, sul punto, v. *inter alios*: A. WESSEL, *Weak Data Protection in EU-Vietnam Trade Agreement*, in *Blog Van Vrijschrift*, 6 febbraio 2020.

facoltativo e la cui portata risulterebbe particolarmente ristretta, ma due obblighi giustapposti. Con il primo le parti si vincolano a consentire il flusso di determinate informazioni. Con il secondo si impegnano ad adottare misure «opportune», o «appropriate», o «adeguate» a salvaguardare la *privacy* e i dati personali, l'esigenza di tutelare i quali viene dunque enfatizzata. In definitiva si tratta di articoli che, come sostenuto anche da certi autori, rappresentano un'indubbia evoluzione rispetto a quelli dell'*Understanding* e dell'*Annex*: essi pongono la responsabilità di proteggere i dati personali su entrambe le parti, e quindi non solo sull'UE, ma di volta in volta anche su Canada, Corea del Sud, Singapore, Vietnam, etc., dal momento che tali Stati hanno assunto un preciso obbligo in tal senso; inoltre, non venendo più richiesto alle misure di essere strettamente «necessarie» alla realizzazione degli interessi perseguiti, lasciano alle parti maggior margine di manovra nella regolamentazione [134].

Non è tutto. Merita infatti di essere notato che, nonostante in alcuni accordi più recenti permangano delle previsioni "vecchio stampo", l'UE si sta sovente impegnando per rimuoverle. Emblematico è il caso dell'art. 8.63 dell'EPA con il Giappone: se da un lato il par. 1 sanciva il consueto *data flows commitment* nel settore dei servizi finanziari, dall'altro il par. 2 conteneva non un secondo obbligo, ma un'eccezione al primo [135]. Inoltre, la possibilità di avvalersi della deroga in questione era subordinata a una precisa condizione: quella in base a cui tale diritto non fosse utilizzato per eludere quanto disposto in determinate sezioni dell'accordo. La presenza simultanea di entrambe le caratteristiche appena menzionate rendeva l'art. 8.63 dell'EPA estremamente simile all'art. B.8 dell'*Understanding on Commitments in Financial Services*: come sostenuto da certa dottrina, si trattava di un ritorno al passato che non giovava di certo alle esigenze di protezione dei dati personali e della *privacy* [136]. Tuttavia, lo si è visto, tale articolo non è oggi più presente all'interno dell'EPA: è stato infatti eliminato dal successivo accordo sui flussi transfrontalieri di dati tra UE e Giappone, il quale ha invece introdotto disposizioni di diversa tipologia (di cui si dirà meglio nel proseguo).

---

[134] Sul fatto che gli «obblighi positivi» («*positive obligations*») in materia di protezione dei dati personali e della *privacy* contenuti negli accordi commerciali bilaterali dell'UE rappresentino un'evoluzione rispetto alle disposizioni presenti nell'*Understanding on Commitments in Financial Services* e nell'*Annex on Telecommunications* v., *inter alios*: A. Wessel, *Broken data protection in EU trade agreements*, cit., par. 2; S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 493-495; A. Bendiek-M. Römer, *Externalizing Europe: the global effects of European data protection*, in *Digital Policy, Regulation and Governance*, 2018.

[135] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 8.63, par. 2.

[136] M. Bartl-K. Irion, *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, cit., p. 5. Sulle problematiche del "vecchio" art. 8.63 dell'EPA con il Giappone, ma in senso parzialmente difforme in quanto meno critico, v. anche: A. Wessel, *EU-Japan trade agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 10 gennaio 2018.

In breve, non è azzardato affermare che, nel corso del tempo, alcuni miglioramenti nella formulazione delle *data protection provisions* possono essere rinvenuti.

3.3. *Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: problematiche perduranti* (segue)

Da un'analisi ancor più attenta emerge però un quadro meno positivo: anche nella formulazione delle disposizioni in materia di dati personali inserite all'interno degli accordi commerciali bilaterali conclusi dall'Unione – nonostante i descritti passi in avanti rispetto agli strumenti adottati in seno all'OMC in epoca più risalente – permangono alcuni aspetti critici.

Innanzitutto, si è sottolineato come la tendenza più recente (quantomeno tra gli accordi visti fin qui) sia quella di prevedere non un obbligo di portata generale e un'eccezione, ma due obblighi: non solo quello di consentire certi trasferimenti, ma anche quello di adottare misure adeguate a tutela di dati personali e *privacy*.

Ciò, tuttavia, non è sempre vero: ancorché raramente, persistono infatti alcune previsioni "vecchio stampo". In particolare, se è vero che l'art. 8.63 dell'EPA col Giappone è stato eliminato, permane invece l'art. 8.44 del medesimo accordo, in materia di servizi di telecomunicazione. Mentre il par. 3 fissa un impegno a consentire la circolazione di determinate informazioni, il par. 4 contiene un'eccezione [137]. A tale clausola derogatoria, inoltre, si può far ricorso solo in presenza delle stesse stringenti condizioni previste all'art. 5, lett. d), dell'*Annex on Telecommunications*: in primo luogo, le misure adottate devono essere «necessarie» a tutelare la riservatezza; in seconda battuta, esse non devono essere applicate «in una forma che costituisca una discriminazione arbitraria o ingiustificata o una restrizione dissimulata degli scambi di servizi». Tali requisiti sono, ancora una volta, gli stessi dell'art. XIV GATS (test di necessità, *chapeau*) che, com'è noto, risultano particolarmente ardui da rispettare. Si può assistere dunque a una regressione delle disposizioni in materia di protezione della *privacy* [138], a cui non è stato ancora posto rimedio.

Il problema più rilevante è tuttavia un altro. Si torni ora a quei numerosi articoli che effettivamente presentano una formulazione più evoluta, consistente come si è detto nella presenza non di un obbligo e di un'eccezione, ma di due obblighi giustapposti. Orbene, pur trattandosi di soluzioni migliorative nell'ottica della protezione dei dati personali e della *privacy*, non si può far a meno di

---

[137] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 8.44, par. 4.

[138] Sulle criticità dell'art. 8.44 dell'EPA con il Giappone v.: M. Bartl-K. Irion, *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, cit., pp. 5-6.

rilevare come anche tali previsioni presentino dei significativi punti deboli, che rischiano di mettere a repentaglio il raggiungimento dell'obiettivo prefissato. Si può infatti notare che, nonostante l'adozione delle misure adeguate rappresenti a tutti gli effetti un secondo obbligo, esso risulta assai meno robusto e centrale del primo (quello di consentire i flussi): le misure di cui sopra devono infatti sovente rispettare determinati limiti e condizioni. Alcuni esempi: l'art. 15.3, par. 4, del CETA prevede che l'adozione delle misure in questione avvenga «[i]n applicazione dell'articolo 28.3 (Eccezioni generali)» il quale, lo si ricorda, è una disposizione pressoché analoga all'art. XIV GATS; inoltre, sempre l'art. 15.3, par. 4, ribadisce che è «fatto salvo l'obbligo di non applicare tali misure in un modo che rappresenti una discriminazione arbitraria o ingiustificata o una restrizione dissimulata agli scambi», formula ormai nota. L'art. 8.54, par. 2, dell'accordo con Singapore prescrive invece che le «garanzie non siano utilizzate per eludere le disposizioni» del trattato, mentre l'art. 8.26 del medesimo strumento prevede che ciascuna parte garantisca la riservatezza, ma «senza restrizioni degli scambi di servizi». Quanto al FTA con il Vietnam, l'art. 8.45, par. 3, e l'art. 8.36 presentano formule quasi del tutto coincidenti, rispettivamente, con le due appena riportate in riferimento all'accordo con Singapore.

Tirando le fila, nonostante ci si trovi di fronte a degli obblighi positivi, i limiti che vengono posti all'adozione delle misure a tutela dei dati personali sono decisamente simili a quelli che abbiamo trovato nelle disposizioni formulate come eccezioni, come l'art. B.8 dell'*Understanding* o l'art. 5, lett. d), dell'*Annex* (nonché il "vecchio" art. 8.63 e l'art. 8.44 dell'EPA col Giappone). Alcuni di tali requisiti, inoltre, richiamano a loro volta quelli dell'art. XIV GATS, la difficoltà di rispettare i quali è già stata più volte evidenziata. Si tratta dunque di condizioni che indeboliscono inevitabilmente le *data protection provisions* negli accordi commerciali bilaterali conclusi dall'Unione[139], e che rendono quanto mai chiaro che ci si trova di fronte a disposizioni pur sempre subordinate agli impegni di liberalizzazione degli scambi, l'osservanza dei quali rimane prioritaria[140].

3.4. *Le criticità derivanti dalla formulazione delle previsioni in materia di dati personali negli accordi commerciali dell'UE: la nozione di «adeguatezza» e il ruolo degli organismi sovranazionali di risoluzione delle controversie* (segue)

Ma le criticità non sono ancora terminate. È infatti opportuno porre l'accento su un altro elemento particolarmente problematico che caratterizza la formu-

[139] Sul punto, con particolare riferimento all'art. 8.54 dell'Accordo di libero scambio con Singapore, v. *inter alios*: A. WESSEL, *EU-Singapore Trade Agreement not compatible with EU data protection*, cit..

[140] S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 495.

lazione degli articoli oggetto di esame, soprattutto di quelli inseriti nei capitoli sui servizi finanziari: ci si riferisce al fatto che le «misure», o «garanzie», che entrambe le parti hanno l'obbligo di adottare, devono essere «adeguate» alla tutela dei dati personali e della *privacy*. Per essere ancor più precisi: in diverse situazioni, anche all'interno della versione italiana dell'accordo, viene adoperato proprio tale aggettivo [141]; nelle altre, pur essendo la terminologia utilizzata in lingua italiana apparentemente differente (si parla di misure «opportune»), nella versione inglese (che, infatti, si è talvolta sentito il bisogno di riportare) figura l'espressione «*adequate safeguards*» [142].

Si tratta di una terminologia che non risulta di certo nuova: è infatti la medesima già incontrata nella parte di trattazione dedicata al Capo V del Regolamento (UE) 2016/679. I due principali meccanismi previsti da quest'ultimo in presenza dei quali è possibile trasferire dati personali verso un Paese extra-UE sono, come noto, la decisione di «adeguatezza», che viene adottata dalla Commissione nei confronti di uno Stato che garantisce un livello di protezione «adeguato», e le garanzie «adeguate», che devono essere fornite da chi trasferisce tali dati. Sia il GDPR, da un lato, che gli accordi commerciali bilaterali dell'UE, dall'altro, sembrano quindi richiedere la presenza di un'adeguata tutela dei dati personali che vengono trasferiti. Si potrebbe dunque credere che l'utilizzo della stessa terminologia abbia l'effetto di fissare un medesimo standard, comune tanto al Regolamento quanto agli accordi, che più nello specifico sarebbe quello definito dalla Corte di giustizia dell'Unione europea nelle sentenze *Schrems I* e *Schrems II* e già ampiamente esaminato all'interno della presente trattazione.

Tale osservazione non corrisponde al vero. Come si è detto, il Giudice di Lussemburgo ritiene che si possa parlare di un livello di protezione «adeguato» quando esso è «sostanzialmente equivalente» a quello garantito all'interno dell'Unione; infatti, arriva a tale interpretazione attraverso una lettura della disciplina UE in materia di dati personali alla luce degli articoli 7 e 8 della Carta di Nizza. Tuttavia, si deve tenere a mente che la risoluzione delle controversie relative all'interpretazione degli accordi commerciali bilaterali è attribuita non certo alla Corte, bensì agli organismi sovranazionali previsti da tali accordi: tali organismi, nel caso si instaurasse una disputa sul punto, non sarebbero ovviamente tenuti a leggere la nozione di «garanzie adeguate» alla luce della Carta dei diritti fondamentali dell'Unione europea [143].

Tale considerazione vale, senza dubbio, per gli organismi deputati a risolvere

---

[141] Ad esempio, nell'art. 8.54, par. 2, del FTA con Singapore, nonché nell'art. 8.45, par. 1, del FTA.

[142] Ad esempio, nell'art. 13.15, par. 2, del CETA; nell'art. 7.43, lett. b), dell'EUKOR; nell'art. 157, par. 2, dell'accordo con Colombia, Perù ed Ecuador; nell'art. 198, par. 2, dell'Accordo di associazione con l'America centrale; nonché nell'art. 129, par. 2, dell'Accordo di associazione con l'Ucraina.

[143] Sul punto, con particolare riferimento all'art. 13.15 del CETA, v.: A. Wessel, *CETA will harm our privacy*, cit..

le controversie che sorgono tra le parti, che sono previsti, con una disciplina piuttosto simile, in tutti gli accordi commerciali bilaterali visti fin qui. Nel CETA, ad esempio, le norme in materia sono dettate dal Capo 29: l'art. 29.17 dello stesso fissa le regole generali di interpretazione, che si limitano a prevedere che essa avvenga secondo le norme di interpretazione consuetudinarie del diritto internazionale pubblico, comprese quelle stabilite dalla Convenzione di Vienna sul diritto dei trattati, e tenendo conto delle pertinenti interpretazioni degli organi OMC [144].

Ma la stessa considerazione vale anche per gli organismi deputati a risolvere le controversie che sorgono tra investitori e Stati in materia di investimenti. Le procedure ISDS, a differenza delle precedenti, non sono previste in tutti gli accordi analizzati finora; talvolta, sono contenute in separati trattati di protezione degli investimenti conclusi con i medesimi Stati, come nei casi di Singapore e Vietnam (tali accordi, nel momento in cui si scrive, non sono però ancora entrati in vigore) [145]. Una procedura ISDS è presente, però, nella Sezione F del Capo 8 del CETA (ancorché, come già rilevato, non formi oggetto di applicazione provvisoria): l'art. 8.31, che si occupa del diritto applicabile nell'ambito di tale procedura, prevede esclusivamente che l'accordo debba essere interpretato in conformità alla Convenzione di Vienna sul diritto dei trattati e alle altre regole e principi di diritto internazionale applicabili tra le parti [146].

Come si può agevolmente notare, dunque, in nessuna delle procedure summenzionate gli organismi sovranazionali sono tenuti, nell'interpretazione dell'accordo, a tenere in considerazione né la Carta dei diritti fondamentali dell'UE, né la giurisprudenza della Corte di giustizia. Di conseguenza, in una controversia in cui dovessero venire in rilievo le disposizioni in materia di dati personali, la nozione di tutela «adeguata» non verrebbe presumibilmente interpretata come «sostanzialmente equivalente» a quella offerta nell'Unione: l'«adeguatezza» prevista dagli accordi commerciali bilaterali dell'UE non ha quindi un contenuto normativo ben preciso [147] e fornisce ai dati personali degli individui una protezione certamente inferiore rispetto all'«adeguatezza» sancita dal Giudice di Lussemburgo nell'ambito della vicenda *Schrems* [148].

---

[144] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 29.17 («Regola generale di interpretazione»).

[145] Sul punto v. con riferimento a Singapore: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/singapore/* (ultimo accesso in data 31 dicembre 2024); con riferimento al Vietnam: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/* (ultimo accesso in data 31 dicembre 2024).

[146] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 8.31 («Diritto applicabile ed interpretazione»), par. 1.

[147] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 495.

[148] A. Wessel, *CETA will harm our privacy*, cit.; v. anche: A. Wessel, *CETA: ISDS and data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 29 aprile 2016.

Si vuole precisare che con tutta probabilità, nell'ottica di dare alla nozione «garanzie adeguate» il significato più ampio possibile, la miglior formulazione tra quelle viste finora potrebbe essere proprio quella dell'art. 13.15, par. 2, del CETA. Tale disposizione, dopo aver sancito il noto obbligo in capo a ciascuna parte di mantenere in vigore le «*adequate safeguards*» a tutela della vita privata, in particolare in relazione alla trasmissione dei dati personali, aggiunge quanto segue: «Qualora le informazioni finanziarie trasmesse contengano dati personali, la trasmissione deve avvenire in conformità della legislazione sulla protezione dei dati personali nel territorio della parte da cui la stessa ha preso avvio». Orbene, è stato autorevolmente sostenuto che tale espressione abbia proprio la funzione di fornire indicazioni su come la nozione di «*adequate safeguards*» debba essere interpretata [149], andando quindi a rafforzarla. Allo stesso tempo, occorre sottolineare che permangono dei dubbi su tale espressione: ad esempio, si potrebbe sostenere che essa fornisca indicazioni sulla «trasmissione» in sé e per sé, senza nulla dire su cosa avvenga dopo la stessa [150]; è poi una disposizione che nulla cambia sul piano della giurisdizione [151]. Inoltre, è utile ripetere che, di tutti gli articoli presi in considerazione fino a qui, l'art. 13.15 del CETA è l'unico a contenere una simile indicazione; tutti gli altri, sia antecedenti che successivi, ne sono sprovvisti.

Tornando quindi all'interpretazione della nozione di garanzia «adeguata», anzi, più in generale al ruolo degli organismi sovranazionali di risoluzione delle controversie relative agli accordi commerciali, si può concludere nel senso di un'inidoneità di questi a proteggere efficacemente i dati personali: ai rilievi precedentemente sviluppati, si aggiunge la più ampia considerazione secondo cui collegi istituiti ai sensi di accordi commerciali difficilmente potranno dare sufficiente peso alle esigenze di tutela dei diritti fondamentali. Come affermato da certa dottrina, le corti e i tribunali specializzati tendono ad essere particolarmente entusiasti nel rivendicare le finalità per cui sono stati istituiti [152], quindi, in questo caso, la progressiva liberalizzazione degli scambi, che ha un'indubbia prevalenza sulle altre istanze alla luce dell'oggetto e dello scopo del trattato [153].

---

[149] A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 3, secondo cui (in riferimento all'art. 13.15, par. 2, del CETA): «*[…] The last sentence then gives guidance to the interpretation of "adequate safeguards" […]*». Nello stesso senso v. anche: A. WESSEL, *CETA will harm our privacy*, cit.; F. VELLI, *op. cit.*, p. 891, secondo cui (sempre in riferimento all'art. 13.15, par. 2, del CETA): «*[…] the second sentence could possibly offer interpretational guidance on the words "adequate safeguards" from the sentence above […]*».

[150] A. WESSEL, *CETA will harm our privacy*, cit., secondo cui (in riferimento all'art. 13.15, par. 2, del CETA): «*[…] the text leaves room to argue that it provides guidance regarding the cross-border transfer, not regarding what happens after the transfer […]*».

[151] A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 3.

[152] *Ibid*., par. 5, secondo cui: «*[…] Specialist courts and tribunals tend to become over-enthusiastic about vindicating the purposes for which they were set up […]*».

[153] S. YAKOVLEVA, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 495.

Insomma, è vero che le *data protection provisions* contenute negli accordi bilaterali dell'UE pongono degli obblighi positivi in capo alle parti, le quali sono dunque tenute ad adottare delle misure «adeguate» a tutela dei dati personali e della *privacy*; al tempo stesso, è del tutto lecito dubitare del fatto che, sul piano prettamente operativo, sia possibile far rispettare efficacemente simili obblighi attraverso il ricorso agli organismi sovranazionali istituiti dagli accordi in questione. Si tratta di collegi creati con altri scopi e il cui ragionamento segue solitamente una logica differente: di norma, essi sono preposti a valutare se una misura sia in contrasto con gli impegni di liberalizzazione assunti dalle parti – ed eventualmente se possa essere giustificata – e non certo a occuparsi della tutela dei diritti fondamentali [154].

È quindi possibile concludere la presente parte della trattazione affermando, ancor più in generale, che la regolamentazione contenuta negli accordi commerciali conclusi dall'UE attribuisce una chiara prevalenza alle esigenze degli scambi: per favorire questi ultimi, l'Unione ha assunto numerosi impegni al trasferimento di dati, controbilanciandoli con misure di salvaguardia la cui portata ed efficacia risultano – per vari motivi – quantomeno dubbie. Ciò può però determinare problemi di coordinamento con l'approccio che contraddistingue la disciplina unilateralmente adottata dall'UE in materia di flussi, più attenta alla protezione delle persone fisiche.

[154] Sul punto v.: K. IRION-S. YAKOVLEVA-M. BARTL, *Trade and Privacy: Complicated Bedfellows?*, cit., p. 44, p. 45 e p. 56; v. anche: A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 2, secondo cui (in riferimento all'art. 7.43, lett. b), dell'EUKOR): «*[…] the safeguard seems hardly enforceable […]*».

CAPITOLO III

L'IMPATTO DEGLI IMPEGNI COMMERCIALI ASSUNTI A LIVELLO INTERNAZIONALE DALL'UE SULLA SUA DISCIPLINA INTERNA

SOMMARIO: 1. Il rischio di una supremazia *de facto* degli impegni commerciali sulla disciplina interna UE. – 1.1. Le conseguenze per l'UE in caso di violazione degli impegni commerciali internazionali. – 1.2. Le ricadute sul piano interno: la pressione su vari attori istituzionali europei. – 2. Le *Horizontal provisions for cross-border data flows and for personal data protection*: una possibile soluzione?. – 2.1. La genesi delle *Horizontal provisions*. – 2.2. Il contenuto delle *Horizontal provisions*. – 2.3. Le *Horizontal provisions* nella prassi: alcuni esempi incoraggianti, con particolare riferimento all'Accordo di libero scambio con la Nuova Zelanda. – 2.4. Le *Horizontal provisions* nella prassi: le criticità perduranti, con particolare riferimento al caso del TCA con il Regno Unito *(segue)*.

1. *Il rischio di una supremazia* de facto *degli impegni commerciali sulla disciplina interna UE*

Fin qui, è stato evidenziato un problema di coordinamento tra la disciplina in materia di dati personali dell'Unione europea e la regolamentazione contenuta negli accordi di natura commerciale conclusi dalla stessa. In questi ultimi, al fine di favorire le esigenze degli scambi, l'UE ha assunto diversi impegni al trasferimento di dati, cercando di controbilanciarli con misure di salvaguardia la cui portata ed efficacia, tuttavia, risulta quantomeno dubbia; ciò stride inevitabilmente con l'approccio, sancito dagli articoli 7 e (soprattutto) 8 della Carta di Nizza nonché dal GDPR, che va nel senso di garantire un elevato livello di protezione ai dati personali, per assicurare il quale sono stabiliti *inter alios* dei rigidi limiti ai flussi degli stessi [1].

A questo punto, dunque, è indispensabile interrogarsi su quali possano essere le conseguenze delle divergenze tra i due approcci, chiedendosi se vi sia il concreto rischio che uno finisca per compromettere l'altro. A tal riguardo, pre-

[1] S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 220, secondo cui: «*[…] committing to free cross-border data flows likely collides with its approach of affording a high level of protection of personal data as is called for by Article 8 of the Charter and as implemented by the GDPR […]*».

liminarmente, è necessario chiedersi se gli accordi commerciali siano idonei o meno a produrre effetti diretti nell'ordinamento dell'UE.

Come noto, i trattati internazionali sono parte integrante dell'ordinamento dell'UE[2] e, più precisamente, nella gerarchia delle fonti si collocano in posizione subordinata rispetto al diritto primario, ma sovraordinata rispetto al diritto derivato: in virtù di ciò, da un lato, essi potrebbero ben essere sindacati di fronte alla Corte in caso di inosservanza di norme primarie di carattere procedurale, ma anche sostanziale, come i diritti fondamentali della Carta tra cui pure quelli degli articoli 7 e 8[3]; dall'altro lato, il rispetto dei trattati costituisce un limite di legittimità degli atti di diritto derivato, che potrebbe portare all'annullamento di questi ultimi[4].

Tuttavia, il fatto che un accordo internazionale diventi parte integrante dell'ordinamento dell'Unione, acquisendo l'appena descritta collocazione nella relativa gerarchia delle fonti, non ha come conseguenza necessaria il fatto che le disposizioni dell'accordo medesimo producano effetti diretti nell'UE: la possibilità di invocarle in giudizio da parte dei singoli è infatti notoriamente condizionata dalla

---

[2] Sul punto v.: UE, Corte di giustizia, sentenza del 30 aprile 1974, 181/73, *R. & V. Haegeman contro Stato belga*, ECLI:EU:C:1974:41, p. 449, §§ 3/5.

[3] Tale è stata la sorte dell'Accordo PNR tra l'Unione europea e il Canada (non avente carattere commerciale): la Corte, espressasi con un parere prima della conclusione del trattato medesimo, ha ritenuto varie norme dello stesso incompatibili con diversi articoli della Carta di Nizza, fra cui proprio gli articoli 7 e 8 (UE, Corte di giustizia, Parere del 26 luglio 2017, 1/15, ECLI:EU:C:2017:592).

[4] Sulla collocazione degli accordi internazionali dell'Unione nell'ambito della gerarchia delle fonti dell'UE, v. *inter alios*: R. Adam-A. Tizzano, *op. cit.*, pp. 174-181. In questa sede, giova ricordare che i trattati internazionali conclusi dall'UE sono subordinati al TUE e al TFUE, dato che l'esercizio delle competenze internazionali dell'Unione deve avvenire nel rispetto delle regole materiali e procedurali in essi stabilite, e più in generale alle fonti aventi rango primario, come i principi generali del diritto UE e la Carta dei diritti fondamentali (che ha «lo stesso valore giuridico dei trattati» *ex* art. 6, par. 1, TUE). La logica conseguenza è che la Corte di giustizia, nei limiti delle competenze riconosciutele, può essere investita della questione della compatibilità di un accordo internazionale con il diritto primario. Ciò può avvenire prima della conclusione del trattato: sulla base di una richiesta avanzata dal Parlamento europeo, dal Consiglio, dalla Commissione o da uno Stato membro, il Giudice di Lussemburgo fornisce un parere che, se negativo, impedisce all'accordo di entrare in vigore, a meno che non sia modificato o vi sia una revisione dei Trattati (*ex* art. 218, par. 11, TFUE). Inoltre, la Corte può essere investita della questione anche dopo la conclusione del trattato stesso, nel quadro di una delle competenze di legittimità che le spettano. Al tempo stesso, occorre ricordare pure che i trattati conclusi dall'Unione vincolano, oltre agli Stati membri, anche le istituzioni (*ex* art. 216, par. 2, TFUE). Ciò significa che il rispetto degli accordi con Stati terzi, e delle decisioni di organi previsti da tali accordi, costituisce per l'appunto un limite di legittimità degli atti di diritto derivato, che può portare all'annullamento di questi ultimi e che comunque implica l'obbligo di interpretare tali atti in maniera per quanto possibile conforme ai detti accordi (sul punto v.: UE, Corte di giustizia, sentenza del 10 gennaio 2006, C-344/04, *The Queen, ex parte International Air Transport Association e European Low Fares Airline Association contro Department for Transport*, ECLI:EU:C:2006:10, § 35 ss.).

Corte di giustizia alla presenza di specifici requisiti [5]. Peraltro, sempre secondo il Giudice di Lussemburgo, qualora una norma di un trattato internazionale non esplichi effetti diretti, un atto delle istituzioni che contrasta con tale norma non può essere oggetto di annullamento, nonostante la gerarchia descritta poc'anzi [6].

