

GIUSEPPE PROIETTI

IL TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO: PROPORZIONALITÀ, POTERI DELLE AGENZIE DI INTELLIGENCE ED EFFETTO BRUXELLES

SOMMARIO: 1. Premessa. — 2. La normativa in tema di trasferimento all'estero dei dati personali in sintesi. — 3. Il *Privacy Shield* e il caso *Schrems II*. — 3.1. Sul principio di proporzionalità e sui diritti fondamentali sanciti nella Carta UE. — 3.2. Sui criteri di valutazione del livello di protezione ai sensi dell'art. 46 del Regolamento. — 3.3. Sui poteri delle autorità di controllo. — 4. Il caso *Google Analytics*. — 5. L'attuale situazione dei trasferimenti dei dati personali verso gli U.S.A. — 5.1. *Data localization* come possibile soluzione? — 5.2. La soluzione del controllo delle attività di *intelligence*. — 5.3. Il modello ibrido. — 6. La deroga del consenso di cui all'art. 49, lett. a), GDPR come base per il trasferimento. — 7. Il *Trans-Atlantic Data Privacy Framework* e la nuova decisione di adeguatezza. — 7.1. I principi in materia di Privacy nel quadro dell'intesa UE-USA. — 7.2. Le azioni e i rimedi previsti nel DPF. — 7.2.1. Il ricorso innanzi un organismo indipendente designato. — 7.2.2. I ricorsi alle autorità indipendenti nazionali (DPA). — 7.2.3. Il procedimento di arbitrato. — 7.3. I poteri delle agenzie di *intelligence* secondo il nuovo accordo. — 7.3.1. Le limitazioni e le garanzie per la raccolta di dati personali per finalità di sicurezza nazionale. — 7.3.2. Le modalità di utilizzo delle informazioni raccolte. — 7.3.3. La supervisione delle attività di *intelligence*. — 7.3.4. I rimedi esperibili secondo il DPF. — 7.3.5. Gli ulteriori strumenti giurisdizionali secondo il DPF. — 8. Il parere dell'EDPB sull'ultima decisione di adeguatezza relativa agli U.S.A. — 9. Verso *Schrems III*? — 10. La decisione di adeguatezza per il Regno Unito.

1. PREMESSA.

I dati personali e la loro circolazione hanno acquisito un valore economico e strategico straordinario. Quando si discute della loro circolazione in un sistema iperconnesso e transfrontaliero come quello digitale, il loro trasferimento oltre confine assurge a elevati profili di importanza. Le dinamiche giuridiche ed economiche si intersecano con quelle geopolitiche, soprattutto per quei casi in cui lo stato esportatore rientra nella sfera d'influenza di quello importatore.

Gli ultimi anni hanno visto il tema rendersi protagonista di dibattiti dottrinali e di storiche pronunce giurisprudenziali come la più recente *Schrems II* della Corte di Giustizia europea; il fermento che lo coinvolge non si è affatto sopito e gli sviluppi che ne seguiranno incideranno ancora su una parte di quegli equilibri delle relazioni geopolitiche tra gli attori coinvolti. Con questo contributo si tenterà perciò di definire i contorni normativi e le vicende che ne hanno segnato il percorso, con uno sguardo sempre rivolto verso gli orizzonti futuri. Le novità hanno riguardato soprattutto il trasferimento dei dati personali dagli Stati membri UE agli USA, nonché (in tempi più recenti) verso il Regno Unito a seguito del c.d. *Brexit*.

Come si vedrà, non sembrano mancare criticità dalla nuova decisione di adeguatezza riguardante gli Stati Uniti — già segnalate dall'EDPB — e dal processo di riforma del settore nel Regno Unito.

2. LA NORMATIVA IN TEMA DI TRASFERIMENTO ALL'ESTERO DEI DATI PERSONALI IN SINTESI.

Il Regolamento generale sulla protezione dei dati personali nel capo V, ovvero dall'art. 44 all'art. 50, disciplina il trasferimento dei dati personali in un paese terzo o organizzazione internazionale¹.

Il legislatore europeo, senza fornire una esplicita definizione di "trasferimento"², ha previsto tre differenti basi giuridiche perché sia legittima una tale operazione oltre i confini europei, *rectius*, al di là dei confini dello Spazio Economico europeo; ciascuna base è subordinata all'insussistenza dei presupposti prescritti nella precedente, ad eccezione di specifiche deroghe che riguardano trasferimenti occasionali e necessari (art. 49 GDPR).