Con specifico riferimento agli accordi commerciali, occorre ricordare che è estremamente improbabile che agli stessi, nonché alle decisioni degli organismi sovranazionali di risoluzione delle controversie in materia commerciale, siano riconosciuti effetti diretti [7]: questi ultimi, in alcuni casi, sono per l'appunto negati dalla giurisprudenza della Corte di giustizia [8]; in molti altri, vengono addirittura esclusi in modo esplicito mediante specifiche previsioni inserite negli accordi medesimi, tra cui si possono menzionare l'art. 23.5 dell'EPA UE-Giappone (rubricato «Assenza di effetti diretti sulle persone») [9], nonché l'art. 16.16 del FTA UE-Singapore [10] e l'art. 17.20 del FTA UE-Vietnam [11]

---

[5] La Corte di giustizia, innanzitutto, richiede la presenza degli stessi requisiti che giustificano l'esplicazione di effetti diretti di norme dei Trattati, nonché di Direttive e Decisioni: la disposizione invocata deve quindi porre un obbligo chiaro e preciso, la cui esecuzione o i cui effetti non risultino subordinati all'adozione di alcun atto ulteriore (sul punto v.: UE, Corte di giustizia, *Meryem Demirel*, cit., § 14). Nel caso delle disposizioni di origine convenzionale, inoltre, la Corte ha aggiunto l'ulteriore necessità di esaminare le stesse alla luce sia dell'oggetto e dello scopo, sia del contesto dell'accordo di cui fanno parte (sul punto v.: UE, Corte di giustizia, sentenza del 26 ottobre 1982, 104/81, *Hauptzollamt Mainz contro C.A. Kupferberg & Cie KG a.A.*, ECLI:EU:C:1982:362, § 23), test che potrebbe anche portare a negare alla radice la possibilità di riconoscere effetti diretti alle disposizioni di un accordo, indipendentemente dalla presenza degli altri requisiti.

[6] Sul punto v.: UE, Corte di giustizia, sentenza del 12 dicembre 1972, cause riunite da 21/72 a 24/72, *International Fruit Company NV e altri contro Produktschap voor Groenten en Fruit*, ECLI:EU:C:1972:115, §§ 7/9. Giova inoltre precisare che ciò è stato affermato non solo con riferimento alla possibilità che l'incompatibilità dell'atto delle istituzioni con la norma internazionale venga invocata da un privato, ma anche quando tale incompatibilità sia fatta valere da uno Stato membro (sul punto v.: UE, Corte di giustizia, sentenza del 5 ottobre 1994, C-280/93, *Repubblica federale di Germania contro Consiglio dell'Unione europea*, ECLI:EU:C:1994:367, § 109 ss.).

[7] In tal senso, v. *inter alios*: A. Semertzi, *The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements*, in *Common Market Law Review*, 2014, Volume 51, Numero 4, pp. 1125-1158, spec. pp. 1132-1135; S. Yakovleva-K. Irion, *The Best of Both Worlds?*, cit., pp. 200-202; S. Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, in *The Journal of World Investment & Trade*, 2020, Volume 21, Numero 6, pp. 881-919, spec. p. 889, secondo cui: «*[…] neither international trade agreements nor the decisions of international trade adjudicating bodies have direct effect in the EU […]*».

[8] Ad esempio, in riferimento alle pronunce degli organi dell'OMC, v.: UE, Corte di giustizia, sentenza del 9 settembre 2008, cause riunite C120/06 P e C121/06 P, *FIAMM e altri contro Consiglio e Commissione*, ECLI:EU:C:2008:476, §§ 129-131.

[9] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 23.5 («Assenza di effetti diretti sulle persone»).

[10] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, cit., art. 16.16 («Mancanza di efficacia diretta»).

[11] UE, *Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam*, cit., art. 17.20 («Mancanza di efficacia diretta»).

(entrambi rubricati «Mancanza di efficacia diretta») [12].

In ragione di quanto appena esposto, per esempio, un'impresa non potrebbe sostenere di fronte a un giudice che un trasferimento di dati personali verso uno Stato terzo è legittimo sulla base di una disposizione, contenuta in un accordo commerciale, che impegna l'UE a consentire i flussi di informazioni verso tale Paese. E, sempre a titolo esemplificativo, neppure si potrebbe chiedere l'annullamento di un atto di diritto derivato come lo stesso Regolamento (UE) 2016/679 adducendo come motivazione la violazione da parte dello stesso di norme di un accordo commerciale.

1.1. *Le conseguenze per l'UE in caso di violazione degli impegni commerciali internazionali*

Non può essere trascurato, tuttavia, un aspetto essenziale ai fini della presente trattazione: l'assenza di effetti diretti non rende gli obblighi assunti dall'Unione europea all'interno degli accordi commerciali meno vincolanti sul piano del diritto internazionale. L'UE deve anzi adempiere ai propri obblighi in buona fede; se non lo fa, può incorrere in responsabilità e conseguenze giuridiche negative, anche là dove il mancato adempimento non sia possibile a causa di vincoli derivanti dalla normativa interna della stessa UE [13]. È proprio per questo che le segnalate difficoltà nel coordinare la disciplina in materia di dati personali dell'Unione europea e la regolamentazione contenuta negli accordi di natura commerciale conclusi dalla stessa possono rappresentare un serio problema.

Nello specifico, uno Stato terzo potrebbe rivolgersi agli organismi deputati a risolvere le controversie che sorgono tra le parti di un trattato, sostenendo che il fatto che l'Unione ostacoli i flussi rappresenti un'infrazione degli impegni da essa assunti: potrebbero essere ritenuti violati tanto i *data flows commitments* «espliciti», quanto quelli che taluno ha definito «impliciti», rappresentati dalle norme di portata più generale sugli scambi di servizi, come trattamento nazionale, clausola della nazione più favorita, accesso al mercato [14]. Le violazioni *prima facie* di questi potrebbero, astrattamente, essere giustificate: così come

---

[12] Sul tema degli effetti diretti degli accordi internazionali dell'UE, v. *inter alios*: F. MARTINES, *Direct Effect of International Agreements of the European Union*, in *The European Journal of International Law*, 2014, Volume 25, Numero 1, pp. 129-147; sullo specifico caso, diverso da quelli menzionati in trattazione, in cui l'esclusione degli effetti diretti sia prevista unilateralmente dall'Unione, v. *inter alios*: G. GAJA, *Il preambolo di una decisione del Consiglio preclude al «GATT 1994» gli effetti diretti nell'ordinamento comunitario?*, in *Rivista di diritto internazionale*, 1995, pp. 407-409.

[13] S. YAKOVLEVA, *Personal Data Transfers in International Trade and EU Law*, cit., p. 889.

[14] Sul punto, con specifico riferimento ai *data flows commitment* «impliciti» contenuti nell'EPA con il Giappone, v: A. WESSEL, *EU-Japan trade agreement not compatible with EU data protection*, cit..

nel sistema OMC sono presenti le eccezioni generali dell'art. XIV GATS, anche negli accordi commerciali bilaterali si possono riscontrare simili disposizioni derogatorie [15]. Ricorrere alle stesse, però, sarebbe assai arduo, e giustificare le infrazioni risulterebbe piuttosto difficile. Anche in ragione di ciò, gli organismi sovranazionali potrebbero dar ragione al Paese extra-UE: se ciò avvenisse, quest'ultimo potrebbe avere il diritto di sospendere i propri obblighi, oppure di ricevere una compensazione.

Non solo: nel caso in cui, nei rapporti con un certo Paese terzo, fossero in vigore norme in materia di risoluzione delle controversie tra investitori e Stati in materia di investimenti, gli investitori di tale Paese che si sentissero pregiudicati da una limitazione dei flussi potrebbero avviare una procedura ISDS («*Investor-State Dispute Settlement*») contro l'UE; quest'ultima, là dove fossero riconosciute le ragioni degli investitori, potrebbe essere condannata a risarcire il danno.

A beneficio di chiarezza, si ritiene ora opportuno fornire un esempio di quanto appena illustrato in termini generali. In particolare, si prenderà in esame il caso del Canada, Stato parte del CETA, nonché destinatario di una delle decisioni di adeguatezza attualmente in vigore. Le due circostanze appena ricordate – combinate tra loro – fanno sì che al momento, apparentemente, non si pongano particolari problemi sul piano che qui interessa: la Decisione 2002/2/CE «riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (*Canadian Personal Information Protection and Electronic Documents Act*)» [16] permette infatti i trasferimenti di dati personali dall'UE verso le organizzazioni canadesi del settore privato che rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali; ciò consente dunque all'Unione di non violare i propri *data flows commitment* assunti col Canada all'interno del CETA.

Un autore, tuttavia, ipotizza il seguente scenario: la Corte di giustizia potrebbe, un domani, invalidare la Decisione 2002/2/CE, magari per ragioni simili a quelle affrontate in riferimento agli Stati Uniti [17]; non si dimentichi, infatti, che il Canada è (come gli stessi USA), uno dei «Cinque Occhi» («*Five Eyes*»), un gruppo ristretto di Paesi impegnati in programmi di sorveglianza di massa [18].

---

[15] Fra tali disposizioni, a titolo meramente esemplificativo, si possono menzionare l'art. 28.3 del CETA, l'art. 7.50 dell'EUKOR, l'art. 8.3 dell'EPA col Giappone e l'art. 8.53 del FTA col Vietnam. In dottrina, con particolare riferimento all'art. 7.50 dell'EUKOR, v.: A. WESSEL, *Broken data protection in EU trade agreements*, cit., par. 2; con particolare riferimento all'art. 8.53 del FTA col Vietnam v.: A. WESSEL, *Weak Data Protection in EU-Vietnam Trade Agreement*, cit..

[16] UE, Decisione della Commissione 2002/2/CE *conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)*, 20 dicembre 2001, GU L 2, 4 gennaio 2002, pp. 13-16.

[17] A. WESSEL, *CETA: ISDS and data protection*, cit..

[18] Sul punto, v.: A. WESSEL, *CETA and mass surveillance*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 13 aprile 2016.

Dopo l'annullamento, vi sarebbero ovviamente dei negoziati per riuscire a trovare in tempi rapidi una soluzione; ma se ciò non fosse possibile, nello scenario estremo prospettato, le autorità di protezione dei dati dell'UE potrebbero arrivare a sospendere, ai sensi del GDPR [19], i flussi di dati personali verso il Canada [20]. A questo punto, tale Stato potrebbe attivare il meccanismo previsto dal Capo 29 del CETA, lamentando una violazione dei *data flows commitments* assunti dall'Unione. Prescrivendo – lo si è visto – le disposizioni in materia di protezione dei dati personali e della *privacy* contenute nel CETA un livello di tutela inferiore rispetto a quello richiesto dalla Corte di giustizia, il collegio arbitrale ben potrebbe dar ragione al Canada nella sua relazione finale: l'Unione dovrebbe dunque dare esecuzione alla stessa; in caso contrario, il Canada avrebbe il diritto di sospendere i propri obblighi o di ricevere una compensazione.

C'è di più. Qualora gli articoli della Sezione F del Capo 8 del CETA fossero entrati in vigore al momento dei fatti ipotizzati, gli investitori canadesi nel settore dei servizi finanziari potrebbero avviare contro l'Unione europea la procedura ISDS ivi disciplinata [21]. Tali investitori potrebbero lamentare una violazione dell'art. 8.10, che impegna l'UE ad accordare a investimenti e investitori un «trattamento giusto ed equo» [22]: permettere, all'interno del CETA, i flussi transfrontalieri di dati personali nel settore dei servizi finanziari sulla base dello standard di protezione dell'art. 13.15 e poi sospendere i flussi sulla base di uno standard di protezione più elevato potrebbe essere qualificato come un «comportamento manifestamente arbitrario» (in presenza del quale l'obbligo di trattamento giusto ed equo risulta violato) [23]. Si potrebbe inoltre ritenere che l'Unione abbia ingenerato legittime aspettative, sulle quali l'investitore abbia fatto affidamento nel decidere se realizzare o mantenere l'investimento, e poi le abbia deluse, circostanza di cui si può tenere conto nel valutare se vi sia stata una violazione dell'art. 8.10 CETA [24]. Alla luce di tali considerazioni, il Tribunale CETA potrebbe dar ragione agli investitori [25], condannando l'Unione europea al risarcimento del danno [26]. Il rischio di simili conseguenze, inoltre, non fini-

[19] UE, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio *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)*, 27 aprile 2016, GU L 119, 4 maggio 2016, pp. 1-88, art. 58 («Poteri»), par. 2, lett. j).

[20] A. Wessel, *CETA: ISDS and data protection*, cit..

[21] Si precisa infatti che l'art. 13.21 del CETA, in materia di «Controversie in materia di investimenti nei servizi finanziari», rinvia proprio al Capo 8 del medesimo accordo.

[22] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra*, cit., art. 8.10 («Trattamento degli investitori e degli investimenti disciplinati»), par. 1.

[23] *Ibid*., par. 2, lett. c).

[24] *Ibid*., par. 4.

[25] A. Wessel, *CETA: ISDS and data protection*, cit..

[26] UE, *Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e*

rebbe del tutto neanche dopo un'eventuale denuncia del CETA: quest'ultimo prevede infatti che, in caso tale accordo cessi di avere efficacia, «le disposizioni di cui al capo 8 (Investimenti) continuano a produrre effetti per un periodo di 20 anni dopo la data della denuncia […] per quanto riguarda gli investimenti realizzati prima di tale data»[27].

1.2. *Le ricadute sul piano interno: la pressione su vari attori istituzionali europei*

Si è dunque preso coscienza delle conseguenze giuridiche negative in cui l'UE può incorrere qualora sia ritenuta inadempiente ai *data flows commitments* («espliciti» o «impliciti») assunti a livello internazionale. Orbene, non si può tacere il fatto che il timore di simili conseguenze potrebbe determinare una forte pressione su vari attori istituzionali europei, compromettendo la loro indipendenza nel proteggere i dati personali degli individui.

Si possono fare vari esempi. In primo luogo, le autorità nazionali di controllo potrebbero essere portate a non esercitare il loro potere, attribuito dal poc'anzi rammentato art. 58, par. 2, lett. j), del GDPR, di sospendere o vietare definitivamente i flussi di dati personali verso Paesi terzi, anche là dove questi ultimi non soddisfacessero gli standard di protezione richiesti dal diritto dell'Unione. Inoltre, anche se questo non si è ancora verificato, in futuro la Corte di giustizia potrebbe essere disincentivata dall'annullare ulteriori decisioni di adeguatezza.

Ma, lo si deve dire, i maggiori dubbi riguardano l'operato della Commissione. Quest'ultima, temendo le conseguenze pregiudizievoli che possono derivare da una violazione degli obblighi commerciali, potrebbe essere indotta ad adottare una decisione di adeguatezza pur in assenza di un livello di protezione «sostanzialmente equivalente» a quello UE. Anzi, si hanno ragioni per ritenere che nella realtà dei fatti ciò sia già avvenuto.

Si è anticipato come la Commissione, soprattutto nei confronti di importanti partner commerciali, abbia adottato alcune decisioni di adeguatezza che appaiono motivate prevalentemente da ragioni di carattere economico, anziché dalla presenza nei Paesi in questione di livelli di protezione «sostanzialmente equivalenti» a quelli UE. Proprio per l'impossibilità di valutare come «adeguati» gli ordinamenti di tali Stati terzi, quantomeno nella loro interezza, la Commissione ha fatto ricorso a soluzioni creative, come decisioni settoriali.

Come esempio, innanzitutto, si può citare nuovamente la decisione concernente il Canada, che copre soltanto i trasferimenti a destinatari soggetti al c.d. «PIPEDA» («*Canadian Personal Information Protection and Electronic Docu-*

---

l'Unione europea e i suoi Stati membri, dall'altra, cit., art. 8.39 («Sentenza definitiva»), par. 1, lett. a).

[27] *Ibid*., art. 30.9 («Denuncia»), par. 2.

ments Act»), ovvero organizzazioni del settore privato che rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali; ma anche quella riguardante Israele, che non si applica al trasferimento di dati personali dall'UE verso tale Stato qualora il trasferimento e il successivo trattamento siano effettuati esclusivamente tramite strumenti non automatizzati [28].

Merita inoltre di essere ricordata, in quanto particolarmente emblematica, anche la situazione del Giappone. Con riferimento a tale Paese, in primo luogo, è stato necessario adottare una decisione settoriale [29], che copre esclusivamente i trasferimenti a operatori economici che gestiscono informazioni personali soggetti alla legge detta «APPI» (Legge sulla protezione delle informazioni personali). Ma soprattutto, è stato indispensabile completare l'ordinamento giapponese con delle «Norme integrative», applicabili esclusivamente ai dati personali trasferiti dall'UE; esse, invece, non si applicano ai dati dei singoli in Giappone o provenienti da Paesi diversi da quelli dell'Unione. Un'architettura che – lo si è visto – non convince pienamente né il Comitato europeo per la protezione dei dati [30], né il Parlamento europeo [31], che non si sono espressi favorevolmente sul punto. Le medesime criticità, peraltro, interessano anche la decisione di adeguatezza concernente la Repubblica di Corea [32], anche se con ogni probabilità in misura minore [33].

È stato necessario trovare una soluzione creativa pure nel caso del Regno Unito. La Commissione ha escluso dall'ambito di applicazione della relativa decisione di adeguatezza [34] i trasferimenti di dati personali dall'Unione verso

---

[28] UE, Decisione della Commissione 2011/61/UE *ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte dello Stato d'Israele in relazione al trattamento automatizzato di tali dati*, 31 gennaio 2011, GU L 27, 1° febbraio 2011, pp. 39-42.

[29] UE, Decisione di esecuzione (UE) 2019/419 della Commissione *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone a norma della legge sulla protezione delle informazioni personali*, 23 gennaio 2019, GU L 76, 19 marzo 2019, pp. 1-58.

[30] UE, Comitato europeo per la protezione dei dati, *Parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone*, 5 dicembre 2018.

[31] UE, Risoluzione del Parlamento europeo *sull'adeguatezza della protezione dei dati personali offerta dal Giappone (2018/2979(RSP))*, 13 dicembre 2018.

[32] UE, Decisione di esecuzione (UE) 2022/254 della Commissione *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica di Corea nel quadro della legge sulla protezione delle informazioni personali [notificata con il numero C(2021) 9316]*, 17 dicembre 2021, GU L 44, 24 febbraio 2022, pp. 1-90. Sul punto v.: UE, Comitato europeo per la protezione dei dati, *Parere 32/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nella Repubblica di Corea*, 24 settembre 2021.

[33] Sul punto v.: G. Greenleaf, *The Draft Korea Adequacy Decision: Submission to European Union Authorities*, in *University of New South Wales Law Research Series*, 2021, Numero 52, p. 14.

[34] UE, Regolamento di esecuzione (UE) 2021/1772 della Commissione *a norma del regola-*

il Regno Unito ai quali può applicarsi la troppo ampia «esenzione per motivi di immigrazione» («*immigration exemption*») prevista dalla normativa UK. Ciò al fine di dare una risposta ad almeno alcuni dei rilievi formulati sempre dall'EDPB [35] e dal Parlamento [36].

Facile capire che attestazioni di adeguatezza così strutturate rischiano di sollevare seri problemi sul piano della loro attuazione operativa: ad esempio, nel caso del Giappone vi è la concreta preoccupazione che gli obblighi previsti dalle Norme integrative vengano elusi, mentre in quello del Regno Unito vi è il timore che i dati ivi trasferiti dall'UE possano comunque rientrare, in alcuni casi, nell'ambito di applicazione dell'«*immigration exemption*», circostanza che determinerebbe un'eccessiva compressione dei diritti delle persone interessate [37].

Infine, tra le decisioni di adeguatezza «creative» merita una menzione pure l'*EU-US Data Privacy Framework* [38]: quest'ultimo, proprio come le due precedenti misure riguardanti gli Stati Uniti, consente i trasferimenti di dati personali dall'UE verso le sole organizzazioni statunitensi che abbiano volontariamente aderito a un insieme di principi e, come esposto ancora una volta dall'EDPB, non è di per sé sufficiente a superare definitivamente tutte le criticità presentatesi in passato [39].

Come si è anticipato, l'adozione di decisioni di questo tipo è avvenuta sotto una forte pressione, dovuta al timore di conseguenze sul piano commerciale. Una circostanza che in alcuni casi ha indotto pure a forzare i tempi rispetto al necessario.

Ciò è avvenuto nel caso del Giappone. La Commissione si è affrettata nell'adozione della relativa decisione di adeguatezza, avvenuta il 23 gennaio 2019,

---

mento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito, 28 giugno 2021, GU L 360, 11 ottobre 2021, pp. 1-68.

[35] UE, Comitato europeo per la protezione dei dati, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 13 aprile 2021.

[36] UE, Risoluzione del Parlamento europeo *sull'adeguata protezione dei dati personali da parte del Regno Unito (2021/2594(RSP))*, 21 maggio 2021.

[37] Sul punto v., in riferimento al Giappone: UE, Comitato europeo per la protezione dei dati, *Parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone*, cit., § 30; UE, Risoluzione del Parlamento europeo *sull'adeguatezza della protezione dei dati personali offerta dal Giappone*, cit., § 12. In riferimento al Regno Unito: A. Choromidou, *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS*, in *International Data Privacy Law*, 2021, p. 13.

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

[39] UE, Comitato europeo per la protezione dei dati, *Parere 5/2023 relativo al progetto di decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali nel contesto del quadro per la protezione dei dati UE-USA*, 28 febbraio 2023.

in modo tale che essa precedesse (ancorché di pochi giorni) l'entrata in vigore dell'accordo EPA, avvenuta il 1° febbraio 2019. Ciò ha evitato alla radice che gli obblighi assunti dall'Unione europea potessero essere violati attraverso restrizioni dei flussi di dati personali verso il Giappone. Un simile accertamento dell'adeguatezza, tuttavia, appare frutto di un compromesso, e ha portato taluno ad affermare che, nell'occasione, la Commissione non si sia rivelata indipendente[40]. Commissione che, peraltro, a seguito di un primo riesame della decisione di cui trattasi, ha ritenuto nell'aprile 2023 di confermarla *in toto*[41], operazione su cui l'EDPB non ha mancato di formulare rilievi[42].

Un discorso molto simile deve essere ripetuto pure in riferimento al Regno Unito. Ai sensi del «*Trade and Cooperation Agreement*» (TCA) tra UE e UK[43] – firmato il 30 dicembre 2020, applicato in via provvisoria dal 1° gennaio 2021 ed entrato definitivamente in vigore il 1° maggio 2021[44] – dopo il 30 giugno 2021 le trasmissioni di dati dall'Unione verso il Regno Unito sarebbero state considerabili a tutti gli effetti trasferimenti verso un Paese terzo[45], con la conseguente necessità (là dove fosse mancata una decisione di adeguatezza) di applicare i meccanismi alternativi del Capo V GDPR. Proprio al fine di evitare tale scenario, che avrebbe potuto portare anche a possibili violazioni degli impegni assunti dall'UE all'interno del TCA (su cui a breve si tornerà), la Commissione ha accelerato nell'adozione della decisione di adeguatezza concernente l'UK, che è avvenuta il 28 giugno 2021 (appena due giorni prima della scadenza).

La necessità di adottare simili decisioni in tempi rapidi ha indotto la Commissione non solo (come già illustrato) ad avvalersi di soluzioni creative, sen-

---

[40] A. Wessel, *EU-Japan trade agreement not compatible with EU data protection*, cit..

[41] UE, Relazione della Commissione al Parlamento europeo e al Consiglio *sul primo riesame del funzionamento della decisione di adeguatezza relativa al Giappone*, 3 aprile 2023, COM/2023/275 final; UE, Commissione europea, *Commission Staff Working Document accompanying the document "Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan"*, 3 aprile 2023, SWD/2023/75 final.

[42] UE, Comitato europeo per la protezione dei dati, *Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan*, 18 luglio 2023.

[43] UE, *Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra*, 30 dicembre 2020, GU L 149, 30 aprile 2021, pp. 10-2539.

[44] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «L'accordo sugli scambi commerciali e la cooperazione tra l'UE e il Regno Unito», consultabile al seguente link: *https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_it* (ultimo accesso in data 31 dicembre 2024). Sul punto v. anche: UE, Comitato europeo per la protezione dei dati, *Nota informativa sui trasferimenti di dati verso il Regno Unito ai sensi del regolamento generale sulla protezione dei dati dopo il periodo di transizione*, 15 dicembre 2020, aggiornata il 13 gennaio 2021.

[45] UE, *Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra*, cit., art. 782.

za il ricorso alle quali non sarebbe stata adottabile alcuna misura, ma anche a non tenere in sufficiente conto alcuni aspetti assai critici segnalati dal Comitato europeo per la protezione dei dati e dal Parlamento europeo. Tra questi, spicca soprattutto la questione dell'accesso ai dati personali da parte delle autorità pubbliche dei Paesi terzi per finalità di sorveglianza: una problematica che ha mostrato tutta la sua delicatezza nell'ambito della vicenda *Schrems*, che continua a preoccupare in relazione agli Stati Uniti [46] – pure dopo la prima revisione del *Data Privacy Framework* svolta dalla Commissione nella seconda metà del 2024, con esito positivo [47], permangono infatti secondo l'EDPB aspetti da monitorare [48] – e che risulta particolarmente critica anche con riferimento ad altri Paesi: ad esempio il Regno Unito, ma non solo.

Quanto appena detto permette di svolgere un'ulteriore riflessione. Infatti la Commissione, in ragione del più volte menzionato timore delle conseguenze pregiudizievoli che possono derivare da una violazione degli obblighi commerciali, potrebbe essere indotta anche a non revocare, né modificare o sospendere, una decisione di adeguatezza già adottata, pur non essendo più presente un livello di protezione «sostanzialmente equivalente» a quello UE.

Si possono fare gli esempi delle misure riguardanti Canada e Nuova Zelanda [49]. Tali Stati sono due dei poc'anzi rammentati «Cinque Occhi» o «*Five Eyes*», insieme proprio al Regno Unito e agli Stati Uniti, nonché all'Australia, i.e. Paesi impegnati in programmi di sorveglianza di massa. I loro ordinamenti sono strutturati in maniera tale da garantire la prevalenza delle esigenze di sicurezza dello Stato su quelle di salvaguardia della *privacy* individuale [50]. Sarebbe dunque lecito aspettarsi una certa attenzione, nelle decisioni di adeguatezza concernenti Canada e Nuova Zelanda, alla tematica dell'accesso ai dati personali da parte delle autorità pubbliche. Invece, gli strumenti in esame, adottati nella vigenza della Direttiva 95/46/CE, oltre ad essere datati sono anche estremamente brevi e scarni, soprattutto là dove paragonati a quelli più recenti. Con ogni proba-

---

[46] UE, Comitato europeo per la protezione dei dati, *Parere 5/2023 relativo al progetto di decisione di esecuzione della Commissione europea per quanto riguarda la protezione adeguata dei dati personali nel contesto del quadro per la protezione dei dati UE-USA*, cit..

[47] UE, Relazione della Commissione al Parlamento europeo e al Consiglio *sul primo riesame periodico del funzionamento della decisione di adeguatezza relativa al quadro UE-USA per la protezione dei dati personali*, 9 ottobre 2024, COM/2024/451 final.

[48] UE, Comitato europeo per la protezione dei dati, *EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 4 novembre 2024.

[49] UE, Decisione di esecuzione della Commissione 2013/65/UE a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Nuova Zelanda, 19 dicembre 2012, GU L 28, 30 gennaio 2013, pp. 12-14.

[50] 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*, cit., pp. 756-757. Sul punto v. anche, *inter alios*: A. Wessel, *CETA and mass surveillance*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 13 aprile 2016.

bilità sarebbe opportuno rimetterli in discussione, adottando magari qualche accorgimento ulteriore per assicurarsi in modo ancor più convincente che la sorveglianza delle autorità non determini ingerenze sproporzionate nei diritti degli interessati. Tuttavia, ciò non si è ancora verificato, anzi: a seguito di un primo riesame delle 11 decisioni più risalenti tra quelle in vigore – novero in cui sono dunque comprese anche le due di cui trattasi – la Commissione europea, in data 15 gennaio 2024, ha deciso di confermare in blocco le suddette misure, nessuna esclusa [51]; un'operazione su cui, peraltro, l'EDPB ha espresso alcune riserve [52]. Si ricordi che una revoca della decisione riguardante il Canada potrebbe determinare conseguenze facilmente ipotizzabili, dato che l'Unione europea potrebbe trovarsi a violare alcuni degli obblighi contenuti nel CETA. In riferimento alla Nuova Zelanda – Stato con cui l'UE dopo lunghi negoziati ha recentemente concluso un Accordo di libero scambio [53], firmato il 9 luglio 2023 [54] ed entrato in vigore in data 1° maggio 2024 [55] – vale invece un discorso parzialmente diverso, su cui a breve si tornerà.

In ogni caso, il fatto che, per pressioni derivanti dagli impegni commerciali, vengano adottate – o comunque mantenute in vita – decisioni di adeguatezza nei confronti di Stati che non garantiscono una tutela «sostanzialmente equivalente» a quella dell'Unione, finisce inevitabilmente per compromettere l'approccio proprio della disciplina UE, che intenderebbe accordare una netta prevalenza alle esigenze di protezione dei dati personali. Di conseguenza, finiscono anche per essere pregiudicate le finalità di tale approccio, tra cui anche quella di esportare gli standard UE verso Paesi terzi – il «*Brussels effect*», in breve – con tutto ciò che ne deriva.

---

[51] UE, Relazione della Commissione europea al Parlamento europeo e al Consiglio *sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE*, 15 gennaio 2024, COM/2024/7 final; UE, Commissione europea, *Commission Staff Working Document "Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC" accompanying the document "Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC"*, 15 gennaio 2024, SWD/2024/3 final.

[52] UE, *Comitato europeo per la protezione dei dati, EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC*, 5 dicembre 2024.

[53] UE, *Accordo di libero scambio tra l'Unione europea e la Nuova Zelanda*, 9 luglio 2023, GU L 2024/866, 25 marzo 2024.

[54] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «*EU-New Zealand: Text of the agreement*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en* (ultimo accesso in data 31 dicembre 2024).

[55] Sul punto, si veda la pagina del sito della Commissione europea dedicata a «*The EU-New Zealand trade agreement*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement_en* (ultimo accesso in data 31 dicembre 2024).

Sul punto, a onor del vero, è d'obbligo una considerazione. L'intento di esportare oltrefrontiera il modello UE rischiererebbe di essere compromesso anche nel caso in cui l'Unione cessasse completamente di adottare decisioni di adeguatezza nei confronti di Stati terzi. Le ragioni sono piuttosto semplici: se fosse *de facto* impossibile ottenere un simile provvedimento, i Paesi extra-UE non proverebbero neppure a modificare le proprie normative al fine di innalzare il livello di tutela, rivelandosi tale sforzo inutile. Il modello in questione darebbe prova di non funzionare correttamente e difficilmente altri Stati vorrebbero imitarlo. Anzi, questi ultimi potrebbero addirittura abbracciare modelli diversi, in particolare proprio quelli ben noti dell'OCSE o dell'APEC, che adottano un approccio meno restrittivo e più favorevole alle esigenze commerciali. Proprio per questo, essi sono fortemente promossi dagli Stati Uniti, che intendono così cercare di contrastare il ruolo del GDPR come «*international rule-setter*» attraverso discipline più congeniali alla loro impostazione e alle loro esigenze[56]. Se vuole evitare questo rischio, la Commissione deve dunque continuare a svolgere accertamenti di adeguatezza, e non può invece adottare un atteggiamento tanto rigido da sfociare nell'immobilismo.

Tuttavia, seppur vero, tale ragionamento non può certo giustificare l'adozione di decisioni nei confronti di Stati che di sicuro non garantiscono un livello di protezione «adeguato». In tal caso, la Commissione non solo metterebbe a serio rischio i dati personali degli europei, ma rinuncerebbe del tutto a esportare gli standard UE, consentendo agli Stati terzi di ricevere i flussi anche senza dover innalzare (in misura sufficiente) le proprie tutele[57].

Emblematico è il descritto caso del Giappone. Le «Norme integrative», senza la cui presenza non sarebbe stata possibile l'adozione di alcuna decisione di adeguatezza, si applicano esclusivamente ai dati personali trasferiti dall'UE, e non ai dati dei singoli in Giappone o provenienti da Paesi diversi da quelli dell'Unione. Come si è detto, vi sono seri dubbi che un sistema così strutturato possa funzionare perfettamente nella pratica. Ma ammettendo che funzioni, l'UE ha comunque rinunciato a una piena esportazione dei propri standard in Giappone: il livello più elevato di protezione riguarda esclusivamente i dati "europei", mentre lo Stato in questione può mantenere tutele inferiori in relazione a tutti gli altri dati personali. Mancherebbero dunque le condizioni per il noto «*Brussels effect*», uno dei presupposti del quale è proprio la non divisibilità degli standard, e ciò rende assai improbabile che il quadro giuridico giapponese in materia di protezione dei dati personali si avvicini significativamente a quello UE[58].

---

[56] M. Scott, *Digital Bridge: Transatlantic competition – Washington's privacy plan – Microsoft lobbying*, in *www.politico.eu*, 2 dicembre 2021.

[57] Sul punto v. *inter alios*: C. Kuner, *Protecting EU Data Outside EU Borders Under the GDPR*, in *Common Market Law Review*, 2023, Volume 60, Numero 1, pp. 77-106.

[58] F.Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, in *Harvard Journal of Law & Technology*, 2020, Volume 33, Numero 2, pp. 661-691, spec. 691, secondo cui: «*[…] it is unlikely that Japan will move significantly closer*

Viceversa, nel caso degli Stati Uniti, l'atteggiamento di assoluta intransigenza dimostrato dalla Corte di giustizia potrebbe portare ad alcuni frutti. Già nel 2015, il c.d. «*Freedom Act*» era intervenuto con alcune modifiche, poi non rivelatesi decisive, che cercavano di ridurre i poteri di sorveglianza delle autorità pubbliche. Giungendo a tempi più recenti, dopo la sentenza *Schrems II* sono arrivate da più parti esortazioni a riformare ulteriormente l'ambito in questione [59] e vi sono stati nuovi dialoghi con l'UE che hanno portato all'adozione da parte del Presidente Biden, nell'ottobre 2022, del già citato *Executive Order* che limita le attività di *intelligence*: solo a quel punto, la Commissione europea ha adottato l'*EU-US Data Privacy Framework*. Se l'Unione europea riuscisse davvero a spingere gli USA verso una sostanziale riforma della propria normativa in materia di sorveglianza, si tratterebbe ovviamente di un grande successo del modello UE e del «*Brussels effect*».

Ma al di là di quest'ultimo caso – dove infatti entrambe le precedenti decisioni di adeguatezza sono state annullate dalla Corte e non già revocate dalla Commissione – tutti gli elementi fin qui forniti vanno a sostegno della considerazione svolta in precedenza, che si procede dunque a ripetere e a puntualizzare: non solo si può dire che l'approccio proprio degli accordi commerciali di cui l'UE è parte è completamente diverso rispetto a quello che caratterizza la disciplina interna UE, ma si può anche affermare che il primo dei due approcci rischia concretamente di compromettere il secondo. Infatti, dal momento che gli accordi commerciali godono, sul piano internazionale, di meccanismi preposti alla loro attuazione assai forti, ciò può creare una supremazia *de facto* delle norme di natura commerciale su quelle a tutela dei diritti fondamentali [60]. Temendo le conseguenze derivanti dai meccanismi in questione, vari attori istituzionali, tra cui soprattutto la Commissione, potrebbero essere portati a non ostacolare i flussi di dati personali, evidentemente a discapito delle esigenze di protezione di questi ultimi.

---

towards an EU-style data privacy framework. Therefore, the EU-Japan Adequacy Decision not only represents a new frontier for global data governance, but also the limits of the Brussels Effect and the European vision of promulgating human rights standards worldwide through the GDPR […]».

[59] Sul punto v., *inter alios*: S. Bradford Franklin-L. Sarkesian, *Congress Has the Opportunity to Enact Meaningful Surveillance Reforms Now: Here's How*, in *www.newamerica.org*, 21 febbraio 2020; S. Bradford Franklin, *Rethinking Surveillance on the 20th Anniversary of the Patriot Act*, in *www.justsecurity.org*, 26 ottobre 2021.

[60] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., p. 502.

2. *Le* Horizontal provisions for cross-border data flows and for personal data protection*: una possibile soluzione?*

2.1. *La genesi delle* Horizontal provisions

La necessità di superare le previsioni sui flussi e sulla protezione dei dati personali così come formulate negli accordi commerciali dell'UE visti fin qui è stata evidenziata non solo da parte della dottrina, ma anche a livello istituzionale.

Nel 2016 il Parlamento europeo, nelle sue raccomandazioni alla Commissione sui negoziati relativi al (poi non concluso) Accordo sugli scambi di servizi (TiSA) [61], ha infatti suggerito di utilizzare una formulazione diversa e più robusta nell'ottica della protezione dei dati e della *privacy*, le quali «non sono ostacoli agli scambi, ma diritti fondamentali»; in particolare, ha proposto l'inserimento di «una disposizione orizzontale, autonoma, globale, inequivocabile e giuridicamente vincolante […] che escluda totalmente dall'ambito di applicazione dell'accordo il vigente e futuro quadro giuridico dell'UE sulla protezione dei dati personali, senza alcuna condizione che ne preveda la coerenza con altre parti» dell'accordo stesso [62].

Il concetto è stato poi ulteriormente ribadito, sempre nel 2016, all'interno di una lettera indirizzata da alcuni membri del Parlamento europeo all'allora Presidente della Commissione, Jean-Claude Juncker. Secondo gli autori della stessa, nulla negli accordi commerciali dovrebbe impedire all'Unione di mantenere, migliorare e applicare la sua disciplina in materia di protezione dei dati: le regole dell'UE sui trasferimenti internazionali di dati personali sono cristalline, dotate di solido fondamento e non devono in alcun modo essere diluite [63].

---

[61] UE, Risoluzione del Parlamento europeo *recante le raccomandazioni del Parlamento europeo alla Commissione sui negoziati relativi all'accordo sugli scambi di servizi (TiSA) (2015/2233(INI))*, 3 febbraio 2016. Su tale documento v., *inter alios*: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., p. VI, p. VIII, p. 24, p. 57 e p. 59; A. Wessel, *Broken data protection in EU trade agreements*, cit..

[62] UE, Risoluzione del Parlamento europeo *recante le raccomandazioni del Parlamento europeo alla Commissione sui negoziati relativi all'accordo sugli scambi di servizi*, cit., § 1.c.iii. All'interno del medesimo documento, il Parlamento europeo ha altresì proseguito il ragionamento, sottolineando la necessità di «assicurare che la circolazione di dati personali dei cittadini europei a livello mondiale avvenga nel pieno rispetto delle norme in materia di protezione […] dei dati vigenti in Europa» (§ 1.c.iv), e di «assicurare in particolare che l'UE mantenga la sua capacità di sospendere il trasferimento di dati personali dall'UE verso paesi terzi, qualora le norme del paese terzo interessato non soddisfino gli standard di adeguatezza dell'Unione, le imprese non utilizzino vie alternative, come norme vincolanti d'impresa o clausole contrattuali standard, e qualora le deroghe […] non siano applicabili» (§ 1.c.viii). Di conseguenza, occorre «respingere […] ogni disposizione universale sui flussi di dati che non contenga alcun riferimento al necessario rispetto delle norme in materia di protezione dei dati» (§ 1.c.iv).

[63] UE, Jan Albrecht e altri, *MEPs Data Flows Letter to President Juncker*, 15 December 2016, secondo cui: «*[N]othing in these trade agreements should prevent the EU from maintaining, improv-*

Per riassumere, il Parlamento europeo prima, e alcuni suoi membri poco dopo, hanno sostenuto, partendo dal consueto presupposto in base a cui il diritto alla protezione dei dati personali non dovrebbe essere oggetto di negoziato, la necessità di inserire negli accordi commerciali disposizioni di nuova tipologia: esse dovrebbero essere formulate in modo da non pregiudicare in alcun modo il rispetto del quadro giuridico UE in materia di dati personali; quest'ultimo dovrebbe essere anzi totalmente escluso dall'ambito di applicazione dell'accordo, e nessuna condizione dovrebbe prevederne la coerenza con altre parti dell'accordo medesimo.

Così, in risposta anche a esigenze come quelle prospettate dal Parlamento europeo, il 31 gennaio 2018 la Commissione europea ha promosso un nuovo meccanismo: si tratta delle cosiddette «*Horizontal provisions for cross-border data flows and for personal data protection*» [64], da inserire nei futuri accordi commerciali dell'UE al posto delle disposizioni "vecchio stampo". Frutto del lavoro di un *team* guidato dal Primo Vicepresidente della Commissione Juncker, Frans Timmermans [65], tali clausole orizzontali sono state pubblicate sul sito della Commissione nel maggio 2018 [66] e, nel luglio dello stesso anno, rese disponibili in una versione ulteriormente revisionata nell'ambito dei negoziati relativi all'accordo commerciale con l'Indonesia [67].

Siffatte clausole – come apparirà ancor più chiaro dalla loro analisi – possono essere considerate a tutti gli effetti come figlie della crescente attenzione da parte dell'UE per la *privacy* e la protezione dei dati personali come diritti fondamentali (aspetto già ampiamente affrontato nella presente trattazione), nonché della volontà di rendere gli accordi internazionali dell'Unione più coerenti possibili con gli elevati standard di tutela sanciti dal GDPR [68].

---

ing and applying its data protection rules. Our rules on international transfers of personal data, are crystal clear, well-grounded and must not in any way be diluted. In other words, data protection should not be subject to trade negotiations. It is a fundamental right, not a trade barrier, and as such, it should be fully excluded from these agreements. Accordingly, any commitments on market access and to international standards on cross-border data flows must be very carefully conditioned. We also believe that the WTO exemption for data protection, known as GATS XIV, should be strengthened». Sul punto v.: S. Yakovleva-K. Irion, *Pitching trade against privacy*, cit., p. 219.

[64] UE, Comunicato stampa della Commissione europea, *European Commission endorses provisions for data flows and data protection in EU trade agreements*, 31 gennaio 2018.

[65] *Ibid*.

[66] È possibile reperire le *Horizontal provisions for cross-border data flows and for personal data protection*, nella loro versione del maggio 2018, sulla pagina del sito della Commissione europea ad esse dedicata, consultabile al seguente link: *https://ec.europa.eu/newsroom/just/items/627665/en* (ultimo accesso in data 31 dicembre 2024).

[67] È possibile reperire le clausole orizzontali, nella loro versione del luglio 2018, al seguente link: *https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/363b4081-c535-4d7c-9365-84a64f9dc582/details* (ultimo accesso in data 31 dicembre 2024).

[68] Sul punto v., *inter alios*: S. Yakovleva-K. Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, in *AJIL Unbound*, 2020, Volume 114, pp. 10-14.

2.2. *Il contenuto delle* Horizontal provisions

Nel comunicato stampa del 31 gennaio 2018 sulla promozione delle clausole orizzontali, la Commissione ricorda che i dialoghi in materia di protezione dei dati e i negoziati commerciali con gli Stati terzi, pur potendo essere tra loro complementari, devono seguire due strade separate (così come già affermato nella Comunicazione del 2017 «Scambio e protezione dei dati personali in un mondo globalizzato»). Alla luce di ciò, la Commissione si è interrogata su come promuovere al meglio gli interessi dell'UE nel settore, soprattutto nei casi in cui una decisione di adeguatezza non possa essere realisticamente raggiunta in parallelo rispetto ai negoziati commerciali in corso. Risultato del lavoro sono state, per l'appunto, le *Horizontal provisions*: esse sono finalizzate a consentire all'Unione di contrastare le pratiche protezionistiche dei Paesi terzi, assicurando al tempo stesso che gli accordi commerciali non possano essere utilizzati per intaccare le forti regole UE sulla protezione dei dati personali [69].

Sono dunque presenti, come illustrato, i due consueti obiettivi che ci hanno accompagnato durante tutto il corso della trattazione: l'esigenza di favorire i flussi transfrontalieri di informazioni e la necessità di tutelare i dati degli individui. A tali obiettivi sono dedicati rispettivamente il primo e il secondo articolo delle clausole orizzontali. Vi è, infine, un'ultima disposizione, riguardante la cooperazione sulle questioni attinenti alla regolamentazione del commercio digitale.

La prima caratteristica da enfatizzare in relazione alle clausole in esame, resa particolarmente evidente dalla loro stessa denominazione, è che esse sono «orizzontali», come del resto era stato suggerito anche dal Parlamento europeo nel 2016: ciò vuol dire che esse coprono tutti i settori economici, e non si limitano ad ambiti specifici come i servizi finanziari o di telecomunicazione [70].

Addentrandosi nel merito delle previsioni di cui trattasi, con il primo articolo le parti si impegnano a garantire i flussi transfrontalieri di dati per agevolare gli scambi nell'economia digitale (par. 1). Siamo dunque di fronte, ancora una volta, a un *data flows commitment* simile a quelli incontrati fin qui. In particolare, i flussi tra le parti non possono essere limitati attraverso l'utilizzo di determinate tecniche, oggetto di specifica elencazione (sempre al par. 1) [71]. È altresì

---

[69] UE, Comunicato stampa della Commissione europea, *European Commission endorses provisions for data flows and data protection in EU trade agreements*, cit., secondo cui: «*[…] Dialogues on data protection and trade negotiations with third countries can complement each other but must follow separate tracks […]. The Commission has looked into how best to advance the EU's interests in this area – especially in cases where an "adequacy decision" (recognising an equivalent level of data protection of a third country) cannot be realistically reached in parallel to ongoing trade negotiations […]. The draft text would allow the EU to tackle protectionist practices in third countries, while ensuring that such trade agreements cannot be used to challenge the strong EU rules on the protection of personal data […]*».

[70] Sul punto v., *inter alios*: F. VELLI, *op. cit.*, p. 892.

[71] Nello specifico, prescrivere l'utilizzo di strutture di calcolo o di elementi di rete nel territorio della parte per l'elaborazione dei dati (anche imponendo l'impiego di strutture

previsto un meccanismo di riesame della disposizione in questione (par. 2)[72].

Ancora più interessante è però il secondo articolo delle *Horizontal provisions*, dedicato all'altra delle due esigenze contrapposte. Innanzitutto, ciascuna parte riconosce che la protezione dei dati personali e della *privacy* è un diritto fondamentale, e che standard elevati a tale proposito contribuiscono alla fiducia nell'economia digitale e allo sviluppo degli scambi (par. 1). Ma la disposizione chiave è quella in base a cui ciascuna parte può adottare e mantenere in vigore le garanzie che essa ritiene appropriate per assicurare la protezione dei dati personali e la *privacy*, anche adottando e applicando regole sui trasferimenti transfrontalieri di dati personali (par. 2). Si può fin da subito notare come la previsione oggetto di analisi sia formulata come un'eccezione rispetto alla regola generale e non come un obbligo positivo, segnando da questo punto di vista un ritorno a uno schema più simile a quello dell'*Understanding* e dell'*Annex*. Tuttavia, a differenza di ciò che avviene in tali strumenti, il ricorso a tale eccezione non è subordinato a rigide condizioni, come la circostanza che la misura adottata sia «necessaria» alla realizzazione dell'interesse perseguito o il fatto che essa non abbia finalità elusive dell'accordo[73]. Al contrario, lo si ripete, ciascuna parte può adottare le garanzie che essa ritiene appropriate («*the safeguards it deems appropriate*»): come l'ha definita qualcuno, si tratta di una «*self-judging exception*»[74], di portata ben più ampia. È inoltre stabilito (sempre al par. 2) che nulla nell'accordo in questione pregiudica la protezione dei dati personali e la *privacy* assicurate dalle rispettive garanzie delle parti. Come era stato suggerito dal Parlamento europeo, la previsione è formulata in modo da non impedire il rispetto del quadro giuridico UE in materia di dati personali, che risulterebbe dunque escluso dagli impegni commerciali assunti dall'Unione[75].

---

di calcolo o di elementi di rete certificati o approvati nel territorio di una parte); esigere la localizzazione dei dati nel territorio della parte per l'archiviazione o l'elaborazione; vietare l'archiviazione o l'elaborazione dei dati nel territorio dell'altra parte; subordinare il trasferimento transfrontaliero di dati all'utilizzo di strutture di calcolo o di elementi di rete nel territorio delle parti o a obblighi di localizzazione nel territorio delle parti. Sul punto v., *inter alios*: S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 219; D. GERAETS-P. VANDER SCHUEREN, *Exporting the EU Privacy Regime Through Trade Instruments?*, in *Mayer Brown*, 19 marzo 2018, par. 2.

[72] Nello specifico, il par. 2 prevede che le parti riesaminino periodicamente l'attuazione della disposizione in questione e ne valutino il funzionamento entro tre anni dall'entrata in vigore dell'accordo nel quale essa è inserita. Stabilisce inoltre che una parte possa in qualsiasi momento proporre all'altra di riesaminare l'elenco delle restrizioni di cui al par. 1 e che tale richiesta debba essere esaminata con debita attenzione.

[73] S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 220, secondo cui: «*[…] The wording goes beyond the existing counterbalancing provisions in the financial and telecommunications sectors in the GATS and as replicated elsewhere, which are subject to a 'necessity' criterion or an anti-circumvention clause […]*».

[74] D. GERAETS-P. VANDER SCHUEREN, *op. cit.*, par. 2.

[75] S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 219, secondo cui: «*[…] the*

Il secondo articolo delle clausole contiene poi altre disposizioni. In particolare, viene imposto a ciascuna parte di informare l'altra in merito alle eventuali garanzie di cui sopra adottate o mantenute in vigore. Viene altresì precisato che, ai fini dell'accordo, con «dato personale» si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile: una definizione perfettamente identica a quella contenuta nel Regolamento (UE) 2016/679 e finalizzata a impedire che le parti attribuiscano alla nozione in questione significati divergenti. Infine, viene stabilito, per maggior certezza, che il sistema giurisdizionale per gli investimenti eventualmente previsto non si applichi alle previsioni contenute nei primi due articoli delle clausole orizzontali. Si eviterebbero così alcuni degli scenari problematici precedentemente prospettati, dal momento che le questioni attinenti alla protezione dei dati personali e alla *privacy* rimarrebbero escluse dalla giurisdizione dell'ICS, mentre le possibili violazioni sarebbero affrontate esclusivamente tra le parti[76].

Infine, non si deve dimenticare il terzo e ultimo articolo delle *Horizontal provisions*, che (come anticipato) concerne la cooperazione sulle questioni attinenti alla regolamentazione del commercio digitale. L'aspetto innovativo non è contenuto nei primi due paragrafi, che prevedono un dialogo tra le parti in materia: simili disposizioni possono essere infatti rinvenute anche in accordi commerciali già conclusi (a titolo puramente esemplificativo, si segnala l'art. 8.52 del FTA col Vietnam). La novità è piuttosto rappresentata dal terzo paragrafo che, per maggior certezza, esclude dalla cooperazione sulla regolamentazione del commercio digitale le regole e le garanzie predisposte da una parte per la protezione dei dati personali e la *privacy*, comprese quelle sui trasferimenti transfrontalieri di dati personali. La *ratio* della previsione è chiaramente quella di impedire alla radice influenze negative o negoziati finalizzati a indebolire lo standard di protezione dei dati dell'Unione europea[77].

In definitiva, la formulazione delle clausole orizzontali rappresenta un indubbio miglioramento rispetto agli articoli contenuti negli accordi commerciali dell'UE visti fin qui. In una lettera a un membro del Parlamento europeo, la Commissione è arrivata ad affermare che tali previsioni, una volta incluse nei futuri accordi commerciali, stabiliranno per la prima volta un chiaro divieto di barriere protezionistiche ai flussi transfrontalieri di informazioni, ma nel pieno rispetto e senza pregiudizio per le regole UE in materia di protezione dei dati personali e *privacy*[78]. Queste ultime vengono infatti escluse dagli impegni com-

---

Commission ultimately accepts the delicacy of excepting the EU data protection acquis from its commitments under trade and investment law that effectively reverses its early stance […]».

[76] Sul punto v.: F. VELLI, *op. cit.*, pp. 892-893.

[77] *Ibid.*, p. 893. Sul punto v. anche: S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 219.

[78] J. FIORETTI, *EU moves to remove barriers to data flows in trade deals*, in *www.reuters.com*, 9 febbraio 2018, in cui si riporta una lettera della Commissione a un membro del Parlamento europeo secondo la quale: «*These horizontal provisions – once included in future trade and invest-*

merciali assunti dell'UE, in ossequio al principio secondo cui i diritti fondamentali, in quanto tali, non possono essere oggetto di negoziato.

Per completezza, occorre menzionare anche il fatto che pure in seno all'OMC, dove dal 2019 sono stati lanciati negoziati per disciplinare l'*e-commerce* a livello globale [79], la Commissione europea aveva assunto un approccio in linea con quello appena descritto: nel «*Joint Statement on Electronic Commerce – EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*» del 26 aprile 2019, la Commissione ha infatti proposto l'adozione di disposizioni in materia di «*Cross-Border Data Flows*» e di «*Protection of Personal Data and Privacy*» pressoché identiche a quelle delle *Horizontal Provisions* [80]. Della sorte di tali negoziati si dirà *infra*.

2.3. *Le* Horizontal provisions *nella prassi: alcuni esempi incoraggianti, con particolare riferimento all'Accordo di libero scambio con la Nuova Zelanda*

Come evidenziato, le clausole orizzontali sono state ideate per essere inserite all'interno degli accordi commerciali negoziati successivamente all'elaborazione delle medesime [81].

Sono vari gli accordi attualmente in via di negoziazione in cui l'UE sta tentando di includere simili articoli [82]: tra questi, possiamo ricordare il già citato

---

ment agreements – will for the first time provide for a straightforward prohibition of protectionist barriers to cross-border data flows, in full compliance with and without prejudice to the EU's data protection and data privacy rules». Sul punto v. anche: D. SCHRIEBERG, *E.U. Hoping New Data Protection Under GDPR Will Have Global Impact*, in *www.forbes.com*, 11 febbraio 2018.

[79] Sul punto v., *inter alios*: M. BURRI, *A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability*, in *Georgetown Journal of International Law*, 2023, Volume 53, pp. 565-625. Si veda anche la pagina del sito del WTO dedicata a «*Joint Initiative on E-commerce*», consultabile al seguente link: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm* (ultimo accesso in data 31 dicembre 2024); nonché la pagina del sito della Commissione europea dedicata a «*State of play of WTO negotiations on e-commerce, investment facilitation and services domestic regulations*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-meetings-civil-society/state-play-wto-negotiations-e-commerce-investment-facilitation-and-services-domestic-regulations-2023-03-07_en* (ultimo accesso in data 31 dicembre 2024).

[80] WTO, *Joint Statement on Electronic Commerce – EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce – Communication from the European Union*, 26 aprile 2019, INF/ECOM/22, § 2.7 («*Cross-Border Data Flows*»).

[81] Sul punto v.: D. GERAETS-P. VANDER SCHUEREN, *op. cit.*; S. YAKOVLEVA-K. IRION, *Pitching trade against privacy*, cit., p. 219; S. YAKOVLEVA, *Personal Data Transfers in International Trade and EU Law*, cit., p. 889.

[82] Sul punto v., *inter alios*: M. BURRI, *Cross-border data flows and privacy in global trade law: has trade trumped data protection?*, in *Oxford Review of Economic Policy*, 2023, Volume 39, Numero 1, pp. 85-97; E. FAHEY, *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?*, in *European Papers*, 2023, Volume 8, Numero 2, pp. 503-511; L.