¹ Per una ampia dissertazione sulla disciplina si veda l'opera di G. RESTA, V. ZENO-ZUNCOVICH (a cura di), *La protezione transnazionale dei dati personali*, in *Consumatori e mercato*, Roma, 2016; si veda altresì: M. MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità int.*, 2016, 4, p. 555; G. M. RICCIO, F. PEZZA, *Trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali*, in Tosi (a cura di) *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

² Si può ritenere, rifacendoci all'art. 12 della Convenzione 108 "sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale",

che si ha "trasferimento" ogni qualvolta in cui un dato personale venga "materialmente" trasferito al di fuori dello Spazio economico europeo. Tuttavia, tale tema ha generato un dibattito, di talché v'è chi ritiene che il GDPR considererebbe solo i flussi dei dati, ma non anche le semplici comunicazioni dei medesimi. Cfr. M.C. MENEGHETTI, *L'adeguatezza dei trasferimenti di dati personali negli USA, anche alla luce del nuovo Regolamento privacy*, in *giustiziacivile.com*, 2017, 9. La questione è stata resa più complessa anche per la diffusione dei nuovi mezzi di comunicazione che rendono labile proprio il concetto di trasferimento materiale come financo testimoniato dalla pronuncia della CGUE del 6 novembre 2003, C-101/01, sul caso *Lindqvist*, consultabile su eur-lex.europa.eu.

La prima base giuridica che legittima il trasferimento transfrontaliero dei dati personali è disciplinata dall'art. 45 GDPR e riguarda le ipotesi in cui sia intervenuta la Commissione europea attraverso l'adozione di una decisione di adeguatezza. Siffatto atto, vincolante per tutti gli Stati membri destinatari ai sensi dell'art. 288, par. 4, TFUE³, presuppone che vi sia stato un esame della normativa del paese terzo in questione e che tale procedimento abbia fornito un esito positivo, nel senso che l'ordinamento giuridico di tale Stato offrirebbe un livello di protezione dei dati personali equivalente a quello europeo.

La Commissione europea, che ogni quattro anni deve sottoporre a riesame la decisione adottata, valuta l'adeguatezza del sistema giuridico del paese terzo alla luce di una serie di elementi enucleati, a titolo esemplificativo, nel secondo paragrafo dell'art. 45 GDPR. Tra tali elementi occorre tener in considerazione lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale, le norme in materia di protezione dei dati, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale. Inoltre, deve essere valutata l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti, nonché gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale, in particolare in relazione alla protezione dei dati personali.

La decisione di adeguatezza disciplinata nel GDPR deve essere tenuta distinta rispetto a quella prevista dalla direttiva UE 2016/680⁴ riguardante la 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 penali⁵.

Nel caso in cui non sia stata adottata una specifica decisione di adeguatezza — oppure nel caso di sua revoca o invalidità —

³ Ai sensi del par. 4 dell'art. 288 del Trattato «La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi».

⁴ L'art. 36, par. 1, della direttiva prevede che gli Stati membri dispongono che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia 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 garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

⁵ Le decisioni di adeguatezza dei LED

dovrebbero tenere conto del loro contesto specifico e soprattutto dei diritti fondamentali che intendono proteggere. Perciò, le decisioni di adeguatezza previste dalla direttiva in questione dovrebbero essere adottate con attenzione, non limitandosi a ricalcare lo schema applicato nelle decisioni di adeguatezza del GDPR. Una tale distinzione ha il vantaggio di poter dedicare la giusta rilevanza a questioni di particolare importanza per la protezione dei dati come la presunzione di innocenza e il diritto a un processo equo per l'uso di algoritmi nelle attività di polizia e/o nelle sentenze. Così L. DRECHSLER, *Comparing LED and GDPR Adequacy: One Standard Two Systems*, in *Global privacy law review*, vol. 1, 2020, 2, p. 103.

soccorre il successivo art. 46 che prevede la possibilità di procedere ugualmente al trasferimento dei dati personali qualora siano state adottate adeguate misure volte a garantire una tutela sostanzialmente equivalente a quella europea⁶. In altri termini, le misure in questione devono sopperire a quel *vulnus* di tutela che emerge da una comparazione dei sistemi giuridici tra i due Stati.

Lo stesso articolo elenca una serie di strumenti di trasferimento contenenti “garanzie adeguate” di cui possono avvalersi gli esportatori per trasferire i dati personali verso paesi terzi. Queste garanzie possono essere a loro volta suddivise in due categorie: quelle che non necessitano di autorizzazione da parte del Garante dei dati personali e quelle che, viceversa, necessitano di una preventiva autorizzazione.