Free Trade Agreement con l'Indonesia, negoziato a partire dal 18 luglio 2016 [83]; quello con l'Australia, i cui negoziati sono stati autorizzati il 22 maggio 2018 [84]; ma anche l'accordo di libero scambio globale e approfondito con la Tunisia, i negoziati del quale erano stati lanciati già il 13 ottobre 2015 [85].

L'UE, inoltre, sta cercando di integrare le *Horizontal provisions* anche nei rapporti con Stati con cui sono già in vigore accordi commerciali (peraltro, già analizzati), inserendo dette disposizioni in separati *Digital Trade Agreements* [86]: a tal riguardo, occorre citare i casi riguardanti Corea del Sud [87] e Singapore [88] (con quest'ultimo paese, i negoziati si sono conclusi in data 25 luglio 2024 [89]), salutati con favore anche dal Garante europeo della protezione dei dati [90].

Brännström, *Global Inequality and the EU International Law Position on Cross-Border Data Flows*, in *Nordic Journal of International Law*, 2023, Volume 92, pp. 119-137.

[83] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Indonesia*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/indonesia/* (ultimo accesso in data 31 dicembre 2024).

[84] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Australia*», consultabile al seguente link: *https://ec.europa.eu/trade/policy/countries-and-regions/countries/australia/* (ultimo accesso in data 31 dicembre 2024).

[85] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Tunisia*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/tunisia_en* (ultimo accesso in data 31 dicembre 2024).

[86] Sui *Digital Trade Agreements*, v. *inter alios*: M. Burri-A. Chander, *What Are Digital Trade and Digital Trade Law?*, in *AJIL Unbound*, 2023, Volume 117, pp. 99-103; M. Burri-K. Kugler, *Regulatory autonomy in digital trade agreements*, in *Journal of International Economic Law*, 2024, Volume 27, Numero 3, pp. 397-423. Si veda anche la pagina del sito della Commissione europea dedicata ai medesimi, consultabile al seguente link: *https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade/digital-trade-agreements_en* (ultimo accesso in data 31 dicembre 2024).

[87] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU-South Korea Free Trade Agreement and Digital Trade Agreement*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/south-korea/eu-south-korea-agreements_en* (ultimo accesso in data 31 dicembre 2024).

[88] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU-Singapore Free Trade Agreement, Investment Protection Agreement and Digital Trade Agreement*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreements_en* (ultimo accesso in data 31 dicembre 2024).

[89] Sul punto vi veda la pagina del sito della Commissione europea dedicata a «*EU and Singapore conclude negotiations for landmark Digital Trade Agreement*», consultabile al seguente link: *https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3982* (ultimo accesso in data 31 dicembre 2024).

[90] UE, Garante europeo della protezione dei dati, *Opinion 18/2023 on the Recommendation for a Council Decision authorising the opening of negotiations for digital trade disciplines with the Republic of Korea and with Singapore*, 15 maggio 2023.

Ma c'è di più. Le clausole orizzontali, infatti, sono già state effettivamente inserite nel testo definitivo di alcuni accordi. In particolare, ci si riferisce all'*Interim Trade Agreement* con il Cile, firmato in data 13 dicembre 2023 [91], ma soprattutto al già citato Accordo di libero scambio con la Nuova Zelanda, il quale (come si è detto) è già in vigore dal 1° maggio 2024 [92]. Con riferimento a quest'ultimo accordo, esso contiene infatti articoli che riproducono piuttosto fedelmente le *Horizontal provisions* elaborate nel 2018: segnatamente, l'art. 12.4 sui «Flussi transfrontalieri di dati» [93] e l'art. 12.5 sulla «Protezione dei dati personali e della vita privata» [94].

Si tratta di un elemento da salutare con indubbio favore. Riprendendo il ragionamento svolto poc'anzi, nella – per ora remota – ipotesi in cui la decisione di adeguatezza concernente la Nuova Zelanda fosse invalidata o revocata e i flussi di dati personali verso tale Stato fossero sospesi, grazie alle citate disposizioni l'Unione europea avrebbe maggior facilità a mettersi al riparo dalle conseguenze negative precedentemente prospettate: le regole UE in materia di protezione dei dati personali e *privacy* non sono infatti pregiudicate dagli impegni commerciali assunti dall'UE nell'accordo. Una circostanza che va indubbiamente a beneficio dell'indipendenza dei vari attori istituzionali europei nel proteggere i dati personali degli individui.

Quanto appena visto, sia negli accordi in via di negoziazione che in quelli conclusi, risulta peraltro pienamente in linea con quelli che sono i mandati indirizzati dal Consiglio alla Commissione: a differenza di quanto avveniva in passato, troviamo ora esplicitamente affermato il fatto che le regole UE in materia di protezione dei dati personali non possono essere né negoziate né intaccate e la legislazione UE non può essere pregiudicata («*[…] while neither negotiating nor affecting the EU's personal data protection rules and without prejudice to the EU legislation […]*») [95].

---

[91] Sul punto si veda la pagina del sito della Commissione europea dedicata a «*EU trade relationships by country/region – Countries and Regions – Chile*», consultabile al seguente link: *https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/chile_en* (ultimo accesso in data 31 dicembre 2024).

[92] Sull'Accordo di libero scambio dell'UE con la Nuova Zelanda, v. *inter alios*: M. Burri-K. Kugler-A.D. Ker, *Digital Trade in the EU–New Zealand Free Trade Agreement: An Appraisal*, in *Legal Issues of Economic Integration*, 2024, Volume 51, Numero 1, pp. 11-46.

[93] UE, *Accordo di libero scambio tra l'Unione europea e la Nuova Zelanda*, cit., art. 12.4 («Flussi transfrontalieri di dati»).

[94] *Ibid.*, art. 12.5 («Protezione dei dati personali e della vita privata»).

[95] In riferimento all'Accordo di libero scambio con l'Australia v.: UE, Consiglio dell'Unione europea, *Documento 7663/18*, 8 maggio 2018, reso pubblico il 25 giugno 2018, p. 13. In riferimento all'Accordo di libero scambio con la Nuova Zelanda v.: UE, Consiglio dell'Unione europea, *Documento 7661/18*, 8 maggio 2018, reso pubblico il 25 giugno 2018, p. 13.

2.4. *Le* Horizontal provisions *nella prassi: le criticità perduranti, con particolare riferimento al caso del TCA con il Regno Unito* (segue)

Nonostante gli apprezzabili passi avanti appena descritti, tuttavia, la questione appare tutt'altro che chiusa. È infatti lecito nutrire ancora alcuni dubbi circa le clausole orizzontali e, nello specifico, circa il fatto che esse vengano effettivamente inserite negli accordi commerciali con tutti gli Stati terzi.

A titolo esemplificativo, si può innanzitutto rammentare il fatto che alcuni dei trattati precedentemente analizzati, come quello col Vietnam, sono stati firmati dopo la promozione, da parte della Commissione, delle *Horizontal provisions*. Queste ultime, avrebbero ben potuto essere inserite nei rispettivi testi, ma ciò non si è verificato, ed è stata invece mantenuta la più debole formulazione "vecchio stampo": secondo taluno, «ciò è frustrante, dal momento che la Commissione sa come fare meglio» [96].

Ma ancor più preoccupante è il fatto che, in alcuni accordi, vengono inseriti articoli apparentemente ispirati alle clausole orizzontali, ma che differiscono da queste ultime proprio in aspetti essenziali.

Un primo esempio è rappresentato dalle previsioni recentemente integrate nell'EPA con il Giappone, a cui si è già fatto parziale cenno. L'originario art. 8.81 dell'accordo prevedeva che le parti valutassero in seguito la necessità di inserire nell'EPA medesimo ulteriori disposizioni relative ai flussi di dati [97]. Queste ultime sono state effettivamente inserite con il successivo accordo UE-Giappone sui flussi transfrontalieri di dati, concluso in data 23 ottobre 2023 ed entrato in vigore il 1° luglio 2024. Ora, l'art. 8.81 – nella sua nuova formulazione [98] – e l'art. 8.82 – inserito invece *ex novo* [99] – contengono disposizioni corrispondenti, rispettivamente, al primo e al secondo articolo delle *Horizontal provisions*: un chiaro miglioramento rispetto alla situazione previgente [100], soprattutto rispetto al rimosso art. 8.63, le cui criticità sono già state messe in evidenza. Tuttavia, non si può non notare come i due nuovi articoli presentino pure alcune rilevanti

---

[96] Sul punto v., proprio con riferimento al FTA col Vietnam: A. WESSEL, *Weak Data Protection in EU-Vietnam Trade Agreement*, cit., secondo cui: «*[…] The proposed EU-Vietnam trade agreement contains weak safeguards for data protection […] This is all the more frustrating as the EU commission knows how to do better […]*». La traduzione riportata nel testo è a opera dello scrivente.

[97] UE, *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, cit., art. 8.81 («Libera circolazione dei dati»).

[98] L'art. 8.81 dell'EPA tra UE e Giappone, nella sua nuova formulazione, è dedicato a «*Cross-border transfer of information by electronic means*».

[99] L'art. 8.82 dell'EPA tra UE e Giappone, inserito all'interno di tale accordo successivamente, è dedicato a «*Protection of Personal Data*».

[100] Sul punto v.: UE, Garante europeo della protezione dei dati, *Opinion 17/2022 on the Recommendation for a Council Decision authorising the opening of negotiations for the inclusion of provisions on cross-border data flows in the Agreement between the European Union and Japan for an Economic Partnership*, 9 agosto 2022.

differenze rispetto alle clausole orizzontali: l'art. 8.82, in particolare, non afferma in modo altrettanto netto che l'accordo non pregiudica le regole in materia di protezione dei dati personali e *privacy* delle parti. Una differenza di cui il Garante europeo della protezione dei dati si è particolarmente rammaricato nel suo Parere del 10 gennaio 2024 [101].

Ancor più emblematico, nonché problematico, è tuttavia il caso del *Trade and Cooperation Agreement* (TCA) tra UE e Regno Unito, in vigore dal 1° maggio 2021, di cui già si è fatta menzione nella presente trattazione. Anche all'interno di tale strumento vi sono disposizioni corrispondenti al primo e al secondo articolo delle *Horizontal provisions*; si tratta, rispettivamente, degli articoli 201 [102] e 202 [103].

Se il testo dell'art. 201 è piuttosto fedele a quello del primo articolo delle clausole orizzontali, lo stesso non può certo dirsi per l'art. 202: esso, al contrario, si discosta dal secondo articolo delle *provisions* proprio negli aspetti più importanti, ragion per cui è stato fortemente criticato sempre dal Garante europeo della protezione dei dati nel suo Parere del 22 febbraio 2021 sulla conclusione dell'accordo commerciale UE-UK [104].

All'interno dello stesso, il GEPD ricorda innanzitutto che l'Unione non dovrebbe assumere alcun impegno commerciale incompatibile con la propria legislazione interna in materia di *data protection*, e che i dialoghi sulla protezione dei dati e i negoziati commerciali, seppur complementari, devono seguire strade separate: i flussi di dati verso Stati terzi, di conseguenza, possono essere consentiti solo là dove si utilizzino i meccanismi previsti dalla normativa UE [105]. Proprio per questo, il Garante accoglie con favore le *Horizontal provisions* pro-

---

[101] UE, Garante europeo della protezione dei dati, *Opinion 3/2024 on the signing and conclusion on behalf of the European Union, of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data*, 10 gennaio 2024, § 19, secondo cui: *«The EDPS regrets that the legal wording of the Horizontal provisions was modified in the Protocol. In particular, the EDPS is concerned that the Protocol, in its current wording, could - contrary to the negotiating directives contained in the Recommendation - affect the EU's personal data protection rules and the possibility for the EU to, in duly justified cases, enact measures that would require controllers or processors to store personal data in the EU/EEA».*

[102] UE, *Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra*, cit., art. 201 («Flussi transfrontalieri di dati»).

[103] *Ibid*., art. 202 («Protezione dei dati personali e della vita privata»).

[104] UE, Garante europeo della protezione dei dati, *Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement*, 22 febbraio 2021.

[105] *Ibid*., § 14, secondo cui: «*[…] The Union cannot and should not embark on any international trade commitments that are incompatible with its domestic data protection legislation. Dialogues on data protection and trade negotiations with third countries can complement each other but must follow separate tracks. Personal data flows between the EU and third countries should be enabled by using the mechanisms provided under the EU data protection legislation*».

mosse dalla Commissione nel 2018, che rappresentano la miglior soluzione possibile per preservare i diritti fondamentali dell'individuo alla protezione dei dati personali e della *privacy*: esse raggiungono un buon compromesso, dal momento che consentono all'Unione di contrastare le pratiche protezionistiche dei Paesi terzi, assicurando al contempo che gli accordi non siano utilizzati per intaccare il livello elevato di protezione garantito dalla Carta di Nizza e dalla legislazione UE; inoltre, come affermato ripetutamente dalla Commissione, tali clausole orizzontali non sono pensate per essere oggetto di negoziato [106].

Proprio alla luce di tali premesse, il Garante si rammarica del fatto che la formulazione delle clausole sia stata modificata all'interno del TCA [107], segnatamente nel suo articolo 202. Innanzitutto, fa notare come il par. 1 di tale articolo non attribuisca al «diritto alla protezione dei dati personale e della vita privata» l'aggettivo «fondamentale» [108]. Ma soprattutto evidenzia che a essere completamente trasfigurato è il par. 2, ovvero quello che nella presente trattazione era stata definito come la disposizione chiave delle *provisions*. Esso, infatti, si limita a prevedere la mera possibilità per una parte di adottare o mantenere in vigore «misure», senza aggiungere «che essa ritiene appropriate» o formule analoghe. Tale possibilità, inoltre, risulta condizionata: le misure possono essere adottate purché la legislazione della parte preveda strumenti che «consentano» i trasferimenti a condizioni di applicazione generale [109] per la protezione dei dati trasferiti [110]. Infine, è totalmente assente una formula che renda chiaro che nulla nell'accordo pregiudica la protezione dei dati personali e la *privacy* assicurate

---

[106] *Ibid*., § 15, secondo cui: «*The EDPS supports the horizontal provisions endorsed by the European Commission in 2018, as the best outcome achievable to preserve individual's fundamental rights to data protection and privacy. The horizontal provisions reach a balanced compromise between public and private interests as they allow the EU to tackle protectionist practices in third countries in relation to digital trade, while ensuring that trade agreements cannot be used to challenge the high level of protection guaranteed by the Charter and the EU legislation on the protection of personal data. Furthermore, the Commission has repeatedly stated that negotiation these horizontal provisions are not up for negotiation*».

[107] *Ibid*., § 16, secondo cui: «*The EDPS therefore regrets that the legal wording of the horizontal provisions was modified in the TCA […]*».

[108] *Ibid*., secondo cui: «*[…] not referring to the right to data protection as a* fundamental *right […]*».

[109] Come precisato nella nota n. 34 del TCA: «A fini di chiarezza, l'espressione «condizioni di applicazione generale» si riferisce alle condizioni formulate in termini oggettivi che si applicano orizzontalmente a un numero non precisato di operatori economici e che pertanto riguardano una serie di situazioni e di casi».

[110] UE, Garante europeo della protezione dei dati, *Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement*, cit., § 16, secondo cui l'articolo in questione: «*[…] merely reaffirms the possibility for a Party to adopt or maintain measures on the protection of personal data or privacy, including on cross-border data transfers, but conditioned on providing for 'instruments enabling transfers under conditions of general application for the protection of personal data'[…]*».

dalle rispettive garanzie delle parti [111]. Alla luce di ciò, il Garante europeo della protezione dei dati conclude sul punto affermando che l'art. 202, par. 2, del TCA non salvaguarda pienamente il modo in cui l'Unione europea regolamenta la protezione dei dati personali e la *privacy* [112], costringendo la stessa UE a dover giustificare il proprio quadro giuridico in materia [113].

Il GEPD segnala altresì che, mentre il terzo e ultimo articolo delle clausole orizzontali esclude dalla cooperazione sulle questioni attinenti alla regolamentazione del commercio digitale le regole e le garanzie predisposte da una parte per la protezione dei dati personali e la *privacy*, comprese quelle sui trasferimenti transfrontalieri di dati personali, al contrario l'art. 7, par. 4, lett. h), del TCA prevede che il Consiglio di partenariato, comprendente rappresentanti di UE e UK, rivolga alle parti raccomandazioni proprio sul trasferimento di dati personali [114].

Per tutte le ragioni esposte, l'*European Data Protection Supervisor* si dice preoccupato: le disposizioni del TCA creano incertezza circa la possibilità per l'Unione di applicare in modo pieno e autonomo le proprie regole interne in materia di *Data protection*, in particolare con riguardo ai trasferimenti di dati personali nelle sue relazioni con il Regno Unito [115], senza che da ciò derivino conseguenze potenzialmente pregiudizievoli sul piano internazionale per la stessa UE. A parziale giustificazione, si può anche dire che il TCA è basato su un rapporto assolutamente unico tra Unione e UK e che la normativa in materia di protezione dei dati personali del Regno Unito presenta notevoli somiglianze con quella dell'UE. Tali circostanze non valgono però per nessun altro partner commerciale dell'Unione: il GEPD auspica quindi che la formulazione contenuta nel TCA rimanga un'assoluta eccezione, e che la Commissione non si discosti dal testo delle *Horizontal provisions* in nessun altro contesto [116].

---

[111] *Ibid.*, § 17, secondo cui: «*In addition, the provision no longer states that '[n]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards' […]*».

[112] *Ibid.*, § 16, secondo cui l'articolo in questione: «*[…] does not fully safeguard* how *the EU regulates the protection of personal data and privacy* […]».

[113] *Ibid.*, § 17, secondo cui: «*[…] the wording of the TCA does not seem to prevent the EU from having to pass strict trade tests to justify its measures safeguarding the fundamental rights to privacy and personal data protection […]*».

[114] *Ibid.*, § 19.

[115] *Ibid.*, § 20, secondo cui: «*The EDPS is concerned that these provisions create uncertainty as to the possibility for the EU to autonomously apply fully its domestic rules on personal data protection, in particular as regards transfers of personal data in its relation to the UK*».

[116] *Ibid.*, § 21, secondo cui: «*At the same time, the EDPS understands that the TCA is based on a unique relationship between the EU and the UK. Also, UK data protection law to a large extent mirrors EU data protection law, at the time of the adoption of this opinion, which is not the case for other EU trading partners. Therefore, the EDPS underlines that the wording agreed with the UK on data protection and privacy must remain an exception and insists that the Commission should remain committed to the horizontal provisions*».

Il fatto che gli articoli del TCA siano privi di elementi essenziali delle clausole orizzontali, peraltro, ha sollevato forti critiche anche in dottrina: secondo taluno, ad esempio, tale assenza è rivelatrice della limitata influenza della posizione dell'UE in materia di flussi transfrontalieri di dati [117].

Deve essere altresì menzionato che qualcosa di simile a quanto illustrato in riferimento al TCA si è verificato, *mutatis mutandis*, anche con riguardo alle regole dell'OMC sull'*e-commerce*: nello «*stabilised text*» a cui i partecipanti sono addivenuti in data 26 luglio 2024 sono presenti articoli in materia di «*Personal Data Protection*»; essi, tuttavia, differiscono proprio negli elementi chiave dalle disposizioni proposte dall'UE il 26 aprile 2019, che – come si è detto sopra – ricalcavano assai fedelmente le *Horizontal Provisions* [118].

Si può dunque concludere la presente parte della trattazione affermando che le clausole orizzontali rappresenterebbero un indubbio passo avanti. Con il loro utilizzo si potrebbe, se non risolvere, quantomeno mitigare la gran parte delle criticità delle previsioni contenute nei precedenti accordi commerciali. Ci si riferisce, con ciò, non solo alle criticità relative alla formulazione di tali disposizioni, che come si è visto risulta particolarmente debole per vari motivi, ma anche a quelle che sono state definite come criticità derivanti dalla «semplice presenza» di articoli in materia di flussi e protezione dei dati personali negli accordi commerciali. Tale presenza, infatti, risulta di dubbia legittimità nei casi in cui le parti vadano a contrattare un diverso livello di protezione dei dati personali rispetto a quello assicurato dalla disciplina UE. Al contrario non risulta problematica l'esistenza di una disposizione che serva proprio a escludere, dagli impegni commerciali assunti dall'Unione, il quadro giuridico UE in materia di dati personali, garantendo che esso non venga pregiudicato: in quest'ultimo caso è infatti rispettato il principio secondo cui la protezione dei dati personali e la *privacy*, in quanto diritti fondamentali, non possono essere negoziati.

Tuttavia, proprio l'ampiezza dell'eccezione contenuta nelle clausole orizzontali può indurre a temere possibili abusi, consistenti in vere e proprie barriere ai flussi di informazioni [119]. Perciò, non è affatto scontato che le controparti dell'Unione europea accettino sempre e comunque il testo delle *Horizontal provisions* senza modifiche, circostanza che induce a non essere eccessivamente ottimisti sull'efficacia di tale strumento.

---

[117] L. Brännström, *op. cit.*, p. 128, secondo cui l'assenza nel TCA tra UE e Regno Unito di un'eccezione ampia come quella delle *Horizontal provisions* «*[…] is revealing of the limited influence of the EU position on cross-border data transfers*».

[118] WTO, *Joint Statement Initiative on Electronic Commerce*, 26 luglio 2024, INF/ECOM/87, art. 16 («*Personal Data Protection*») e art. 25 («*Personal Data Protection Exception*»).

[119] Sul punto v.: F. Velli, *op. cit.*, p. 893; S. Yakovleva-K. Irion, *Pitching trade against privacy*, cit., pp. 219-220.

CONCLUSIONI

CONCLUSIONI

È ora possibile tentare di svolgere alcune considerazioni che vadano a riassumere, nonché soprattutto a concludere, la presente trattazione.

L'interesse per i flussi transfrontalieri di dati personali è giustificato da una serie di fattori che sono stati illustrati nell'introduzione di questo lavoro. Nell'ambito della trasformazione digitale dell'economia mondiale attualmente in corso, infatti, l'importanza che i dati e i flussi degli stessi assumono per le imprese è in costante crescita. Ciò vale indubbiamente per quelle aziende che fanno dei dati le loro risorse più preziose («*data-enabled businesses*»), come i colossi del digitale (Google, Amazon, Facebook, Apple, Microsoft); ma vale anche per attività di tipo più tradizionale («*data-enhanced businesses*»), pure quelle di piccole e medie dimensioni. Un fenomeno che va ovviamente di pari passo con l'incessante sviluppo di nuove tecnologie, come quelle di intelligenza artificiale, il cui carburante è rappresentato proprio dai dati.

I flussi possono coinvolgere varie tipologie di dati. Tuttavia, nella presente trattazione si è deciso di prendere in esame esclusivamente quelli concernenti i dati *personali*, ovvero quelle informazioni riguardanti persone fisiche identificate o identificabili. Non si tratta di una scelta casuale: da un lato, i dati personali – in quanto tali – sono estremamente preziosi per l'attività di un'impresa; dall'altro lato, essendo per l'appunto riferibili a una persona fisica, il loro trattamento e trasferimento fa sorgere problemi di tutela della stessa: rischiano infatti di essere intaccati alcuni suoi diritti consacrati in strumenti giuridici di vario rango, in particolare i diritti alla *privacy* e alla protezione dei dati di carattere personale.

Per quanto riguarda il diritto alla *privacy* (o alla vita privata, o alla riservatezza), le cui radici vengono generalmente ricondotte al contesto statunitense di fine XIX secolo, esso offre una tutela "negativa", "statica", limitandosi a escludere i terzi dalla conoscenza di vicende strettamente personali e familiari, mantenendo riservate alcune informazioni. Esso ha trovato riconoscimento in varie fonti a livello internazionale; guardando specificamente al contesto europeo, lo si trova codificato all'art. 8 della CEDU, nonché all'art. 7 della Carta dei diritti fondamentali dell'Unione europea.

Il diritto alla protezione dei dati personali, invece, offre una tutela "positiva", "dinamica", concretizzandosi in poteri di controllo e di intervento che seguono i dati nella loro circolazione. Nel panorama internazionale, è stato introdotto con l'art. 8 della Carta di Nizza, in cui, per certi aspetti, appare come un diritto fondamentale innovativo, mentre per altri, a ben vedere, non risulta poi così

nuovo. Gli elementi che lo costituiscono affondano infatti le radici in strumenti precedentemente esistenti, sia a livello UE, segnatamente la Direttiva 95/46/CE, sia a livello internazionale, come la Convenzione 108 del Consiglio d'Europa (1981) e le Linee guida OCSE (1980). La novità della Carta di Nizza sta nel fatto che simili elementi devono essere ora tutelati in quanto componenti di un diritto fondamentale che merita protezione di per sé.

Tali diritti, dunque, possono essere messi a serio rischio dai trasferimenti oltrefrontiera di dati personali. Ciò si verifica, in particolar modo, quando vi è la possibilità che lo Stato di destinazione accordi ai diritti in questione una tutela inferiore rispetto al Paese da cui il flusso ha avuto origine. Tale circostanza fa inevitabilmente sorgere delle preoccupazioni circa le sorti delle informazioni trasmesse e può indurre a prevedere determinati limiti e condizioni a simili trasferimenti.

Proprio per questo sono stati elaborati strumenti giuridici di vario tipo che hanno come obiettivo proprio quello di bilanciare le due istanze contrapposte: da un lato, l'esigenza di favorire i *cross-border flows of personal data*, in ragione della loro rilevanza strategica per l'espansione del commercio internazionale; dall'altro lato, la necessità di tutelare i diritti degli individui, segnatamente quelli alla *privacy* e alla *personal data protection*, limitando quegli stessi flussi. Tale bilanciamento può essere effettuato con tecniche normative che presentano tra di loro significative differenze, privilegiando in alcuni casi la prima delle due esigenze menzionate, in altri la seconda.

Nella presente trattazione, tuttavia, interessava una specifica disciplina in materia di trasferimenti oltrefrontiera di dati personali: quella adottata dall'Unione europea. Essa è stata debitamente analizzata, in questo lavoro, con l'obiettivo di rispondere a un preciso interrogativo: ci si è infatti mossi per comprendere se l'UE riesca – attraverso gli strumenti da essa predisposti per regolamentare i flussi di dati personali che originano nel suo territorio e sono diretti verso Stati terzi – a trovare un equilibrio ottimale tra le due esigenze che vengono in gioco oppure se, nei fatti, finisca per privilegiarne una a scapito dell'altra. In tale seconda ipotesi, diventava poi importante capire quale delle due istanze prevalesse e quale fosse sacrificata, quali fossero le ragioni di ciò e quali invece le possibili conseguenze di tale approccio.

Orbene, si ritiene di aver fornito sufficienti elementi per provare a rispondere a tale interrogativo. Ciò, tuttavia, non prima di averlo ulteriormente scomposto in due distinti quesiti.

In primo luogo, infatti, è stato opportuno capire il modo con cui la disciplina unilateralmente adottata dall'Unione europea in materia di trasferimenti di dati personali verso Stati extra-UE – per come delineata dal legislatore nel Regolamento (UE) 2016/679, interpretata dalla Corte di giustizia nelle sue sentenze, nonché attuata dalla Commissione nei suoi atti (decisioni di adeguatezza e non solo) – va a bilanciare la necessità di proteggere i dati personali con quella di favorire i flussi dei medesimi.

In secondo luogo, è stato indispensabile interrogarsi circa determinati obblighi internazionali di natura commerciale, concernenti sia in generale la liberalizzazione dei servizi che in modo più specifico la tematica dei trasferimenti di dati, assunti dall'UE. Si è dovuto infatti comprendere se essi siano coerenti con il bilanciamento poc'anzi menzionato e, in caso contrario, se può esservi un impatto di qualche tipo su quest'ultimo.

CAPITOLO I

CONSIDERAZIONI RIEPILOGATIVE SULL'ATTUALE DISCIPLINA INTERNA UE: LA PREVALENZA DELLE ISTANZE DI PROTEZIONE DEI DATI PERSONALI

SOMMARIO: 1. L'evoluzione che ha portato all'attuale disciplina UE e la sua *ratio* ispiratrice: rafforzare il diritto fondamentale alla protezione dei dati personali. – 2. Gli strumenti dell'attuale disciplina UE: un dato normativo, una giurisprudenza e una prassi applicativa che privilegiano le esigenze di protezione dei dati. – 3. Gli obiettivi dell'attuale disciplina UE: impedire l'elusione del GDPR, nonché esportare gli standard UE con finalità di tipo strategico

Per quanto riguarda il primo dei due quesiti in cui è stato scomposto l'interrogativo principale della trattazione, si può tentare di rispondere attraverso gli elementi forniti all'interno della prima parte del presente lavoro. Questa si è concentrata preliminarmente sulla genesi della disciplina interna UE in materia di flussi transfrontalieri di dati personali: sono stati dunque presi in esame gli strumenti di diritto internazionale che hanno preceduto – e influenzato – l'Unione europea nel settore, i.e. le Linee guida dell'OCSE e la Convenzione 108 del CoE; la prima normativa UE in materia, ovverosia la Direttiva 95/46/CE; nonché le trasformazioni nell'ordinamento dell'UE che hanno portato all'adozione del quadro giuridico attuale. Subito dopo, la trattazione si è occupata proprio dell'attuale disciplina unilateralmente adottata dall'UE in materia di flussi transfrontalieri di dati personali – contenuta nel ben noto Regolamento (UE) 2016/679 o GDPR – e degli strumenti ivi previsti: la decisione di adeguatezza, le garanzie adeguate e le deroghe in specifiche situazioni. Infine, sono stati indagati gli obiettivi che una simile disciplina mira a raggiungere.

Alla luce di quanto esposto in tale parte della trattazione, ad avviso di chi scrive è possibile affermare che la disciplina unilateralmente adottata dall'Unione europea in materia di trasferimenti di dati personali verso Stati extra-UE – per come delineata dal legislatore nel GDPR, per come interpretata dalla Corte di giustizia nelle sue sentenze (soprattutto), ma anche per come attuata dalla Commissione attraverso l'adozione di certi atti – effettua un'opera di bilanciamento in cui le esigenze di protezione dei dati personali prevalgono chiaramente su quelle di carattere commerciale. Una simile affermazione è motivata da considerazione di vario tipo, che si andranno ora a raccogliere in breve.

1. *L'evoluzione che ha portato all'attuale disciplina UE e la sua* ratio *ispiratrice: rafforzare il diritto fondamentale alla protezione dei dati personali*

A) In primis, è necessario riproporre alcune riflessioni concernenti il cammino che ha condotto all'attuale disciplina UE in materia di flussi di dati personali verso Stati terzi.

Il quadro giuridico UE in esame affonda le proprie radici in due importanti strumenti di diritto internazionale che, oltretutto, assumono particolare rilievo poiché rappresentano alla perfezione altrettanti approcci adottabili nella regolamentazione dei trasferimenti oltrefrontiera di dati personali e, dunque, nel bilanciamento tra le esigenze commerciali e quelle di protezione dei dati personali. Tali strumenti sono, ovviamente, le Linee guida dell'OCSE, datate 1980 (non vincolanti, ma estremamente influenti) e la Convenzione 108 del Consiglio d'Europa del 1981 (giuridicamente vincolante). Entrambi gli strumenti, giova ricordarlo, sono stati modernizzati più di recente: nel 2013 è stata adottata una versione aggiornata delle *OECD Guidelines* (anch'essa non vincolante), mentre nel 2018 ha visto la luce la Convenzione 108+ (che, tuttavia, nel momento in cui si scrive non è ancora entrata in vigore).

Quanto alle Linee guida dell'OCSE, esse dettano una regolamentazione della materia dei flussi che può essere definita «dal basso verso l'alto», o «*bottom-up regulatory design*». La tecnica normativa utilizzata, inoltre, rappresenta una perfetta espressione di quello che è denominato approccio «su base organizzativa», o «*organizationally-based approach*» (altrimenti detto «*accountability approach*»). Il risultato è una disciplina che, nel bilanciamento tra esigenze contrapposte, sacrifica la tutela dei diritti degli individui a vantaggio della promozione dei trasferimenti oltrefrontiera di dati personali, tanto importanti per l'espansione del commercio internazionale. L'impostazione delle Linee guida OCSE ha altresì ispirato la Cooperazione economica Asia-Pacifico (APEC) nell'elaborazione del suo «*Privacy Framework*» (del 2005, aggiornate nel 2015).

Discorso diverso per la Convenzione 108 del CoE, strumento giuridicamente vincolante che, seppur concepito in un contesto regionale, ha aspirazione universale, potendo essere ratificato anche da Paesi non europei. La Convenzione (*rectius*, il suo Protocollo addizionale del 2001), con riferimento ai trasferimenti verso Stati non parte, detta una regolamentazione «dall'alto verso il basso», o «*top-down regulatory design*». Inoltre, il fatto che ai Paesi non parte venga richiesto un livello «adeguato» di protezione è tipico dell'approccio «su base geografica», o «*geographically-based approach*» (che si contrappone all'«*accountability approach*»). La conseguenza è una disciplina che appare indubbiamente più attenta alle esigenze di tutela dei dati personali che non a quelle di carattere economico.

B) Le Linee guida OCSE e la Convenzione 108, dunque, disciplinano la mate-

ria dei flussi transfrontalieri di dati personali in modi profondamente diversi, che fanno sì che il bilanciamento tra le note esigenze contrapposte abbia esiti differenti. Allo stesso tempo, nonostante le divergenze quanto ai trasferimenti oltrefrontiera, tali strumenti hanno anche molti aspetti in comune e dettano principi in gran parte corrispondenti [1], in ragione del dialogo estremamente proficuo instauratosi tra le due organizzazioni. Orbene, i principi in questione hanno finito per influenzare profondamente la successiva disciplina dell'Unione europea in materia di protezione e libera circolazione dei dati personali. Nel 1995, infatti, anche l'UE ha adottato uno strumento nel settore: si tratta, ovviamente, della Direttiva 95/46/CE.

Tale strumento, pur avendo due «obiettivi gemelli», ovvero la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, enfatizzava maggiormente proprio quest'ultimo aspetto. La Direttiva aveva infatti come base giuridica l'art. 100 A del Trattato CE, disposizione che consentiva l'adozione di misure aventi per oggetto «l'instaurazione ed il funzionamento del mercato interno», e poneva l'accento sulla strumentalità della disciplina in materia di protezione dei dati personali alle esigenze degli scambi intracomunitari: il livello di tutela doveva essere il più possibile equivalente in tutti i Paesi UE proprio nell'ottica di permettere una circolazione dei dati senza ostacoli.

Guardando come i due obiettivi menzionati venivano perseguiti, si deve dire innanzitutto che, per tutelare le persone fisiche con riguardo al trattamento dei dati personali, la Direttiva dettava (come anticipato) principi che erano in gran parte corrispondenti a quelli delle Linee guida OCSE e della Convenzione 108 del CoE, nonché altre norme (e.g. sulle autorità di controllo nazionali e sul Gruppo di lavoro «Articolo 29»).

Per quanto invece riguarda il secondo obiettivo, si proibiva agli Stati UE di restringere o vietare la libera circolazione dei dati personali tra di loro per motivi connessi alla tutela dei diritti delle persone fisiche. Come risulta evidente, dunque, la «libera circolazione» a cui la Direttiva 95/46/CE dedicava una posizione tanto centrale era soprattutto quella tra Stati membri dell'Unione. Vi erano però anche disposizioni, seppur non particolarmente approfondite, sui flussi di dati personali verso Paesi terzi; esse dettavano sul punto una disciplina simile a quella menzionata parlando del CoE: i trasferimenti verso Stati extra-UE erano vietati, a meno che tale Stato non garantisse un livello di protezione «adeguato»; figuravano poi alcune eccezioni.

---

[1] Tra i principi che possono essere rinvenuti fin dalle origini tanto nelle Linee guida OCSE del 1980 che nella Convenzione 108 del 1981, si possono ricordare i principi di liceità e correttezza; il principio secondo il quale le finalità del trattamento devono essere determinate; i principi in base a cui i dati devono essere pertinenti rispetto a tali finalità, nonché esatti e aggiornati; la necessità di adottare adeguate misure di sicurezza; la facoltà per la persona interessata di esercitare una serie di diritti, come il diritto a ottenere certe informazioni, il diritto di accesso, il diritto di rettifica o cancellazione e il diritto di disporre di una possibilità di ricorso.

C) Dopo aver ripercorso il cammino che ha portato dai primi strumenti di diritto internazionale all'originaria disciplina adottata dall'Unione, ci pare utile ricordare in questa sede anche l'evoluzione che ha avuto luogo nello stesso ordinamento dell'UE e che ha condotto all'elaborazione della disciplina attuale.

Dopo l'adozione della Direttiva, la protezione dei dati, nata come uno strumento funzionale alla creazione del mercato interno («*market-building device*»), ha ricevuto una crescente attenzione nella sua qualità di diritto fondamentale. Ciò principalmente grazie all'avvento della Carta di Nizza – il cui art. 8 sancisce la protezione dei dati di carattere personale come vero e proprio diritto fondamentale – e all'entrata in vigore del Trattato di Lisbona, in seguito al quale l'art. 16 TFUE fornisce una base giuridica *ad hoc* per l'adozione (con la procedura legislativa ordinaria) di una normativa in materia di dati personali: non vi è quindi più la necessità di utilizzare come fondamento disposizioni sull'instaurazione e il funzionamento del mercato interno.

In uno scenario così mutato, la Direttiva si è presto dimostrata non più idonea: dopo la firma del Trattato di Lisbona, le istituzioni UE hanno avvertito il bisogno, anche alla luce degli sviluppi tecnologici, di un nuovo quadro giuridico per rafforzare i diritti delle persone – coerentemente con l'importanza che il diritto alla protezione dei dati personali stava assumendo nell'UE – e per ottenere più armonizzazione. Tra gli elementi meno convincenti della Direttiva, peraltro, figuravano proprio le regole sui trasferimenti di dati personali verso Stati terzi, scarne e lacunose, che causavano una notevole disparità tra gli approcci degli Stati membri. Pareva insomma opportuna una disciplina più dettagliata, che rendesse più chiare le regole sui trasferimenti.

Così, nel 2012 la Commissione ha presentato la propria Proposta per un Regolamento generale sulla protezione dei dati, profondamente influenzata anche dal fatto che, dopo il Trattato di Lisbona, era diventata competente in materia DG JUST, più sensibile verso i consumatori che non verso il mercato: una conseguenza pratica della maggior attenzione nei confronti della protezione dei dati nella sua dimensione di diritto individuale. Al termine di un lungo e complesso *iter legis*, ha finalmente visto la luce il Regolamento (UE) 2016/679.

2. *Gli strumenti dell'attuale disciplina UE: un dato normativo, una giurisprudenza e una prassi applicativa che privilegiano le esigenze di protezione dei dati*

Una volta aver compreso l'evoluzione che ha portato all'attuale disciplina UE in materia di protezione dei dati personali e flussi dei medesimi, nonché la *ratio* che l'ha ispirata, ci si è dunque concentrati su tale quadro giuridico.

A) Innanzitutto, per quanto riguarda il GDPR nel suo insieme, è noto che esso rafforza notevolmente – attraverso un gran numero di istituti – la posizio-

ne delle persone i cui dati vengono trattati, in linea con l'importanza assunta nell'UE dalla protezione dei dati personali come diritto fondamentale. Rimane comunque centrale anche l'aspetto della libera circolazione dei dati personali all'interno dell'UE, che viene incentivata con vari meccanismi.

Giungendo finalmente ai trasferimenti di dati personali verso Paesi terzi – nozione non definita espressamente dal Regolamento e su cui, nonostante interventi della Corte di giustizia e del Comitato europeo per la protezione dei dati, permangono alcune incertezze – il Capo V del GDPR ricalca l'impostazione della Direttiva 95/46/CE, sancendo così un «divieto con deroghe». In linea di principio vi è un divieto di trasmettere dati personali fuori dall'Unione. I trasferimenti diventano però consentiti in presenza di un *numerus clausus* di condizioni: si tratta della decisione di adeguatezza, che la Commissione adotta nei confronti di un Paese terzo; delle garanzie adeguate, strumenti di natura contrattuale tra cui spiccano le clausole contrattuali tipo (SCC) e le norme vincolanti d'impresa (BCR); e delle deroghe in specifiche situazioni, come il consenso dell'interessato e la necessità del trasferimento a determinati fini.

Il GDPR fa dunque uso di quella tecnica di regolamentazione dei flussi di dati personali che può essere definita «dall'alto verso il basso»: si parte da un elevato livello di protezione e lo si diminuisce solo a certe condizioni. Inoltre, il meccanismo principale contemplato dalla normativa (la decisione di adeguatezza), dal momento che richiede al Paese terzo di garantire un livello «adeguato» di protezione per poter essere destinatario di flussi, è un classico esempio di approccio «su base geografica».

Il fatto che vengano adoperate tali tecniche normative è certamente un indizio di un quadro giuridico più attento all'esigenza di proteggere i dati personali degli individui anziché a quella di favorire i flussi per ragioni di carattere commerciale. Tuttavia, tale elemento non è decisivo di per sé: anche la Direttiva 95/46/CE poteva essere considerata un esempio di «*top-down regulatory design*» e di «*geographically-based approach*»; nonostante ciò, la disciplina dei trasferimenti verso Stati terzi risultava piuttosto trascurata, circostanza da cui derivava una disparità tra i Paesi UE nel bilanciamento degli interessi in gioco.

Si è dunque arrivati a concludere che la disciplina UE in materia di flussi predilige le esigenze di protezione rispetto a quelle economiche solo al termine di un'indagine ben più approfondita dei singoli strumenti contemplati dal GDPR. Un'analisi che non ha riguardato solo il testo normativo così come adottato dal legislatore, ma anche la pertinente giurisprudenza della Corte di giustizia, nonché gli atti di implementazione della Commissione.

B) Partendo dalla decisione di adeguatezza, e segnatamente dal dato testuale del GDPR, si è notato immediatamente come le regole dettate da quest'ultimo siano ben più complete e dettagliate rispetto a quelle della Direttiva.

Una simile disciplina è coerente con la più volte menzionata valorizzazione della protezione dei dati personali nella sua dimensione di diritto fondamentale. Il rafforzamento della posizione delle persone interessate ottenuto nel GDPR,

infatti, sarebbe vanificato se fosse possibile sfuggire agevolmente alle regole UE trasferendo i dati personali verso Paesi terzi. La regolamentazione dei flussi deve dunque impedire che i medesimi possano compromettere l'elevato livello di tutela assicurato nell'UE e, perciò, assume un'importanza centrale e risulta estremamente approfondita.

Tale disciplina ha assunto una connotazione perfino più marcata grazie all'operato del Gruppo di lavoro «Articolo 29» (e poi del CEPD), secondo cui uno Stato terzo per essere «adeguato» deve applicare certi principi fondamentali propri della normativa UE; ma soprattutto grazie alla giurisprudenza della Corte di giustizia, che ancor più autorevolmente ha riempito di significato il termine «adeguatezza». Secondo la Corte, infatti, tale nozione esige che lo Stato extra-UE assicuri un livello di protezione «sostanzialmente equivalente» a quello garantito nell'UE dalla pertinente normativa letta alla luce della Carta di Nizza. In altre parole, valorizzando gli articoli 7 e (soprattutto) 8 della Carta, il Giudice di Lussemburgo compie un'opera di innalzamento del parametro di «adeguatezza» in uno di «sostanziale equivalenza»: un'interpretazione che privilegia le esigenze di tutela delle persone fisiche, anche a costo di sacrificare le ragioni economiche.

Si rammenta che tale lettura ha portato, nell'ambito della vicenda *Schrems*, a valutare *de facto* l'ordinamento degli Stati Uniti alla luce dei principi caratterizzanti quello dell'Unione. A conclusione di una simile valutazione, si è ritenuto che il contenuto essenziale dei diritti sanciti dalla Carta di Nizza fosse pregiudicato dalla normativa USA in materia di sorveglianza a fini di sicurezza nazionale. Come ulteriore conseguenza, le due decisioni di adeguatezza «*Safe Harbor*» (del 2000) e «*Privacy Shield*» (del 2016) sono state annullate dalla Corte, rispettivamente con la sentenza *Schrems I* del 6 ottobre 2015 e con la sentenza *Schrems II* del 20 luglio 2020. La giurisprudenza *Schrems*, occorre ricordarlo, non è di certo isolata rispetto al resto dell'operato della Corte: al contrario, essa si colloca in un ricco filone giurisprudenziale nel cui ambito la protezione dei dati ha finito costantemente per prevalere sulle esigenze contrapposte, tra cui quelle di sicurezza e, per l'appunto, quelle economiche.

Tornando dunque alla decisione di adeguatezza, ai sensi del GDPR e (soprattutto) della giurisprudenza della Corte, essa richiede quindi uno standard di protezione elevatissimo. Ciò la rende estremamente difficile da adottare: nel momento in cui si scrive, la Commissione, all'interno della quale la Direzione generale competente è DG JUST, ha indirizzato tale misura solamente nei confronti di 15 Stati extra-UE. Si tratta di Paesi che sono strettamente integrati con l'Unione europea e i suoi Stati membri (Svizzera, Guernsey, Isola di Man, Jersey, Isole Fær Øer e Andorra), di Stati che qualche anno fa hanno avuto un ruolo di pioniere nell'elaborazione di leggi sulla protezione dei dati nella loro regione (Uruguay e Nuova Zelanda), oppure di importanti partner commerciali dell'UE (Canada, Argentina, Israele, Giappone, Regno Unito, Repubblica di Corea e, dopo l'adozione di una terza decisione di adeguatezza nel 2023, Stati Uniti). Per altri Paesi, invece, il procedimento di valutazione da parte della Commissione – magari dopo essersi protratto per anni – non ha avuto esito positivo (e.g. per

Australia, Marocco, Principato di Monaco); molti di più, inoltre, neppure tentano di ottenere una decisione, consci presumibilmente delle difficoltà che incontrerebbero nel vedere il loro livello di protezione riconosciuto come «adeguato».

In buona sostanza, la decisione di adeguatezza, per come configurata nel Regolamento (UE) 2016/679, per come interpretata dalla Corte di giustizia e per come (tendenzialmente) applicata dalla Commissione, si rivela uno strumento che privilegia le esigenze di protezione dei dati rispetto a quelle degli scambi commerciali.

C) L'indagine, tuttavia, non si è certo fermata alle decisioni di adeguatezza. Un'ipotetica interpretazione dei meccanismi alternativi che ne consentisse un ampio utilizzo, senza richiedere una tutela elevata, modificherebbe l'impostazione della disciplina nel senso opposto a quello visto finora.

Il passaggio successivo è stato dunque un esame, partito ancora una volta dal testo del GDPR, delle garanzie adeguate di natura contrattuale. Sul punto si può dire in primo luogo che esse presentano dei limiti intrinseci che le rendono utilizzabili solo in situazioni circoscritte.

Le clausole contrattuali tipo, oltre a determinare un aumento dei costi transattivi, sono altresì anelastiche, essendo adottate dalla Commissione europea (o da questa approvate) e non potendo essere modificate dalle parti. Al contrario, le clausole contrattuali *ad hoc*, stipulate in autonomia dalle parti, necessitano di una specifica approvazione da parte dell'autorità nazionale competente, circostanza che non le rende particolarmente affidabili.

Quanto alle norme vincolanti d'impresa, dovendo essere presenti svariate condizioni, nonché un controllo da parte dell'autorità competente, sono assai limitate: possono essere adoperate solo in un gruppo e non con società terze; richiedono tempi di approvazione considerevoli; presentano costi non trascurabili. Discorso pressoché analogo per i codici di condotta e per i meccanismi di certificazione.

Infine, gli strumenti tra autorità pubbliche giovano ben poco alle imprese, che interessano ai fini della presente trattazione.

Anche in questo caso, tuttavia, non si può giungere a conclusioni certe sulle garanzie adeguate senza aver prima considerato anche la giurisprudenza della Corte. E dal suo studio ci si è resi conto che essa – completando un dato normativo che già di per sé sembra non voler consentire l'utilizzo delle garanzie per trasferimenti massicci di dati – va a stabilire che tali strumenti possono essere adoperati solo qualora sia assicurato uno standard estremamente elevato di protezione.

Infatti la Corte, sempre nella sentenza *Schrems II*, afferma che pure le garanzie adeguate devono assicurare che i dati trasferiti godano di un livello di protezione «sostanzialmente equivalente» a quello UE; ciò può richiedere l'adozione, da parte del titolare o del responsabile del trattamento, di misure supplementari. Là dove invece non sia comunque possibile ottenere la protezione richiesta, il titolare o il responsabile, o in subordine l'autorità di controllo competente, deve sospendere o porre fine al trasferimento di dati. In sostanza, il Giudice di

Lussemburgo mira a evitare che le clausole contrattuali tipo vengano utilizzate dalle società commerciali come mere finzioni giuridiche e le rende a tutti gli effetti delle «mini-decisioni di adeguatezza».

L'impostazione della Corte, lo si rammenta, è stata ulteriormente corroborata da due Raccomandazioni del Comitato europeo per la protezione dei dati, nonché dalla Decisione di esecuzione (UE) 2021/914 in materia di clausole contrattuali tipo, adottata dalla Commissione il 4 giugno 2021.

Così come le decisioni di adeguatezza, pure le garanzie adeguate – stando al dato testuale del Regolamento, all'interpretazione del Giudice di Lussemburgo, nonché agli atti della Commissione (e non solo) – devono essere dunque considerate come strumenti che prediligono le esigenze di protezione, anche a discapito di quelle commerciali.

D) Le deroghe in specifiche situazioni, infine, sono pensate per situazioni in cui nel Paese terzo verso cui i dati sono destinati non vi è un livello di protezione adeguato, ma i rischi per la persona sono relativamente ridotti, oppure altri interessi prevalgono sul diritto alla protezione dei dati: si tratta, insomma, di una "valvola di sicurezza".

Tuttavia, ciò richiede che esse siano interpretate restrittivamente, non potendo fornire un quadro adeguato in caso di trasferimenti ripetuti o strutturali di dati personali; sarebbe altrimenti contraddetta la loro natura eccezionale. Ciò emerge dal testo del GDPR, che prevede varie restrizioni al loro utilizzo, ma è stato puntualizzato anche dal Gruppo di lavoro «Articolo 29» e (poi) dal Comitato, nonché soprattutto dalla costante giurisprudenza della Corte: in base a quest'ultima, tutte le deroghe ai diritti fondamentali devono operare entro i limiti dello stretto necessario.

Anche per le deroghe in specifiche situazioni sono dunque riproponibili le medesime riflessioni già svolte sulle decisioni di adeguatezza, nonché sulle garanzie adeguate.

3. *Gli obiettivi dell'attuale disciplina UE: impedire l'elusione del GDPR, nonché esportare gli standard UE con finalità di tipo strategico.*

È stata dunque motivata l'affermazione in base a cui la disciplina unilateralmente adottata dall'UE in materia di trasferimenti di dati personali verso Stati terzi predilige, nel bilanciamento, le esigenze di tutela dei diritti rispetto a quelle di carattere commerciale.

Tale impostazione ha molteplici finalità. In primo luogo, lo si ripete, le istituzioni UE vogliono impedire che il livello di tutela delle persone fisiche garantito nell'Unione sia compromesso da trasferimenti dei loro dati verso Paesi terzi. In assenza di una disciplina dei flussi tanto rigorosa, infatti, l'irrobustimento dei diritti compiuto nel Regolamento sarebbe vanificato.

Ma sono presenti pure altre finalità. L'UE ha anche l'esplicito obiettivo di esportare i propri elevati standard verso un numero più ampio possibile di Paesi terzi. Se questi ultimi vogliono consentire alle imprese e alle altre entità presenti sul proprio territorio di ricevere dati personali dall'UE e di avere accesso al mercato europeo, devono infatti adottare e implementare efficacemente legislazioni rispettose dei più importanti principi UE in materia di protezione dei dati personali.

Si tratta di un aspetto del c.d. «*Brussels effect*», i.e. l'influenza sulle normative di Stati terzi che l'UE esercita unilateralmente grazie alla propria posizione centrale nell'economia globale. Un fenomeno qui possibile in ragione della presenza di certe condizioni: un mercato interno di grandissime dimensioni, un'efficace capacità di regolamentazione, una certa rigidità degli standard, il fatto che la regolamentazione sia rivolta a obiettivi «anelastici» (i «*data subjects*») e la «non divisibilità» degli standard.

L'intenzione di esportare gli standard UE in materia di *personal data protection* era presente fin dalle origini ed è stata una delle ragioni che ha portato all'adozione del nuovo quadro giuridico. Orbene, i risultati raggiunti sul punto sono già ad ora significativi: come sostenuto sia dalla Commissione, che da importanti autori, la normativa UE è davvero diventata un punto di riferimento a livello internazionale e ha ispirato un consistente numero di Paesi nell'elaborazione delle rispettive discipline.

Si deve altresì precisare che vi sono varie modalità attraverso cui l'UE esporta verso gli Stati terzi, e verso i soggetti ivi ubicati, i propri standard in materia di protezione dei dati personali. Non si deve ad esempio trascurare il ruolo dell'art. 3 GDPR, che richiede direttamente alle singole entità ubicate in Paesi extra-UE, le quali abbiano come *target* il mercato europeo o comunque i soggetti che si trovano nell'UE, di conformarsi alle norme del Regolamento. La finalità ultima è dunque, ancora una volta, l'estensione di tutele oltre i confini del territorio europeo. Tale estensione, inoltre, può avvenire non solo unilateralmente (attraverso gli istituti del GDPR), ma anche sfruttando strumenti di tipo multilaterale: proprio in quest'ottica, l'UE sta promuovendo quanto possibile la diffusione della Convenzione 108+ del Consiglio d'Europa.

L'esportazione dei principi UE verso Stati terzi ha, a propria volta, varie finalità. *In primis*, vi è l'intento di promuovere i diritti fondamentali a livello globale, in linea con gli obiettivi dell'azione esterna UE: essa si prefigge infatti di promuovere nel resto del mondo i principi che hanno informato la creazione, lo sviluppo e l'allargamento dell'Unione (art. 21 TUE).

Ma, in secondo luogo, vi è anche una finalità di tipo strategico: tentare di conferire un vantaggio competitivo alle imprese europee rispetto alle concorrenti extra-UE. Le prime, infatti, possono mantenere il loro approccio in materia di protezione dei dati, mentre le seconde sono costrette a conformarsi agli standard UE, sostenendo a tal fine costi non indifferenti. Altrimenti, non potrebbero ricevere e trattare i dati degli europei, del cui valore economico beneficerebbero le sole imprese dell'Unione.

In buona sostanza, il conflitto tra esigenze di tutela dei diritti fondamentali e istanze di carattere commerciale presenta in realtà contorni molto più complessi: anche dietro la limitazione dei flussi, infatti, si celano considerazioni economiche, consistenti nella volontà di proteggere le imprese europee dall'agguerrita concorrenza di società statunitensi e di altri Paesi terzi.

Fin qui, dunque, è stato ricapitolato l'approccio della disciplina UE, nonché le finalità del medesimo. Non si può tuttavia non ricordare che, dall'indagine svolta, sono emersi anche certi elementi che potrebbero rappresentare delle crepe nella costruzione descritta, rischiando di comprometterla. Infatti, è vero che la Commissione è stata in genere parsimoniosa nell'adozione delle decisioni di adeguatezza e che diverse di tali misure non presentano problemi significativi; ma è anche vero che talune decisioni, riguardanti specialmente importanti partner commerciali dell'UE, sollevano criticità: esse sembrano motivate più da ragioni economiche che dalla presenza di livelli di protezione «adeguati». Ciò ha richiesto l'elaborazione di soluzioni creative, come decisioni settoriali (ci si riferisce a casi come quelli di Canada, Israele, Giappone, Regno Unito, Repubblica di Corea, Stati Uniti), che – lo si è visto e lo si ricorderà – possono avere un impatto sul disegno complessivo appena descritto.

Capitolo II

CONSIDERAZIONI RIEPILOGATIVE SUGLI IMPEGNI COMMERCIALI UE: LA PRIMAZIA DELLE ESIGENZE DEGLI SCAMBI E LE RAGIONI PER CUI LA DISCIPLINA INTERNA UE PUÒ RISULTARE COMPROMESSA

Sommario: 1. Gli obblighi OMC alla liberalizzazione dei servizi: il rischio di violazioni del GATS difficilmente giustificabili. – 2. Gli impegni, inseriti in accordi commerciali UE, a consentire i flussi di dati: le criticità delle misure di salvaguardia pensate per controbilanciarli. – 3. Le ragioni per cui l'approccio degli accordi commerciali può compromettere quello della disciplina interna UE.

Dopo aver risposto al primo dei due quesiti in cui è stato scomposto l'interrogativo che permea il presente lavoro, occorre ora concentrarsi sul secondo, a cui si può tentare di rispondere utilizzando gli elementi forniti nella seconda parte della trattazione. Quest'ultima, lo si ricorda, si è occupata di determinati obblighi internazionali di natura commerciale, concernenti sia in generale la liberalizzazione dei servizi che in modo più specifico la tematica dei trasferimenti di dati, assunti dall'Unione europea; ha altresì cercato di comprendere se detti obblighi siano coerenti con l'approccio proprio della disciplina interna UE, nonché se, in caso contrario, possa esservi un impatto di qualche tipo su quest'ultimo.

In virtù di quanto esposto in tale parte della trattazione, si ritiene possibile affermare non solo che gli impegni commerciali assunti dall'UE a livello internazionale attribuiscono una chiara prevalenza alle esigenze degli scambi rispetto a quelle di protezione dei dati, risultando così incoerenti con l'approccio della disciplina interna UE, ma anche che tale approccio rischia conseguentemente di essere compromesso. Si andranno ora a ricapitolare le considerazioni che motivano una simile affermazione.

1. *Gli obblighi OMC alla liberalizzazione dei servizi: il rischio di violazioni del GATS difficilmente giustificabili*

Si parta riproponendo alcune riflessioni riguardanti, in generale, il diritto dell'Organizzazione mondiale del commercio. In tale contesto, assume rilievo

il *General Agreement on Trade in Services*, strumento finalizzato alla liberalizzazione dei servizi: tra tali servizi, infatti, figurano anche quelli forniti in modo transfrontaliero che si sostanziano proprio in flussi di dati. Da qui, l'interesse per l'Accordo in questione.

Ci si è dunque interrogati sulla compatibilità della normativa UE in materia di flussi di dati personali con i rilevanti obblighi del GATS. Si è trattato di vedere, in primo luogo, se la pertinente disciplina del GDPR e le misure adottate ai sensi della stessa (specialmente le decisioni di adeguatezza) rispettino o meno detti obblighi; in secondo luogo, in caso di incompatibilità *prima facie*, se le norme UE possano essere giustificate ai sensi di una delle eccezioni dello stesso GATS. Un'opera di indagine in cui si sono rivelati assai utili alcuni rapporti degli organi OMC.

A) Per prima cosa, si è verificata la compatibilità della normativa UE con gli obblighi generali, partendo dalla clausola della nazione più favorita (art. II GATS). Orbene, la disciplina dell'Unione in materia di trasferimenti oltrefrontiera di dati personali accorda ai servizi e prestatori di alcuni membri dell'OMC (quelli non destinatari di una decisione di adeguatezza) un trattamento meno favorevole rispetto a quello accordato a servizi e prestatori «analoghi» di altri Stati (che invece beneficiano di una simile misura): una violazione della clausola in esame, almeno *prima facie*, è dunque configurabile.

Sono altresì ipotizzabili infrazioni delle norme in materia di regolamentazione interna (segnatamente, dell'art. VI.1), dal momento che la prassi della Commissione nell'adozione delle decisioni di adeguatezza non è sempre ragionevole, obiettiva e imparziale.

Giungendo agli impegni specifici, è stato preliminarmente ricordato che l'UE ha effettivamente assunto simili impegni anche in settori che implicano il trattamento (e il trasferimento) di dati personali. Premesso ciò, è stato detto come in tali settori potrebbero essere ravvisate violazioni delle norme in materia di trattamento nazionale (art. XVII), nonché, in casi limite, di quelle in materia di accesso al mercato (art. XVI).

B) Dal momento che le norme di diritto UE in materia di flussi (o l'applicazione delle stesse) possono porsi *prima facie* in contrasto con svariati obblighi sanciti all'interno del GATS, si è rivelato necessario interrogarsi sulle possibili giustificazioni.

L'ipotesi dell'integrazione economica potrebbe fornire un aiuto, ma limitatamente a un numero ridotto di situazioni. È stato dunque indispensabile esaminare le eccezioni generali dell'art. XIV. Tale disposizione, all'apparenza risolutiva, richiede in realtà condizioni assai stringenti. In particolare, le misure adottate dall'UE potrebbero avere serie difficoltà a superare il «test di necessità»: potrebbe essere messo in dubbio il loro reale contributo alla realizzazione dell'obiettivo perseguito e si potrebbe sostenere che erano ragionevolmente disponibili alternative parimenti efficaci, ma meno restrittive.

Ma anche là dove tale test dovesse essere superato, l'analisi non sarebbe conclusa: il «cappello» introduttivo dell'art. XIV GATS, infatti, richiede anche la coerenza delle misure contestate. L'UE potrebbe non riuscire a dimostrare il rispetto di tale requisito: di fronte a Stati terzi i cui ordinamenti non assicurano, nella loro interezza, un livello di protezione adeguato, in alcuni casi si è fatto uno sforzo per addivenire a una decisione settoriale, mentre in altri non è stato adottato alcun provvedimento, con conseguente pregiudizio per i servizi e i prestatori dei Paesi interessati.

In definitiva, l'analisi condotta ha portato alla seguente considerazione conclusiva: l'approccio proprio del diritto OMC, che dà grande importanza alle esigenze dell'espansione del commercio internazionale, diverge sensibilmente da quello assai restrittivo che caratterizza la disciplina UE in materia di flussi di dati personali verso Paesi terzi. Ciò implica che quest'ultima possa porsi in contrasto con svariati obblighi presenti nel GATS (clausola della nazione più favorita, regolamentazione interna, trattamento nazionale, accesso al mercato). Tali violazioni, nel caso in cui vi fosse una procedura di fronte agli organi OMC, sarebbero piuttosto difficili da giustificare. L'UE potrebbe dunque incorrere in una pronuncia sfavorevole e in tutte le conseguenze negative da essa derivanti.

2. *Gli impegni, inseriti in accordi commerciali UE, a consentire i flussi di dati: le criticità delle misure di salvaguardia pensate per controbilanciarli*

A) L'analisi si è occupata altresì del rapporto tra la normativa UE e certe disposizioni che l'Unione ha inserito in alcuni degli accordi internazionali di natura (esclusivamente o anche solo parzialmente) commerciale da essa conclusi e che rappresentano dei veri e propri impegni al trasferimento dei dati («*data flows commitments*»); tali impegni, finalizzati a incentivare i flussi di dati personali in ragione dell'importanza che essi rivestono per il commercio globale, sono poi controbilanciati da previsioni per salvaguardare la *privacy* e il diritto alla protezione dei dati personali.

A tal riguardo, innanzitutto, si è fatto riferimento a due strumenti multilaterali facenti parte del *corpus* normativo dell'OMC, ovvero l'«*Understanding on Commitments in Financial Services*» e l'«*Annex on Telecommunications*»: essi, infatti, contengono articoli come quelli poc'anzi descritti.

Ci si è poi soffermati, ancor di più, su alcuni dei principali accordi bilaterali che l'UE ha successivamente concluso al di fuori del quadro giuridico OMC. In particolare, ci si è focalizzati sul CETA con il Canada (trattato ampiamente in ragione della sua importanza e notorietà); su alcuni accordi più risalenti, come quelli con Corea del Sud, Colombia-Perù-Ecuador, America Centrale e Ucraina; nonché su alcuni accordi successivi, come quelli con Giappone, Singapore e Vietnam. Essi annoverano infatti varie norme in materia di scambi di servizi:

tra queste, figurano non solo alcuni degli obblighi chiave già visti nel GATS (trattamento nazionale, clausola della nazione più favorita, accesso al mercato), ma anche *data flows commitments* accompagnati da *data protection provisions*, specialmente in settori come i servizi finanziari o di telecomunicazione.

A) Orbene, le disposizioni sui trasferimenti e sulla protezione dei dati contenute nei citati strumenti presentano significative criticità, che sono state evidenziate.

Alcune problematiche riguardano la semplice presenza di simili previsioni negli accordi conclusi dall'UE. Nei mandati del Consiglio relativi a tali accordi, infatti, la tutela della *privacy* e la protezione dei dati personali non sono menzionate. Non è dunque chiaro fino a che punto la Commissione, all'interno della quale si occupa della materia la Direzione generale «Commercio» o DG TRADE, avesse il mandato di negoziare disposizioni che potessero avere effetto sulla sfera in questione.

Inoltre, sono rilevanti anche le criticità riguardanti la concreta formulazione delle disposizioni esaminate. Sul punto, in verità, vi sono stati alcuni miglioramenti nel corso del tempo, specialmente rispetto all'*Understanding* e all'*Annex*. Tuttavia, anche le previsioni contenute negli accordi bilaterali risultano problematiche. Le misure «adeguate» alla protezione della *privacy* e dei dati personali devono infatti rispettare vari limiti e condizioni. Inoltre, l'«adeguatezza» a cui si fa riferimento in tali disposizioni non indica certo «sostanziale equivalenza» agli standard UE: a differenza della Corte di giustizia, infatti, gli organismi sovranazionali a cui è attribuita la risoluzione delle controversie sull'interpretazione degli accordi commerciali non leggerebbero certo la nozione di «adeguatezza» alla luce della Carta di Nizza.

Sempre sugli organismi sovranazionali di risoluzione delle controversie si può dire, più in generale, che difficilmente essi potranno dare sufficiente peso alle esigenze di tutela dei diritti fondamentali, essendo stati istituiti per finalità diverse.

Alla luce di tutto ciò, si può affermare che la regolamentazione degli accordi commerciali dell'UE attribuisce una netta prevalenza alle esigenze degli scambi: per favorirli, l'Unione ha assunto impegni al trasferimento di dati, controbilanciandoli con misure di salvaguardia la cui portata ed efficacia risultano quantomeno dubbie. Ciò, tuttavia, può determinare problemi di coordinamento con l'approccio della disciplina interna UE in materia di flussi, più sensibile alla protezione degli individui.

3. *Le ragioni per cui l'approccio degli accordi commerciali può compromettere quello della disciplina interna UE*

A) Si devono, infine, riepilogare le conseguenze delle divergenze tra l'approccio proprio degli accordi commerciali di cui l'UE è parte, da un lato, e

quello che caratterizza la disciplina interna UE, dall'altro: ad avviso di chi scrive, infatti, il primo dei due approcci sopra menzionati rischia concretamente di compromettere il secondo.

Per prima cosa, è doveroso ricordare che è estremamente improbabile che agli accordi commerciali, nonché alle decisioni degli organismi sovranazionali di risoluzione delle controversie in materia commerciale, siano riconosciuti effetti diretti: essi, pertanto, non potranno essere invocati in giudizio dai singoli e un'eventuale violazione degli stessi da parte di un atto di diritto derivato UE non potrà portare all'annullamento di quest'ultimo.

Vi possono però essere altre rilevanti ripercussioni: quanto detto, infatti, non rende gli obblighi assunti dall'UE negli accordi commerciali meno vincolanti sul piano del diritto internazionale. Se l'UE non adempie ai propri obblighi, può incorrere in responsabilità e conseguenze giuridiche negative.

Il timore di queste ultime potrebbe determinare una forte pressione su vari attori istituzionali, compromettendo la loro indipendenza nel proteggere i dati personali. Ad esempio, in primo luogo, le autorità nazionali di controllo potrebbero essere portate a non esercitare il loro potere di sospendere o vietare i flussi di dati personali verso Paesi terzi. Inoltre, la Corte di giustizia potrebbe essere disincentivata dall'annullare ulteriori decisioni di adeguatezza. I maggiori dubbi, tuttavia, riguardano l'operato della Commissione, che potrebbe essere indotta ad adottare una decisione di adeguatezza pur in assenza di un livello di protezione «sostanzialmente equivalente» a quello UE. Nella realtà dei fatti si ritiene che ciò sia già avvenuto.

Si è detto e ripetuto che la Commissione, specialmente per importanti partner commerciali, ha adottato decisioni di adeguatezza motivate più da ragioni economiche che dalla presenza di una protezione «sostanzialmente equivalente» a quella UE. L'impossibilità di valutare come «adeguati» gli ordinamenti di tali Stati nella loro interezza ha costretto la Commissione a ricorrere a soluzioni creative, come decisioni settoriali.

Si possono citare come esempi i casi di Canada e Israele. Ancor più emblematica è però la vicenda che coinvolge il Giappone: con riferimento a tale Paese, in primo luogo, è stato necessario adottare una decisione settoriale, che copre esclusivamente certi trasferimenti; ma soprattutto, è stato indispensabile completare l'ordinamento giapponese con delle «Norme integrative», applicabili solo ai dati personali trasferiti dall'UE e non ai dati dei singoli in Giappone o provenienti da Paesi diversi. Riflessioni simili, ancorché in misura minore, valgono anche per la decisione concernente la Repubblica di Corea. È stato necessario trovare una soluzione creativa pure per l'UK: la Commissione ha escluso dall'applicazione della relativa decisione i trasferimenti a cui può applicarsi la troppo ampia «esenzione per motivi di immigrazione». Facile capire che attestazioni di adeguatezza così strutturate rischiano di sollevare problemi sul piano della loro attuazione operativa. Infine, tra le decisioni «creative», è da annoverare pure l'*EU-US Data Privacy Framework*, assai simile alle due precedenti misure riguardanti gli Stati Uniti e pertanto non sufficiente, di per sé, a superare definitivamente tutte le criticità del passato.

L'adozione di decisioni di questo tipo è avvenuta sotto una forte pressione, dovuta al timore di conseguenze sul piano commerciale, che ha indotto talvolta a forzare i tempi rispetto al necessario.

Nel caso del Giappone, ad esempio, la Commissione si è affrettata nell'adozione della relativa decisione di adeguatezza, in modo che essa precedesse (ancorché di pochi giorni) l'entrata in vigore dell'accordo EPA: ciò ha evitato *ab origine* che gli obblighi assunti dall'UE potessero essere violati da restrizioni dei flussi verso il Giappone. Tale soluzione appare però frutto di un compromesso e, nell'occasione, l'indipendenza della Commissione è stata messa in dubbio.

Discorso simile per il Regno Unito: ai sensi del TCA, dopo il 30 giugno 2021 le trasmissioni di dati dall'UE all'UK sarebbero state considerabili a tutti gli effetti trasferimenti verso uno Stato terzo. Per evitare tale scenario, che avrebbe potuto comportare violazioni degli impegni assunti dall'UE nel TCA, la Commissione ha accelerato nell'adozione della relativa decisione.

La necessità di adottare simili decisioni in tempi rapidi ha indotto la Commissione non solo ad avvalersi di soluzioni creative, ma anche a non tenere in sufficiente conto aspetti assai critici segnalati dal CEPD e dal Parlamento europeo. Tra questi, l'accesso ai dati da parte delle autorità pubbliche dei Paesi terzi per finalità di sorveglianza.

Da non dimenticare che la Commissione potrebbe essere indotta – dal timore delle conseguenze di cui sopra – anche a non revocare, né modificare o sospendere, una decisione di adeguatezza già adottata, pur non essendo più presente una protezione «sostanzialmente equivalente» a quella UE. Si possono, a tal proposito, citare le misure riguardanti Canada e Nuova Zelanda, brevi e scarne, che andrebbero con ogni probabilità rimesse in discussione e che invece sono state confermate.

Il fatto che, per pressioni derivanti dagli impegni commerciali, vengano adottate o mantenute in vita decisioni di adeguatezza nei confronti di Stati che non garantiscono una tutela «sostanzialmente equivalente» a quella europea, finisce per compromettere l'approccio della disciplina UE, che intenderebbe accordare una prevalenza alle esigenze di tutela dei diritti. Finiscono quindi per essere pregiudicate anche le finalità di tale approccio, tra cui quella di esportare gli standard UE.

Quest'ultima finalità, a onor del vero, rischiererebbe di essere compromessa anche qualora l'Unione cessasse completamente di adottare decisioni di adeguatezza: se fosse pressoché impossibile ottenere un simile provvedimento, i Paesi extra-UE non proverebbero neppure a innalzare il livello di tutela e sarebbero addirittura spinti ad abbracciare modelli diversi, più favorevoli alle esigenze commerciali (come quelli OCSE o APEC). Se vuole evitare questo rischio, la Commissione deve dunque continuare a svolgere accertamenti di adeguatezza.

Quanto sopra, tuttavia, non può certo legittimare decisioni nei confronti di Paesi che di certo non garantiscono una protezione «adeguata». La Commissione, così facendo, metterebbe a rischio i dati degli europei e rinuncerebbe pure a esportare gli standard UE, come avvenuto ad esempio nel caso del Giappone:

il livello più elevato di protezione previsto dalle «Norme integrative» riguarda esclusivamente i dati "europei", mentre lo Stato in questione può mantenere tutele inferiori in relazione a tutti gli altri dati personali. Venendo meno le condizioni per il noto «*Brussels effect*» (uno dei presupposti del quale è proprio la non divisibilità degli standard), risulta difficile che il quadro giuridico giapponese possa avvicinarsi significativamente a quello UE.

Un atteggiamento intransigente, come quello dimostrato dalla Corte nei riguardi degli USA, potrebbe invece portare ad alcuni frutti. Negli ultimi anni, soprattutto nel 2022, gli Stati Uniti sono infatti intervenuti per modificare la propria normativa in materia di sorveglianza. Se l'Unione riuscisse davvero a spingere gli USA verso una sostanziale riforma di tale ambito, si tratterebbe ovviamente di un grande successo del modello UE e del «*Brussels effect*».

Ma al di là di quest'ultimo caso, gli elementi fin qui forniti vanno a sostegno di quanto già affermato: non solo l'approccio degli accordi commerciali di cui l'UE è parte differisce da quello della disciplina interna UE, ma il primo dei due approcci rischia anche di pregiudicare il secondo. I forti meccanismi di attuazione di cui godono, sul piano internazionale, gli accordi commerciali possono creare una supremazia *de facto* di questi ultimi sulle norme a tutela dei diritti fondamentali: temendo simili meccanismi, attori istituzionali come la Commissione potrebbero essere portati a non restringere i flussi di dati personali, anche a discapito della protezione di questi ultimi.

B) In chiusura, va ricordato come, in verità, una soluzione a tale problematica è stata cercata. Nel 2018 la Commissione ha infatti promosso un nuovo meccanismo: si tratta delle cosiddette «*Horizontal provisions*», da inserire nei futuri accordi commerciali dell'UE al posto delle disposizioni "vecchio stampo". Esse, da un lato, contengono *data flows commitments*, che riguardano però tutti i settori economici (non solo ambiti specifici come i servizi finanziari o di telecomunicazione): per questo si parla di clausole «orizzontali». Dall'altro lato, presentano disposizioni dedicate al diritto fondamentale alla protezione dei dati personali e della *privacy*: esse hanno una formulazione diversa rispetto al passato, finalizzata a consentire il rispetto del quadro giuridico UE in materia di dati personali, che risulterebbe escluso dagli impegni commerciali assunti dall'Unione. Per inciso, nel 2019 la Commissione aveva proposto l'adozione di previsioni in gran parte similari pure in seno all'OMC, nell'ambito dei negoziati per disciplinare l'*e-commerce* a livello globale.

Grazie a simili disposizioni finirebbero per essere superate svariate delle criticità esposte: si ridurrebbe infatti il rischio che l'UE possa subire conseguenze per aver limitato i flussi verso Paesi terzi, e diminuirebbe la pressione sulla Commissione e sugli altri attori istituzionali, che sarebbero più indipendenti nel loro operato.

Occorre dunque salutare con grande favore non solo il fatto che l'UE stia tentando di includere tali previsioni negli accordi attualmente in via di negoziazione (e.g. con Indonesia, Australia, Tunisia) e nei rapporti con Stati con

cui sono già in vigore trattati commerciali (e.g. Corea del Sud, Singapore), ma ancor di più il fatto che sia effettivamente riuscita a inserirle nel testo definitivo di alcuni strumenti: l'*Interim Trade Agreement* con il Cile e, soprattutto, l'Accordo di libero scambio con la Nuova Zelanda (già in vigore) rappresentano esempi assai virtuosi.

Tuttavia, vi sono seri motivi per dubitare che le clausole orizzontali vengano concretamente inserite nei futuri accordi commerciali con tutti gli Stati terzi. Tali perplessità sorgono dall'osservazione empirica di alcuni casi, tra cui quelli riguardanti Vietnam e Giappone, ma soprattutto Regno Unito: il TCA con tale Paese si discosta dalle *Horizontal provisions* proprio negli aspetti più importanti. A causa di tali divergenze, permane incertezza sulla possibilità per l'UE di applicare in modo pieno e autonomo le proprie regole interne senza che da ciò derivino conseguenze potenzialmente pregiudizievoli sul piano internazionale. Qualcosa di simile si è verificato anche in riferimento alle regole dell'OMC in materia di *e-commerce*: lo «*stabilised text*» adottato nel 2024 differisce negli elementi chiave dalla proposta UE.

In definitiva, l'ampiezza dell'eccezione contenuta nelle clausole orizzontali può indurre le controparti dell'UE a non accettare sempre e comunque il testo delle *Horizontal provisions* senza modifiche. Ciò porta a non essere eccessivamente ottimisti sull'efficacia di tali strumenti: essi potrebbero non essere in grado di impedire del tutto che l'approccio UE in materia di dati personali sia compromesso dagli obblighi commerciali assunti dall'Unione. Risulta dunque impossibile dire di aver trovato una soluzione definitiva alle criticità esposte.

Capitolo III

RIFLESSIONI DI CARATTERE PROSPETTICO

La presente trattazione, innanzitutto, ha mostrato che la disciplina unilateralmente adottata dall'Unione europea in materia di trasferimenti di dati personali verso Stati extra-UE – per come delineata dal legislatore nel GDPR, per come interpretata dalla Corte di giustizia nelle sue sentenze (soprattutto), e per come attuata dalla Commissione con alcuni atti (ancorché non con tutti) – effettua un'opera di bilanciamento in cui le esigenze di protezione dei dati personali prevalgono chiaramente su quelle di carattere commerciale.

Detto in altri termini, l'approccio dell'Unione europea alla materia, creato grazie al Regolamento (UE) 2016/679, consiste nel costruire attorno ai dati personali una vera e propria "fortezza", per entrare nella quale è necessario adeguarsi agli elevati standard UE di protezione dei diritti fondamentali. Chi vuole relazionarsi con l'UE, accedendo al suo mercato e ricevendo i dati dei cittadini europei, deve allinearsi alle sue indicazioni, conformandosi a determinati principi, rispettando certi obblighi, garantendo particolari diritti.

Un simile atteggiamento ha varie finalità. Da un lato, si vuole evitare che i trasferimenti di dati personali verso Paesi terzi siano utilizzati per aggirare il robusto quadro disegnato dal GDPR: si vuole dunque garantire la continuità dell'elevato livello di tutela che contraddistingue l'UE, anche dopo che i dati vengono trasmessi oltrefrontiera. Dall'altro lato, l'Unione ha anche l'obiettivo di esportare i propri standard verso un numero più ampio possibile di Stati terzi, esercitando unilateralmente un'influenza sulle loro normative grazie alla sua posizione centrale nell'economia globale («*Brussels effect*»).

L'esportazione degli standard, a sua volta, ha molteplici scopi. Essa si pone chiaramente in linea con gli obiettivi dell'azione esterna UE, la quale si prefigge di promuovere nel resto del mondo i principi che hanno informato la creazione, lo sviluppo e l'allargamento dell'Unione, tra cui i diritti dell'uomo. Ma ha anche finalità di tipo strategico, consistenti nel tentare di conferire un vantaggio competitivo alle imprese UE rispetto alle società concorrenti extra-UE.

Appare quanto mai chiaro che quello che viene effettuato dalla normativa UE non è solo un bilanciamento tra l'esigenza di tutelare i diritti fondamentali, da un lato, e quella di favorire l'espansione del commercio internazionale, dall'altro. La questione assume contorni ben più complessi: anche dietro la protezione dei dati personali, che per l'appunto finisce per prevalere, si celano

considerazioni di carattere economico, consistenti nella volontà di proteggere le imprese dell'Unione dalla concorrenza di società di altri Paesi.

Al tempo stesso, la presente trattazione ha anche messo in luce come il descritto approccio sia contraddetto da quello che invece caratterizza determinati obblighi di natura commerciale, assunti dall'Unione sia nell'ambito dell'Organizzazione mondiale del commercio, sia all'interno di accordi commerciali bilaterali con Stati terzi. L'UE si è infatti impegnata sul piano internazionale a consentire certi flussi transfrontalieri di dati: ciò, non solo mediante *data flows commitments* «impliciti», consistenti in norme di portata generale sulla liberalizzazione dei servizi (come clausola della nazione più favorita, trattamento nazionale, accesso al mercato); ma anche attraverso *data flows commitments* «espliciti», che impongono proprio di non ostacolare i trasferimenti, spesso in settori come i servizi finanziari o quelli di telecomunicazione.

È vero che simili impegni sono controbilanciati da clausole di vario tipo, che spesso contemplano in modo specifico la possibilità di deroghe finalizzate alla protezione dei dati personali e della *privacy*. Tuttavia, è anche vero che la portata e l'efficacia di simili salvaguardie risultano assai limitate ed esse non sembrano in grado di tutelare efficacemente i diritti fondamentali degli individui. Gli accordi commerciali conclusi dall'UE, dunque, accordano alle esigenze degli scambi una prevalenza piuttosto netta.

Una simile contraddittorietà tra l'approccio che contraddistingue la disciplina interna dell'Unione e quello che caratterizza i suoi trattati con Stati terzi induce a significative considerazioni. Si palesa in tutta la sua evidenza il fatto che i vari attori istituzionali dell'Unione europea, e talvolta persino le varie ramificazioni interne alla stessa istituzione (segnatamente, alla Commissione), hanno visioni e strategie spesso estremamente differenti. Ciò potrebbe ispirare commenti di carattere ancor più generale, riguardanti non solo la materia oggetto della presente trattazione, ma anche altri ambiti di competenza UE. Potrebbe portare, ad esempio, a mettere in dubbio l'affermazione secondo cui l'azione esterna dell'Unione è sempre guidata dallo stesso approccio che informa la disciplina interna UE. Anzi, potrebbe spingere ad affermare che i valori e i principi che l'Unione "inietta" nei suoi accordi internazionali sono spesso assai differenti da quelli propri della sua legislazione, proprio in ragione delle profonde divergenze di vedute tra i vari attori istituzionali.

Tornando più nello specifico all'ambito su cui si è concentrata la trattazione, si vede come esistano, da un lato, alcuni attori istituzionali UE che abbracciano un approccio che mette al centro la protezione dei dati («*data-protection-centred approach*»). *In primis*, deve essere citata la Corte di giustizia, che ha sempre privilegiato le esigenze di *privacy* e *personal data protection* rispetto a tutte le istanze concorrenti, dimostrandosi in ciò assolutamente intransigente e non scendendo mai a compromessi. Ma deve essere menzionato anche il Parlamento europeo, che si è spesso rivelato attento alla tutela dei diritti; nonché ovviamente il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati (l'inclusione di questi ultimi nell'elenco non è certo sorprendente, essendo

stati istituiti proprio con lo specifico compito di proteggere i dati personali). Infine, in questa lista può essere in realtà annoverata anche la Commissione, ma limitatamente alla sua Direzione generale «Giustizia e consumatori» (DG JUST), che *inter alia* si è occupata della fase di redazione del GDPR e cura l'adozione delle decisioni di adeguatezza: tale Direzione generale ha infatti una maggior sensibilità verso i consumatori che non verso il mercato.

Dall'altro lato, però, esiste anche un approccio che mette al centro le esigenze di libero scambio («*free-trade-centred approach*»), proprio soprattutto di un'altra articolazione della Commissione, ovvero la Direzione generale «Commercio» (DG TRADE), responsabile della politica per il commercio con i Paesi del resto del mondo. Quest'ultima, in ragione sia della sua finalità, che delle formazioni e sensibilità personali dei suoi componenti, finisce per non essere particolarmente attenta alle esigenze di protezione dei dati personali; essa, probabilmente, sovrastima la portata delle salvaguardie inserite negli accordi commerciali e sottovaluta invece i rischi che i dati in questione corrono.

La presente trattazione, tuttavia, non si è limitata a mettere in evidenza simili divergenze. Essa è anche arrivata ad affermare che le due impostazioni non possono coesistere: al contrario, l'approccio proprio degli accordi commerciali di cui l'UE è parte rischia concretamente di compromettere quello che caratterizza la disciplina interna UE. Gli accordi commerciali godono infatti, sul piano internazionale, di meccanismi preposti alla loro attuazione assai forti, circostanza che può determinare una loro supremazia *de facto*. Il timore delle conseguenze derivanti da simili meccanismi potrebbe determinare una forte pressione su vari attori istituzionali, compromettendo la loro indipendenza nel proteggere i dati personali degli individui.

Ciò vale, astrattamente, per le autorità nazionali di controllo, che potrebbero essere indotte a non sospendere o vietare i flussi di dati verso Paesi terzi, nonché per la Corte di giustizia, che in futuro potrebbe essere disincentivata dall'annullare ulteriori decisioni di adeguatezza. Ma soprattutto vale per la Commissione, che è stata effettivamente indotta, in più di un'occasione, ad adottare, o a non revocare, decisioni di adeguatezza pur in assenza di livelli di protezione «sostanzialmente equivalenti» a quello UE. Detto in altri termini, si potrebbe affermare che l'approccio di DG TRADE ha finito per "contagiare" DG JUST: quest'ultima, sotto la pressione di conseguenze per l'Unione derivanti dagli impegni commerciali assunti da DG TRADE, in più di una circostanza non ha perseguito nel migliore dei modi l'interesse alla protezione dei dati personali.

La "fortezza" costruita dall'UE attraverso la sua disciplina interna, di cui si è parlato poc'anzi, rischia dunque di cedere, e ciò finirebbe inevitabilmente per compromettere anche gli obiettivi della stessa: ci si riferisce quindi anche all'esportazione degli standard UE nel resto del mondo, nonché alla protezione delle imprese europee dalla concorrenza straniera.

A questo punto, sia concesso a chi scrive concludere la presente trattazione con una riflessione di carattere prospettico. Si ritiene infatti che, per l'Unione europea, sarebbe preferibile scegliere in modo più netto l'approccio da abbrac-

ciare, indipendentemente dal fatto che sia l'uno o l'altro tra quelli descritti; una volta presa tale decisione, l'impostazione prescelta dovrebbe essere perseguita con coerenza da tutti gli attori istituzionali, nessuno escluso.

Chiaramente, la scelta dell'approccio per cui optare non può certo essere casuale, ma deve essere fatta tenendo conto non solo dei valori, ma anche degli interessi dell'Unione europea. *Inter alia*, ci si deve chiedere se è vero che i flussi transfrontalieri di dati personali sono così convenienti dal punto di vista economico per le imprese europee; oppure se al contrario essi vadano in misura prevalente a beneficio dei *big player* del mercato mondiale dei servizi digitale (ubicati principalmente fuori dall'Europa e soprattutto negli Stati Uniti), i quali, alimentandosi anche dei dati personali provenienti dall'UE, potrebbero creare un *gap* incolmabile tra loro e le imprese europee: in ragione di ciò, i flussi oltrefrontiera di dati personali potrebbero essere ritenuti addirittura dannosi per l'economia digitale europea, che necessiterebbe dunque di maggiore protezione.

Valutazioni di questo tipo, è bene dirlo, sono in corso in tutto il mondo. Basti pensare che perfino gli USA, che hanno sempre sostenuto la necessità della libera circolazione delle informazioni e che dalla trasmissione delle medesime hanno sempre tratto grande giovamento, stanno introducendo limitazioni ai flussi oltrefrontiera di dati personali, con particolare riferimento a quelli diretti verso la Cina. Coerentemente con l'approccio statunitense, tali misure sono motivate da ragioni legate non tanto alla tutela della *privacy*, quanto alla sicurezza nazionale. Ma ciò non cambia il fatto che simili restrizioni siano anche finalizzate a promuovere ulteriormente l'industria digitale nazionale, assicurandosi che il valore prodotto dai dati dei cittadini rimanga all'interno del Paese e che non sia invece sfruttato da *competitor* di Stati terzi [1].

Orbene, anche per l'Unione europea è imprescindibile interrogarsi circa la convenienza per la propria economia digitale dei flussi transfrontalieri di dati personali. Al termine di tale valutazione, là dove ritenesse che simili flussi, oltre ad essere coerenti coi propri valori, siano anche tali da arrecare alle imprese UE più benefici che rischi, sarebbe forse opportuno un ripensamento del Regolamento (UE) 2016/679 e degli strumenti da esso previsti e l'adozione di un approccio maggiormente in linea con quello che caratterizza gli accordi commerciali conclusi dall'Unione.

Se, al contrario, l'UE si rendesse conto che i *transborder flows of personal data*, oltre a pregiudicare i diritti fondamentali degli europei, danneggiano irre-

---

[1] Sul punto v., *inter alios*: S. YAKOVLEVA, *Editorial: On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows*, in *Legal Issues of Economic Integration*, 2022, Volume 49, Numero 4, pp. 339-348; S. YAKOVLEVA, *EU's trade policy on cross-border data flows in the global landscape: navigating the thin line between liberalizing digital trade, "digital sovereignty" and multilateralism*, Institute for Information Law Research Paper No. 2022-12, Amsterdam, 2022; S. YAKOVLEVA, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, Institute for Information Law Research Paper No. 2022-09, Amsterdam, 2022; K. IRION-M.E. KAMINSKI-S. YAKOVLEVA, *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, in *University of Chicago Law Review Online*, 2023.

parabilmente anche l'economia digitale dell'Unione, allora dovrebbe cercare di seguire maggiormente la strada tracciata dalla Corte di giustizia e di non assumere impegni sul piano internazionale che la obblighino a consentire flussi di dati, liberandosi, ove possibile, di quelli esistenti: ciò, ad esempio, avvalendosi di quelle disposizioni che consentono di apportare modifiche agli accordi già conclusi [2], se non addirittura di quelle che ne consentono la denuncia [3]. L'unica eccezione potrebbe essere rappresentata dalle *Horizontal Provisions*, a patto che sia mantenuta la loro formulazione originaria.

Ciò che certamente non appare logico, invece, è che l'Unione prosegua per la sua strada attuale, consistente nel mantenere intatta la disciplina giuridica interna, continuando al tempo stesso a vincolarsi attraverso *data flows commitments* di varia natura. Tale mancata scelta, a sua volta, equivarrebbe a una scelta, dal momento che gli impegni commerciali finirebbero in ogni caso per compromettere gli obiettivi del quadro legislativo.

[2] Fra tali disposizioni, a titolo meramente esemplificativo, si può menzionare l'art. 30.2 del CETA con il Canada, dedicato alle «Modifiche».

[3] Fra tali disposizioni, a titolo meramente esemplificativo, si può menzionare l'art. 30.9 del CETA con il Canada, dedicato alla «Denuncia».

BIBLIOGRAFIA

AARONSON S.A., *The Digital Trade Imbalance and Its Implications for Internet Governance*, in *Global Commission on Internet Governance Paper Series*, 2016, Numero 25.

AARONSON S.A.-LEBLOND P., *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 2018, Volume 21, Numero 2, pp. 245-272.

ADAM R.-TIZZANO A., *Manuale di diritto dell'Unione europea. Quarta edizione*, Giappichelli, Torino, 2024.

ALGOSTINO A., *ISDS (Investor-State Dispute Settlement), il cuore di tenebra della global economic governance e il costituzionalismo*, in *Costituzionalismo.it*, 2016, Numero 1, pp. 103-174.

ARUP C., *The New World Trade Organization Agreements: Globalizing Law Through Services and Intellectual Property*, Cambridge University Press, Cambridge, 2001.

ATKINSON R.D., *International Data Flows: Promoting Digital Trade in the 21st Century*, Testimony Before the U.S. House Judiciary Committee – Subcommittee on Courts, Intellectual Property and the Internet, 3 novembre 2015.

BARTL M.-IRION K., *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, University of Amsterdam, Amsterdam, 2017.

BATURONES J.J.E., *La regulación de los datos sensibles a la Directiva 95/46/CE*, in *Informática y derecho: Revista iberoamericana de derecho informático*, 1998, Numeri 23-26, pp. 1217-1248.

BEESON M., *Institutions of the Asia Pacific. ASEAN, APEC and beyond*, Routledge, New York, 2009.

BENDIEK A.-RÖMER M., *Externalizing Europe: the global effects of European data protection*, in *Digital Policy, Regulation and Governance*, 2018.

BENNET C.-RAAB C., *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, Aldershot, 2003.

BERNSDORFF N., *Kapitel II, Freiheiten: Artikel 6 Bis 19*, in MEYER J. (a cura di), *Kommentar zur Charta der Grundrechte der Europäischen Union*, Nomos Verlagsgesellschaft, Baden-Baden, 2003, pp. 135-262.

BHAGESHPUR K., *Data Is The New Oil – And That's A Good Thing*, in *www.forbes.com*, 15 novembre 2019.

BIGNAMI F., *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*, 2007, Volume 48, Numero 3, pp. 609-698.

BIGNAMI F.-RESTA G., *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *Law and Contemporary Problems*, 2015, Volume 78, Numero 4, pp. 231-266.

BLACKMORE N., *Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific*, in *www.kennedyslaw.com*, 26 marzo 2019.

BODÓ B., *The Commodification of Trust*, Institute for Information Law (IViR) Research Paper No. 2021-01, Amsterdam, 2021.

BOSSE-PLATIÈRE I.-RAPOPORT C., *Negotiating and implementing EU free trade agreements in an uncertain environment*, in BOSSE-PLATIÈRE I.-RAPOPORT C. (a cura di), *The Conclusion and Implementation of EU Free Trade Agreements. Constitutional Challenges*, Edward Elgar Publishing, Cheltenham, 2019, pp. 1-21.

BOWDEN C., *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Document requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Bruxelles, 2013.

BRADFORD A., *The Brussels Effect*, in *Northwestern University Law Review*, Volume 107, Numero 1, 2012, pp. 1-68.

BRADFORD A., *The Brussels effect: How the European Union rules the world*, Oxford University Press, Oxford, 2020.

BRADFORD FRANKLIN S., *Rethinking Surveillance on the 20th Anniversary of the Patriot Act*, in *www.justsecurity.org*, 26 ottobre 2021.

BRADFORD FRANKLIN S.-SARKESIAN L., *Congress Has the Opportunity to Enact Meaningful Surveillance Reforms Now: Here's How*, in *www.newamerica.org*, 21 febbraio 2020.

BRAIBANT G., *La Charte des Droits fondamentaux de l'Union européenne*, Editions du Seuil, Parigi, 2001.

BRÄNNSTRÖM L., *Global Inequality and the EU International Law Position on Cross-Border Data Flows*, in *Nordic Journal of International Law*, 2023, Volume 92, pp. 119-137.

BRÜHANN U., *La directive européenne relative à la protection des données: fondement, histoire, points forts*, in *Revue française d'administration publique*, Gennaio-marzo 1999, Numero 89, pp. 9-19.

BRYNJOLFSSON E.-MCELHERAN K., *Data in Action: Data-Driven Decision Making in U.S. Manufacturing*, U.S. Census Bureau Center for Economic Studies Working Paper 16-06, Washington DC, Gennaio 2016.

BURRI M., *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, in *University of California Davis Law Review*, 2017, Volume 51, pp. 65-132.

BURRI M., *Interfacing Privacy and Trade*, in *Case Western Reserve Journal of International Law*, 2021, Volume 53, Numero 1, pp. 35-87.

BURRI M., *A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability*, in *Georgetown Journal of International Law*, 2023, Volume 53, pp. 565-625.

BURRI M., *Creating Data Flow Rules through Preferential Trade Agreements*, in CHANDER A.-SUN H. (a cura di), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, New York, 2023, pp. 264-291.

BURRI M., *Cross-border data flows and privacy in global trade law: has trade trumped data protection?*, in *Oxford Review of Economic Policy*, 2023, Volume 39, Numero 1, pp. 85-97.

BURRI M.-CHANDER A., *What Are Digital Trade and Digital Trade Law?*, in *AJIL Unbound*, 2023, Volume 117, pp. 99-103.

BURRI M.-KUGLER K., *Regulatory autonomy in digital trade agreements*, in *Journal of International Economic Law*, 2024, Volume 27, Numero 3, pp. 397-423.

BURRI M.-KUGLER K.-KER A.D., *Digital Trade in the EU–New Zealand Free Trade Agreement: An Appraisal*, in *Legal Issues of Economic Integration*, 2024, Volume 51, Numero 1, pp. 11-46.

BYGRAVE L.A., *Data Privacy Law. An International Perspective*, Oxford University Press, Oxford, 2014, pp. 75-79.

BYGRAVE L.A., *Data protection by design and by default*, in KUNER C.-BYGRAVE L.A.-DOCKSEY C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 571-581.

CAGGIANO G., *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza* Schrems II *della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, Volume XV, Numero 3, pp. 563-585.

CASORIA M.-ALSARRAF E.M., *The Impact of the GDPR on Extra-EU Legal Systems: The Case of the Kingdom of Bahrain*, in TZANOU M. (a cura di), *Personal Data Protection and Legal Developments in the European Union*, IGI Global, Hershey, 2019, pp. 224-237.

CASSANO G.-CIMINO I.P., *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 *Giurisprudenza italiana*, 2004, pp. 1805-1809.

CASTRO D.-MCQUINN A., *Cross-Border Data Flows Enable Growth in All Industries*, Information Technology & Innovation Foundation, Febbraio 2015.

CELLERINO C., *L'ambito di applicazione "territoriale" della normativa UE in materia di protezione dei dati personali (GDPR) e l'economia globale dei dati: quale modello regolatorio?*, in DOMINELLI S.-GRECO G.L. (a cura di), *I mercati dei servizi fra regolazione e governance*, Giappichelli, Torino, 2020, pp. 135-156.

CHANDER A., *Artificial Intelligence and Trade*, in BURRI M. (a cura di), *Big Data and Global Trade*, Cambridge University Press, Cambridge, 2021, pp. 115-127.

CHANDER A.-SCHWARTZ P.M., *Privacy and/or Trade*, in *The University of Chicago Law Review*, 2023, Volume 90, Numero 1, pp. 49-135.

CHENAOUI H., *Moroccan data protection law: Moving to align with EU data protection?*, in *www.iapp.org*, 11 settembre 2018.

CHOROMIDOU A., *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS*, in *International Data Privacy Law*, 2021.

CHRISTAKIS T., *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)*, in *European Law Blog*, 13 novembre 2020.

CHRISTAKIS T., *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)*, in *European Law Blog*, 16 novembre 2020.

CHRISTAKIS T., *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)*, in *European Law Blog*, 17 novembre 2020.

CITIZEN.ORG, *Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded*, 19 agosto 2015.

COHEN G., *The Negligence-Opportunism Tradeoff in Contract Law*, in *Hofstra Law Review*, 1992, Volume 20, Numero 4, pp. 941-1016.

COMANDÉ G.-MALGIERI G. (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018.

COMELLA C., *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza* Safe Harbor *della Corte di giustizia dell'Unione Europea*, in RESTA G.-ZENO-ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 49-71.

CONVERTI A., *Istituzioni di diritto dell'Unione europea*, Halley, Macerata, 2003.

COSTA E., *Article 7. Conditions for consent*, in KUNER C.-BYGRAVE L.A.-DOCKSEY C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 345-354.

COSTELLO R.A., *Schrems II: Everything is Illuminated?*, in *European Papers*, 2020, Volume 5, Numero 2, pp. 1045-1059.

COUDRAY L., *La protection des données personnelles dans l'Union européenne, Naissance et consécration d'un droit fondamental*, Éditions Universitaires européennes, Berlino, 2010.

D'ACQUISTO G.-PIZZETTI F., *Regolamentazione dell'economia dei dati e protezione dei dati*

personali, in *Analisi Giuridica dell'Economia*, Giugno 2019, Numero 1, giugno 2019, pp. 89-108.

D'Agata C., *I meccanismi di comunicazione tra le Autorità di controllo*, in Comandé G.-Malgieri G. (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 89-97.

D'Agata C., *Flussi transfrontalieri di dati personali e ruolo del Garante*, in Comandé G.-Malgieri G. (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 97-103.

D'Alterio E., «*Il bruco e la farfalla*». *Libertà di commercio ed eccezione culturale*, in *Giornale di diritto amministrativo*, 2010, Numero 8, pp. 847-857.

De Bustos J.C.M.-Izquierdo-Castillo J., *Who will control the media? The impact of GAFAM on the media industries in the digital economy*, in *Revista Latina de Comunicación Social*, 2019, Numero 74, pp. 803-821.

De Schutter O., *La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi*, in *Revue trimestrielle des droits de l'homme*, 2003, Numero 54, pp. 627-664.

De Terwangne C., *Article 5. Principles relating to processing of personal data*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 309-320.

Del Federico C.-Popoli A.R., *Le definizioni*, in Finocchiaro G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 63-109.

Docquir B., *Le droit à la vie privée*, De Boeck-Larcier, Bruxelles, 2008.

Dongo D.-Bergamini S., *CETA, via libera della Corte di Giustizia al 'trita-norme' a servizio delle 'Corporation'*, in *Greatitalianfoodtrade.it*, 6 maggio 2019.

Dordi C., *L'Accordo generale sul commercio dei servizi*, in Venturini G. (a cura di), *L'Organizzazione Mondiale del Commercio*, Giuffrè, Milano, 2015, pp. 151-197.

Drechsler L.-Yakovleva S., *Contribution to the public consultation on the Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Institute for Information Law Research Paper No. 2022-14, Amsterdam, 2022.

Eger J., *Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?*, in *Law and Policy in International Business*, 1978, Volume 10, Numero 4, pp. 1065-66.

Ekmekdjian M.A.-Pizzolo C., *Hábeas data: El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996.

Ercolani G., *Novità in materia di protezione dei dati personali: la Commissione europea adotta nuove clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento 2016/679 UE*, in *Eurojus.it*, 24 giugno 2021.

Espinel V., *Executive Survey Shows the Benefits of Data Innovation Across the Whole Economy*, in *BSA Tech Post*, 10 dicembre 2014.

Esposito M.S., *Il trattamento transfrontaliero e la cooperazione tra Autorità garanti. Il meccanismo di coerenza*, in Finocchiaro G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 690-724.

Evola M., *The EU-Ukraine Association Agreement between the European Neighbourhood Policy and admission*, in *Il Diritto dell'Unione europea*, 2015, Numero 1, pp. 199-236.

FAHEY E., *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?*, in *European Papers*, 2023, Volume 8, Numero 2, pp. 503-511.

FERRACANE M.F.-HOEKMAN B.-VAN DER MAREL E.-SANTI F., *Digital Trade, Data Protection and EU Adequacy Decisions*, RSC Working Paper 2023/37, Firenze, 2023.

FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in RESTA G.-ZENO-ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 113-135.

FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019.

FINOCCHIARO G., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 1-26.

FIORETTI J., *EU moves to remove barriers to data flows in trade deals*, in *www.reuters.com*, 9 febbraio 2018.

FUMAGALLI MERAVIGLIA M., *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016, Fascicolo 1, pp. 1-39.

GAGLIARDI M., *Gli adempimenti previsti dal regolamento: quadro generale, registri*, in COMANDÉ G.-MALGIERI G. (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 63-67.

GAJA G., *Il preambolo di una decisione del Consiglio preclude al «GATT 1994» gli effetti diretti nell'ordinamento comunitario?*, in *Rivista di diritto internazionale*, 1995, pp. 407-409.

GASSMANN H.P., *30 Years After: The Impact of the OECD Privacy Guidelines*, Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP), Parigi, 10 marzo 2010.

GENTOT M., *La protection des données personnelles à la croisée des chemins*, in TABATONI P. (a cura di), *La protection de la vie privée dans la société d'information: Tome 3*, Presses Universitaires de France, Parigi, 2000, pp. 24-46.

GERAETS D.-VANDER SCHUEREN P., *Exporting the EU Privacy Regime Through Trade Instruments?*, in *Mayer Brown*, 19 marzo 2018.

GERLACH N.-KEUSTERMANS J.F., *Europe and Japan towards the Future – the first post GDPR adequacy decision of the European Commission*, 11th Annual Sedona Conference International Programme on Cross-Border Data Transfers and Data Protection Laws, 14 giugno 2019.

GIANNACCARI A.-UMBERTAZZI T.M., *Il caso Lindqvist: i limiti della privacy europea*, in *Danno e responsabilità*, 2004, Numero 4, pp. 377-388.

GÖMANN M., *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, in *Common Market Law Review*, 2017, Volume 54, Numero 2, pp. 567-590.

GONZÁLEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht, 2014.

GRANGER M.P.-IRION K., *The right to protection of personal data: the new posterchild of European Union citizenship?*, in DE VRIES S.-DE WAELE H.-GRANGER M.P. (a cura di), *Civil Rights and EU Citizenship. Challenges at the Crossroads of the European, National and Private Spheres*, Edward Elgar, Cheltenham, 2018, pp. 279-302.

GREENLEAF G., *Death of the EU Privacy Directive? Choppy waters in the Safe Harbor*, in *Privacy Law & Policy Reporter*, 1999, Volume 6, Numero 6, pp. 81-83.

GREENLEAF G., *Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$*, in *Privacy Law & Policy Reporter*, 2000, Volume 7, Numero 3, pp. 45-47.

GREENLEAF G., *A world data privacy treaty? 'Globalisation' and 'modernisation' of Council of Europe Convention 108*, in WITZLEB N. e altri (a cura di), *Emerging Challenges in Privacy Law: Comparative Perspectives*, Cambridge University Press, Cambridge, 2014, pp. 92-138.

GREENLEAF G., *Renewing Data Protection Convention 108: The Coe's 'Gdpr Lite' Initiatives*, in *Privacy Laws & Business International Report*, 2016, Volume 142, pp. 1-8.

GREENLEAF G., *Japan and Korea: Different paths to EU adequacy*, in *Privacy Laws & Business International Report*, 2018, Numero 156, pp. 9-11.

GREENLEAF G., *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*, in *Privacy Laws & Business International Report*, 2019.

GREENLEAF G., *2020 Ends a Decade of 62 New Data Privacy Laws*, in *Privacy Laws & Business International Report*, 2020.

GREENLEAF G., *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*, in *Privacy Laws & Business International Report*, 2021.

GREENLEAF G., *The Draft Korea Adequacy Decision: Submission to European Union Authorities*, in *University of New South Wales Law Research Series*, 2021, Numero 52.

GREENLEAF G., *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, in *Privacy Laws & Business International Report*, 2022.

GREENLEAF G., *Global data privacy laws 2023: 162 national laws and 20 Bills*, in *Privacy Laws & Business International Report*, 2023.

GSTREIN O.J.-ZWITTER A.J., *Extraterritorial application of the GDPR: promoting European values or power?*, in *Internet Policy Review*, 2021, Volume 10, Numero 3, pp. 1-30.

HEIL H., *Directive 95/46/EC of the European Parliament and of the Council: Introductory remarks*, in BÜLLESBACH A.-GIJRATH S.-POULLET Y.-PRINS C. (a cura di), *Concise European IT Law (Second Edition)*, Kluwer Law International, Alphen aan den Rijn, 2010, pp. 9-32.

HILDÉN J., *The Politics of Datafication: The Influence of Lobbyists on the EU's Data Protection Reform and its Consequences for the Legitimacy of the General Data Protection Regulation*, University of Helsinki, Helsinki, 2019.

HOEKMAN B., *Services and Intellectual Property Rights*, in COLLINS S.M., BOSWORTH B.P. (a cura di), *The New GATT: Implications for the United States*, Brookings, Washington, 1994.

HÖGLUND W., *Exporting data protection law. The extraterritorial reach of the GDPR*, Umeå Universitet, Umeå, 2018.

HONDIUS F.W., *The Council of Europe's work in the area of computers and privacy*, Discussion paper of round table on the use of data processing for parliamentary work, Strasburgo, 18-19 maggio 1978.

HONDIUS F.W., *A Decade of International Data Protection*, in *Netherlands International Law Review*, 1983, Volume 30, pp. 103-128.

HU M., *Small Data Surveillance v. Big Data Cybersurveillance*, in *Pepperdine Law Review*, 2015, Volume 42, Numero 4, pp. 773-844.

HUGHES-CROMWICK E.-CORONADO J., *The Value of US Government Data to US Business Decisions*, *in Journal of Economic Perspectives*, 2019, Volume 33, Numero 1, pp. 131-146.

IRION K.-BURRI M.-KOLK A.-MILAN S., *Governing "European values" inside data flows: Interdisciplinary perspectives*, in *Internet Policy Review*, 2021, Volume 10, Numero 3.

Irion K.-Kaminski M.E.-Yakovleva S., *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, in *University of Chicago Law Review Online*, 2023.

Irion K.-Luchetta G., *Online Personal Data Processing and the EU Data Protection Reform*, Centre for European Policy Studies, Bruxelles, 2013, p. 35.

Irion K.-Williams J., *Prospective Policy Study on Articial Intelligence and EU Trade Policy*, Institute for Information Law (IViR), Amsterdam, 2019.

Irion K.-Yakovleva S.-Bartl M., *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements*, Institute for Information Law (IViR), Amsterdam, 2016.

Juncker J.C., *Un nuovo inizio per l'Europa. Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico – Orientamenti politici per la prossima Commissione europea*, Strasburgo, 15 luglio 2014.

Kirby M.D., *International guidelines to protect privacy in transborder data flows*, ANZAAS (Australian & New Zealand Association for the Advancement of Science) Jubilee conference, Adelaide, 15 maggio 1980.

Kirby M.D., *Informatics and Law Reform*, in *Journal of Law and Information Science*, 1981, Volume 1, Numero 1, pp. 1-22.

Kirby M.D., *The history, achievement and future of the 1980 OECD guidelines on privacy*, in *International Data Privacy Law*, Febbraio 2011, Volume 1, Numero 1, pp. 6-14.

Kotschy W., *The proposal for a new General Data Protection Regulation – problems solved?*, in *International Data Privacy Law*, Novembre 2014, Volume 4, Numero 4, pp. 274-281.

Kris D.S., *On the Bulk Collection of Tangible Things*, in *Journal of National Security Law & Policy*, 2014, Volume 7, Numero 2, pp. 209-295.

Kuner C., *Developing an Adequate Legal Framework for International Data Transfers*, in Gutwirth S.-Poullet Y.-De Hert P.-De Terwangne C.-Nouwt S. (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 263-273.

Kuner C., *Transborder Data Flows and Data Privacy Law*, Oxford University Press, Oxford, 2013.

Kuner C., *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 2018, Volume 55, Numero 3, pp. 857-882.

Kuner C., *Article 44. General principle for transfers*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 755-770.

Kuner C., *Article 45. Transfers on the basis of an adequacy decision*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 771-796.

Kuner C., *Article 46. Transfers subject to appropriate safeguards*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 797-812.

Kuner C., *Article 47. Binding corporate rules*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 813-824.

Kuner C., *Article 49. Derogations for specific situations*, in Kuner C.-Bygrave L.A.-Docksey C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 841-856.

Kuner C., *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 17 luglio 2020.

KUNER C., *Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR*, in *European Law Blog*, 13 dicembre 2021.

KUNER C., *Protecting EU Data Outside EU Borders Under the GDPR*, in *Common Market Law Review*, 2023, Volume 60, Numero 1, pp. 77-106.

KUNER C.-BYGRAVE L.A.-DOCKSEY C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020.

KUSCHEWSKY M., *Revised OECD Privacy Guidelines Strengthen Accountability Principle*, in *Inside Privacy*, 23 settembre 2013.

LAURER M.-SEIDL T., *Regulating the European Data Driven Economy: A Case Study on the General Data Protection Regulation*, in *Policy & Internet*, 2020, pp. 257-277.

LENAERTS K., *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, 2019, Volume 20, Numero 6, pp. 779-793.

MAGALHAES G.-ROSEIRA C., *Open government data and the private sector: An empirical view on business models and value creation*, in *Government Information Quarterly*, Luglio 2020, Volume 37, Numero 3, pp. 1-10.

MALGIERI G., *I principi generali del Regolamento alla base del trattamento di dati personali*, in COMANDÉ G.-MALGIERI G. (a cura di), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Il Sole 24 Ore, Milano, 2018, pp. 16-20.

MARRELLA F., *Manuale di diritto del commercio internazionale. Contratti internazionali, imprese globali ed arbitrato*, CEDAM, Padova, 2017.

MARTINES F., *L'onere della prova nell'Organizzazione Mondiale del Commercio e valori del sistema*, Maggioli, Rimini, 2012.

MARTINES F., *Direct Effect of International Agreements of the European Union*, in *The European Journal of International Law*, 2014, Volume 25, Numero 1, pp. 129-147.

MATTOO A.-MELTZER J.P., *International Data Flows and Privacy: The Conflict and Its Resolution*, in *Journal of International Economic Law*, Dicembre 2018, Volume 21, Numero 4, pp. 769-789.

MCKINSEY GLOBAL INSTITUTE, *Digital Globalization: The New Era of Global Flows*, McKinsey&Company, Marzo 2016.

MCKINSEY GLOBAL INSTITUTE, *Globalization in Transition: The Future of Trade and Value Chains*, McKinsey&Company, Gennaio 2019.

MCKINSEY GLOBAL INSTITUTE, *Global flows: The ties that bind in an interconnected world*, McKinsey&Company, Novembre 2022.

MENDEZ M., *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, in *European Papers*, Volume 2, Numero 3, pp. 803-818.

MENEGHETTI M.C., *I trasferimenti di dati personali all'estero*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 594-661.

MENGOZZI P., *Il parere 1/17 della Corte di giustizia UE sul Trattato CETA e il principio di autonomia del diritto UE*, in *Studi sull'integrazione europea*, 2020, Volume XV, Numero 2, pp. 323-338.

MICHAEL J., *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, Dartmouth/UNESCO, Aldershot, 1994.

MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, in *Diritti comparati. Comparare i diritti fondamentali in Europa*, 4 dicembre 2014.

MULA D., *Il trattamento dei dati nel territorio dell'Unione e il meccanismo "One Stop Shop"*, in SICA S.-D'ANTONIO V.-RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016, p. 271 ss..

MULAS L., *Il Comprehensive Economic and Trade Agreement (CETA): tra liberalizzazione e regolamentazione prudenziale*, in *Diritto comunitario e degli scambi internazionali*, 2020, Numero 2, pp. 415-449.

NEWMAN A., *Protecting Privacy in Europe: Policy Feedback and Regional Politics*, in MEUNIER S.-MCNAMARA K.R. (a cura di), *The state of the European Union. Vol. 8. Making history: European integration and institutional change at fifty*, Oxford University Press, Oxford, 2007, pp. 123-138.

NINO M., *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il diritto dell'Unione europea*, 2016, Numero 4, pp. 755-787.

NINO M., *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, Volume 14, Numero 3, pp. 733-759.

NOUWT S., *Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, in GUTWIRTH S.-POULLET Y.-DE HERT P.-DE TERWANGNE C.-NOUWT S. (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 275-282.

OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, Numero 176, OECD Publishing, Parigi, 6 aprile 2011.

OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows. A Business Perspective*, in *OECD Digital Economy Papers*, Numero 297, OECD Publishing, Parigi, Agosto 2020.

OGUS A., *Regulation: Legal Form and Economic Theory*, Clarendon Press, Oxford, 1994.

PASQUALI L., *Il contributo dell'accordo UE – Mercosur alla governance internazionale dell'ambiente*, in *Nomos*, Volume 20, Numero 3, 2020, pp. 179-200.

PASQUALI L., *The EU-MERCOSUR Agreement as Source of Development of Specific Global Norms and Standards*, in GARCÍA SEGURA C., IBÁÑEZ J., PAREJA P. (a cura di), *Actores Regionales y Normas Globales: la Unión Europea y los BRICS como Actores Normativos*, Tirant lo Blanch, Valencia, 2021, pp. 131-142.

PETROVA A.P., *The WTO Internet Gambling Dispute as a Case of First Impression: How to Interpret Exceptions Under GATS Article XIV(a) and How to Set the Trend for Implementation and Compliance in WTO Cases Involving "Public Morals" and "Public Order" Concerns?*, in *Richmond Journal of Global Law & Business*, 2006, Volume 6, Numero 1, pp. 45-76.

PICONE P.-LIGUSTRO A., *Diritto dell'organizzazione mondiale del commercio*, CEDAM, Padova, 2002.

PIRODDI P., *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in RESTA G.-ZENO-ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 169-213.

POLLICINO O., *L'"autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, 16 ottobre 2019, Numero 19.

POLLICINO O.-BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel reasoning*

dei giudici di Lussemburgo, in Resta G.-Zeno-Zencovich V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 73-112.

Pollicino O.-Bassini M., *La Corte di giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto penale contemporaneo*, 9 gennaio 2017, p. 9.

Poullet Y., *Transborder Data Flows and Extraterritoriality: The European Position*, in *Journal of International Commercial Law & Technology*, 2007, Volume 2, Numero 3, pp. 141-153.

Poullet Y., Gutwirth S., *The Contribution of the article 29 Working Party to the construction of a harmonised European Data Protection System; an Illustration of 'Reflexive Governance'?*, in Perez Asinari M.V.-Palazzi P. (a cura di), *Défis du droit a la protection de la vie privée. Challenges of privacy and data protection law*, Bruylant, Bruxelles, 2008, pp. 570-610.

Pupalova N., *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?*, University of Oslo, Oslo, 2017.

Raghavan C., *Financial Services, the WTO and Initiatives for Global Financial Reform*, in Sundaram J.K. (a cura di), *Reforming the International Financial System for Development*, Columbia University Press, New York, pp. 218-242.

Reidenberg J.R., *E-Commerce and Trans-Atlantic Privacy*, in *Houston Law Review*, 2001, Volume 38, Numero 3, pp. 717-749.

Rentzhog M.-Jonströmer H., *No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, Kommerskollegium, Stoccolma, Gennaio 2014.

Resta G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in Resta G.-Zeno-Zencovich V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 23-48.

Reyes C.L., *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, in *Melbourne Journal of International Law*, 2011, Volume 12, Numero 1, pp. 1-36.

Ricci A., *I diritti dell'interessato*, in Finocchiaro G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 392-472.

Riccio G.M., *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in Resta G.-Zeno-Zencovich V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 215-238.

Rodotà S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e diritto privato*, 2004, Numero 1, pp. 1-12.

Rodotà S., *Data Protection as a Fundamental Right*, in Gutwirth S.-Poullet Y.-De Hert P.-De Terwangne C.-Nouwt S. (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 77-82.

Rouvroy A.-Poullet Y., *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in Gutwirth S.-Poullet Y.-De Hert P.-De Terwangne C.-Nouwt S. (a cura di), *Reinventing Data Protection?*, Springer, New York, 2009, pp. 45-76.

Ruotolo G.M., *La disciplina multilaterale del commercio digitale*, in *Diritto pubblico comparato ed europeo*, 2014, Numero 4, pp. 1887-1919.

Ruschemeier H., *Nothing new in the west? The executive order on US surveillance activities and the GDPR*, in *European Law Blog*, 14 novembre 2022.

SALUZZO S., *Tutela dei dati personali e deroghe in materia di sicurezza nazionale dopo l'entrata in vigore del Privacy Shield*, in *SIDIBlog*, 13 settembre 2016.

SCHÄFER H.B.-OTT C., *The Economic Analysis of Civil Law*, Edward Elgar Publishing, Cheltenham, 2000.

SCHRIEBERG D., *E.U. Hoping New Data Protection Under GDPR Will Have Global Impact*, in *www.forbes.com*, 11 febbraio 2018.

SCHROPP S.A.B.-PALMETER D., *Commentary on the Appellate Body Report in EC–Bananas III (Article 21.5): waiver-thin, or lock, stock, and metric ton?*, in *World Trade Review*, 2010, Volume 9, Numero 1, pp. 7-57

SCHWARTZ P., *Data Processing and Government Administration: The Failure of the American Response to the Computer*, in *Hastings Law Journal*, 1992, Volume 43, Numero 5, pp. 1321-1389.

SCHWEITZER F.J.-SACCOMANNO I.-SAIKA N.N., *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade – Part 1*, in *The Global Trade Law Journal*, 2024, Volume 1, Numero 2.

SCORZA G., *Executive order di Biden, ecco i punti critici, quelli positivi e quelli da chiarire*, in *AgendaDigitale*, 10 ottobre 2022.

SCOTT M., *Digital Bridge: Transatlantic competition – Washington's privacy plan – Microsoft lobbying*, in *www.politico.eu*, 2 dicembre 2021.

SEMERTZI A., *The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements*, in *Common Market Law Review*, 2014, Volume 51, Numero 4, pp. 1125-1158.

SICA S.-D'ANTONIO V., *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in RESTA G.-ZENO-ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, pp. 137-167.

SICA S.-D'ANTONIO V.-RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, CEDAM, Padova, 2016.

SOUSA DE JESUS A., *Data Protection in EU Financial Services*, ECRI Research Report No. 6, April 2004.

SPANGARO A., *L'ambito di applicazione materiale della disciplina del Regolamento europeo 679/2016*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019, pp. 27-62.

SPILLER E., *La sentenza Tele2 Sverige: verso una* Digital Rule of Law *europea?*, in *IANUS*, 2017, Numero 15-16, pp. 279-309.

SUDA Y., *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy*, Routledge, New York, 2018.

SVANTESSON D.J.B., Article 3. Territorial Scope, in KUNER C.-BYGRAVE L.A.-DOCKSEY C. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 74-99.

SZMIGIERA M., *Biggest companies in the world by market capitalization 2021*, in *www.statista.com*, 10 settembre 2021.

TASSINARI F., *The Externalization of Europe's Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows*, in *Peace & Security – Paix et Sécurité Internationales*, 2021, Numero 9.

TERPAN F., *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?*, in *European Papers*, 2018, Volume 3, Numero 3, pp. 1045-1059.

THE ECONOMIST, *The world's most valuable resource is no longer oil, but data*, in *www.economist.com*, 6 maggio 2017.

TRACOL X., *Le règlement et la directive relatifs à la protection des données à caractère personnel*, in *Europe: actualité du droit de l'Union européenne*, 2016, Volume 26, Numero 10, pp. 5-10.

TZANOU M., *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, Oxford, 2017.

UNCTAD, *Information Economy Report 2009 – Trends and Outlook in Turbulent Times*, United Nations Publication, New York/Ginevra, 2009.

UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, United Nations Publication, New York/Ginevra, 2016.

VAN DER MAREL E., *Disentangling the Flows of Data: Inside or Outside the Multinational Company?*, ECIPE OCCASIONAL PAPER No. 7, 2015.

VELLI F., *The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements*, in *European Papers*, 2019, Volume 4, Numero 3, pp. 881-894.

VENTURINI G. (a cura di), *L'Organizzazione Mondiale del Commercio*, Giuffrè, Milano, 2015.

VON DER LEYEN U., *Un'Unione più ambiziosa. Il mio programma per l'Europa – Orientamenti politici per la prossima Commissione europea 2019-2024*, 2019.

VON DER LEYEN U., *La scelta dell'Europa – Orientamenti politici per la prossima Commissione europea 2024-2029*, Strasburgo, 18 luglio 2024.

VOON T., *China and Cultural Products at the WTO*, in *Legal Issues of Economic Integration*, 2010, Volume 37, Numero 3, pp. 253-259.

WANG F.Y., *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, in *Harvard Journal of Law & Technology*, 2020, Volume 33, Numero 2, pp. 661-691.

WARREN S.D.-BRANDEIS L.D., *The Right to Privacy*, in *Harvard Law Review*, 15 dicembre 1890, Volume 4, Numero 5, pp. 193-220.

WEISS M.A.-ARCHICK K., *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shiel*d, Congressional Research Service Report, 19 maggio 2016.

WESSEL A., *CETA will harm our privacy*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 15 aprile 2016.

WESSEL A., *CETA: ISDS and data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 29 aprile 2016.

WESSEL A., *Broken data protection in EU trade agreements*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 22 settembre 2016.

WESSEL A., *EU-Japan trade agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 10 gennaio 2018.

WESSEL A., *EU-Singapore Trade Agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 19 aprile 2018.

WESSEL A., *Weak Data Protection in EU-Vietnam Trade Agreement*, in *Blog Van Vrijschrift*, 6 febbraio 2020.

WOOLCOCK S., *European Union policy towards Free Trade Agreements*, ECIPE WORKING PAPER No. 3, 2007.

WRIGHT D.-DE HERT P.-GUTWIRTH S., *Are the OECD Guidelines at 30 Showing Their Age?*, in *Communications of the ACM (Association for Computing Machinery)*, 2011, Volume 54, Numero 2, pp. 119-127.

YAKOVLEVA S., *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, in *World Trade Review*, Luglio 2018, Volume 17, Numero 3, pp. 477-508.

YAKOVLEVA S., *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, in *The Journal of World Investment & Trade*, 2020, Volume 21, Numero 6, pp. 881-919.

YAKOVLEVA S., *GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives*, in *European Law Blog*, 9 dicembre 2021.

YAKOVLEVA S., *Editorial: On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows*, in *Legal Issues of Economic Integration*, 2022, Volume 49, Numero 4, pp. 339-348.

YAKOVLEVA S., *EU's trade policy on cross-border data flows in the global landscape: navigating the thin line between liberalizing digital trade, "digital sovereignty" and multilateralism*, Institute for Information Law Research Paper No. 2022-12, Amsterdam, 2022.

YAKOVLEVA S., *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, Institute for Information Law Research Paper No. 2022-09, Amsterdam, 2022.

YAKOVLEVA S.-IRION K., *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 2016, Volume 2, Numero 2, pp. 191-208.

YAKOVLEVA S.-IRION K., *Pitching trade against privacy: reconciling EU governance of personal data flows with external trade*, in *International Data Privacy Law*, 2020, Volume 10, Numero 3, pp. 201-221.

YAKOVLEVA S.-IRION K., *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, in *AJIL Unbound*, 2020, Volume 114, pp. 10-14.

YAKOVLEVA S.-VAN HOBOKEN J., *The Algorithmic Learning Deficit: Artificial Intelligence, Data Protection, and Trade*, Institute for Information Law Research Paper No. 2022-10, Amsterdam, 2022.

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

COLLANA DEL DIPARTIMENTO DI GIURISPRUDENZA
DELL'UNIVERSITÀ DI PISA

Volumi pubblicati

1. V. Casamassima, *L'opposizione in Parlamento. Le esperienze britannica e italiana a confronto*, 2013, pp. XXII-546.
2. F. Biondi Dal Monte, *Dai diritti sociali alla cittadinanza. La condizione giuridica dello straniero tra ordinamento italiano e prospettive sovranazionali*, 2013, pp. XVI-320.
3. AA.VV., *Libertà dal carcere, libertà nel carcere*, 2013, pp. XXVIII-452.
4. AA.VV., Internet *e Costituzione*, 2014, pp. X-374.
5. F. Azzarri, Res perit domino *e diritto europeo. La frantumazione del dogma*, 2014, pp. XVIII-446.
6. C. Murgo, *Il tempo e i diritti. Criticità dell'istituto della prescrizione tra norme interne e fonti europee*, 2014, pp. XII-292.
7. E. Navarretta (a cura di), *La metafora delle fonti e il diritto privato europeo. Giornate di studio per Umberto Breccia*, Pisa, 17-18 ottobre 2013, 2015, pp. XVI-224.
8. M. Nisticò, *L'interpretazione giudiziale nella tensione tra i poteri dello Stato. Contributo al dibattito sui confini della giurisdizione*, 2015, pp. XIV-326.
9. AA.VV., *Stupefacenti e diritto penale: un rapporto di non lieve entità*, a cura di G. Morgante, 2015, pp. XII-276.
10. M. Passalacqua (a cura di), *Il «disordine» dei servizi pubblici locali. Dalla promozione del mercato ai vincoli di finanza pubblica*, 2015, pp. XVIII-398.
11. C. Favilli, *La responsabilità adeguata alla famiglia*, 2015, pp. XVI-528.
12. L. Pasquali, *Multilinguismo negli atti normativi internazionali e necessità di soluzioni interpretative differenziate*, 2016, pp. X-198.
13. M. Del Chicca, *La pirateria marittima. Evoluzione di un crimine antico*, 2016, pp. X-294.
14. G. De Francesco-E. Marzaduri (a cura di), *Il reato lungo gli impervi sentieri del processo*, Atti dell'Incontro di studi svoltosi a Pisa il 26 febbraio 2016, 2016, pp. X-222.
15. A. Landi-A. Petrucci (a cura di), *Pluralismo delle fonti e metamorfosi del diritto soggettivo nella storia della cultura giuridica*, vol. I, *La prospettiva storica*, 2016, pp. X-242.
16. I. Belloni-T. Greco-L. Milazzo (a cura di), *Pluralismo delle fonti e metamorfosi del diritto soggettivo nella storia della cultura giuridica*, vol. II, *La prospettiva filosofica: teorie dei diritti e questioni di fine vita*, 2016, pp. XII-164.
17. A. Fioritto (a cura di), *Nuove forme e nuove discipline del partenariato pubblico privato*, 2016, pp. XIV-490.

18. A. Landi, *Dalla gratuità necessaria alla presunzione di onerosità*, I, *Il mutuo ad interesse dal tardo Diritto comune alla codificazione civile italiana del 1865*, 2017, pp. VIII-160.
19. A.M. Calamia (a cura di), *L'abuso del diritto. Casi scelti tra principi, regole e giurisprudenza*, 2017, pp. XII-276.
20. C. Napoli, *Spoyls system e Costituzione. Contributo allo studio dei rapporti tra politica ed amministrazione*, 2017, pp. X-218.
21. C.J. Piernas-L. Pasquali-F.P. Vives (edited by), *Solidarity and Protection of Individuals in E.U. Law. Addressing new challenges of the Union*, 2017, pp. XVIII-326.

Nuova Serie

Monografie

22. G. Donadio, *Modelli e questioni di diritto contrattuale antidiscriminatorio*, 2017, pp. X-214.
23. A. Cassarino, *Il* vocare in tributum *nelle fonti classiche e bizantine*, 2018, pp. X-214.
24. E. Bacciardi, *Il recesso del consumatore nell'orizzonte delle scienze comportamentali*, 2019, pp. VIII-256.
25. A. Grillone, *La gestione immobiliare urbana tra la tarda Repubblica e l'età dei Severi. Profili giuridici*, con prefazione di Luigi Capogrossi Colognesi, 2019, pp. XVIII-246.
26. M. Pedone, Per argentarium solvere. *Ricerche sul* receptum argentarii, 2020, pp. X-198.
27. F. Procchi, *Profili giuridici delle* insulae *a Roma antica. I. Contesto urbano, esigenze abitative ed investimenti immobiliari tra tarda Repubblica ed Alto impero*, 2020, pp. XXIV-248.
28. C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, 2020, pp. XII-252.
29. G. Donadio, *Gli accordi per la crisi di coppia tra autonomia e giustizia*, 2020, pp. X-206.
30. G. Famiglietti, *Il richiedente protezione internazionale davanti ai suoi "giudici"*, 2021, pp. X-294.
31. S. Campanella, *Malattia psichiatrica e pericolosità sociale: tra sistema penale e servizi sanitari*, 2021, pp. X-390.
32. A. Petrucci, *Organizzazione ed esercizio delle attività economiche nell'esperienza giuridica romana. I dati delle fonti e le più recenti vedute dei moderni*, 2021, pp. VIII-312.
33. M. Monti, *Federalismo disintegrativo? Secessione e asimmetria in Italia e Spagna*, 2021, pp. VIII-456.

34. D. Perrone, *La prognosi postuma tra distorsioni cognitive e* software *predittivi. Limiti e possibilità del ricorso alla "giustizia digitale integrata" in sede di accertamento della colpa*, 2021, pp. X-142.
35. A. Montesano, *Le assicurazioni marittime obbligatorie*. Blue cards *e attività di certificazione*, 2023, pp. XII-260.
36. G. Battaglia, Amici curiae *e giudizio incidentale sulle leggi. Contributo allo studio della recente "apertura" della Corte, anche nella prospettiva della tutela multilivello dei diritti*, 2024, pp. XVI-232.
37. F. Nugnes, *Povertà abitativa e Costituzione. Nuovi itinerari di ricerca*, 2024, pp. VI-282.
38. G. Spanò, *Un modello islamico? Sistemi e paradigmi macro-comparati oltre la* Rule of (Traditional) Law, 2024, pp. VI-226.
39. G. Rugani, *La regolamentazione dei flussi di dati personali dall'UE verso Paesi terzi. Alla ricerca di un bilanciamento tra espansione del commercio internazionale e* personal data protection, 2024, pp. XII-228.

Saggi e ricerche

1. E. Navarretta, *Costituzione, Europa e diritto privato. Effettività e* Drittwirkung *ripensando la complessità giuridica*, 2017, pp. XVI-228.
2. E. Navarretta (a cura di), *Effettività e* Drittwirkung *nelle discipline di settore. Diritti civili, diritti sociali, diritto al cibo e alla sicurezza alimentare*, 2017, pp. VI-298.
3. M. Passalacqua-B. Pozzo (a cura di), *Diritto e rigenerazione dei* Brownfields. *Amministrazione, obblighi civilistici, tutele*, 2019, pp. XXXII-744.
4. A. Petrucci (a cura di), *I rapporti fiduciari: temi e problemi*, 2020, pp. XVIII-382.
5. A. Montesano (a cura di), *Sicurezza della navigazione e tutela dell'ambiente marino nelle Bocche di Bonifacio*, 2021, pp. XIV-322.
6. A. Montesano (a cura di), *Concessioni e trasporti. Procedure di affidamento e attività di vigilanza sulla gestione concessoria*, 2024, pp. VIII-176.
7. A. Cassarino (a cura di), *Morte, discendenza, eredità. Una storia umana tra natura, cultura e diritto*, 2024, pp. VIII-232.

Atti di Convegno

1. E. Navarretta (a cura di), *Effettività e* Drittwirkung*: idee a confronto. Atti del convegno di Pisa, 24-25 febbraio 2017*, 2017, pp. X-254.
2. A. Pertici-M. Trapani (a cura di), *La prevenzione della corruzione. Quadro normativo e strumenti di un sistema in evoluzione*. Atti del convegno di Pisa, 5 ottobre 2018, 2019, pp. XIV-266.
3. G. De Francesco-A. Gargani-D. Notaro-A. Vallini (a cura di), *La tutela della per-*

sona umana. *Dignità*, *salute*, *scelte di libertà (per Francesco Palazzo)*, Atti del Convegno di Pisa, 12 ottobre 2018, 2019, pp. XXII-282.

4. G. De Francesco-A. Gargani-E. Marzaduri-D. Notaro (a cura di), *Istanze di deflazione tra coerenza dogmatica*, *funzionalità applicativa e principi di garanzia*, Atti dell'incontro di studi di Pisa, 22 marzo 2019, 2020, pp. X-246.
5. V. Pinto (a cura di), *Crisi di impresa e continuità aziendale: problemi e prospettive*, Atti dell'incontro di studi, Pisa, 7 febbraio 2020, 2020, pp. X-190.
6. E. Navarretta (a cura di), *La funzione delle norme generali sui contratti e sugli atti di autonomia privata*. *Prospettive di riforma del Codice civile*, Atti del Convegno, Pisa, 29, 30 novembre e 1° dicembre 2018, 2021, pp. XII-428.
7. M. Bevilacqua-L. Notaro-G. Profeta-L. Ricci-A. Savarino (a cura di), *Malattia psichiatrica e pericolosità sociale*. *Tra sistema penale e servizi sanitari*, Atti del Convegno di Pisa, 16-17 ottobre 2020, 2021, pp. XXVIII-324.

8/I. E. Navarretta-L. Ricci-A. Vallini (a cura di), *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di* blockchain, vol. I, Blockchain*, democrazia e tutela dei diritti fondamentali*, Atti del ciclo di seminari, Pisa, 18 dicembre 2020-30 aprile 2021, 2021, pp. XIV-226.

8/II. E. Navarretta-L. Ricci-A. Vallini (a cura di), *Il potere della tecnica e la funzione del diritto: un'analisi interdisciplinare di* blockchain, vol. II, Blockchain*, mercato e circolazione della ricchezza*, Atti del ciclo di seminari, Pisa, 18 dicembre 2020-30 aprile 2021, 2021, pp. X-262.

9. F. Dal Canto-A. Sperti (a cura di), *Gli strumenti di analisi e di valutazione delle politiche pubbliche*, Atti della giornata di studio svoltasi a Pisa l'11 giugno 2021, 2022, pp. XII-164.
10. A. Bartalena-L. Della Tommasina-G. Iermano-L. Spataro (a cura di), *Enhancing Sustainable Transport*. *Interdisciplinary Issues*, 2022, pp. X-294.
11. P. Albi (a cura di), *Salario minimo e salario giusto*, 2023, pp. XXVI-374.

Finito di stampare nel mese di dicembre 2024
da Stampatre s.r.l., Torino