Nella prima, rientrano le clausole contrattuali tipo di protezione dei dati⁷, le norme vincolanti d’impresa (disciplinate nell’art. 47 GDPR), i codici di condotta, i meccanismi di certificazione e gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici. Nella seconda, invece, le clausole contrattuali *ad hoc* e gli accordi amministrativi tra autorità o organismi pubblici. Queste misure non devono essere intese in senso rigido e automatico. Infatti, l’assetto normativo del paese terzo verso il quale sono trasferiti i dati può comunque richiedere una integrazione di tali strumenti di trasferimento e le garanzie in essi contenute con misure supplementari volte a garantire un livello di protezione sostanzialmente equivalente⁸. La valutazione delle misure da adottare caso per caso, in virtù del principio di *accountability*, che contraddistingue l’intero assetto normativo della materia, è rimessa in primo luogo in capo al titolare e/o al responsabile del trattamento.

L’art. 49 del Regolamento, invece, stabilisce una serie specifica di ipotesi derogatorie per le quali il titolare (o il responsabile) del trattamento può procedere con il trasferimento dei dati anche in mancanza di una decisione di adeguatezza e delle adeguate garanzie di cui all’art. 46 GDPR.

⁶ Sul test di equivalenza, da effettuare sulla base del principio di proporzionalità, secondo alcuni la Corte di Giustizia dovrebbe fornire parametri più chiari individuando le possibili garanzie attuabili dai responsabili. In tal senso, L. DRECHSLER, I. KAMARA, *Essential equivalence as a benchmark for international data transfers after Schrems II*, in *Research Handbook on EU data protection law*, 2022, pp. 351-352.

⁷ Queste vengono adottate dalla Commissione europea con una apposita decisione secondo la procedura d’esame disciplinata all’art. 93, par. 2, del Regolamento. Mentre con la decisione di cui all’art. 45 si deve accertare, con effetto vincolante, e

previo esame della normativa, che un paese terzo garantisce un livello di protezione adeguato, con la decisione relativa alle clausole tipo, la commissione non è tenuta ad una siffatta valutazione dell’adeguatezza del livello di protezione garantito dai paesi terzi verso i quali potrebbero essere trasferiti i dati personali in base alle clausole adottate.

⁸ Si vedano, a tal proposito, le raccomandazioni adottate il 10 novembre 2020 dall’EDPB “*Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell’UE*”, consultabile su edpb.europa.eu.

Le ipotesi in questione, menzionate dalla lett. a) alla lett. g) del primo paragrafo riguardano il caso in cui l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate⁹; il caso di un trasferimento necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; il caso di un trasferimento necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato¹⁰. Le lettere d) ed e) menzionano invece l'ipotesi di un trasferimento necessario per importanti motivi di interesse pubblico, nonché quello volto ad accertare, esercitare o difendere un diritto in sede giudiziaria.

Le ultime due fattispecie, invece, riguardano il trasferimento per la tutela di interessi vitali dell'interessato qualora questi sia in stato di incapacità fisica o giuridica di prestare il proprio consenso e quella di un trasferimento che origini da un registro funzionale a fornire informazioni al pubblico. La disposizione prosegue stabilendo un'ultima e residuale ipotesi in cui sarebbe ammesso un trasferimento transfrontaliero se la fattispecie non rientra neppure in una delle ipotesi summenzionate. Si tratta del caso in cui il trasferimento sarebbe necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento. L'operazione non deve essere ripetitiva e può riguardare un numero limitato di interessati.

Gli Stati Uniti d'America e l'Unione europea hanno vissuto un complicato rapporto sulla questione relativa allo scambio di dati personali dovuto agli interventi della Corte di Giustizia europea che finora ha sempre invalidato gli accordi intercorsi.

3. IL *PRIVACY SHIELD* E IL CASO *SCHREMS II*.

In tema di trasferimento dei dati personali verso gli Stati Uniti si è assistito ad una sequenza di eventi che hanno condotto alla nota sentenza della Corte di Giustizia europea C-311/18 del 16

⁹ Il consenso deve essere specifico, perciò, secondo l'EDPB, non sarebbe possibile ottenerlo in via preventiva per un trasferimento futuro già all'atto della raccolta dei dati; se ad esempio le circostanze specifiche e il trasferimento stesso non sono noti al momento in cui è richiesto il consenso, non è possibile verificarne l'impatto sull'interessato. In questo senso le "Linee guida 2/2018

sulle deroghe di cui all'art. 49 del regolamento 2016/679" del 25 maggio 2018 adottate dall'EDPB, p. 7.

¹⁰ Queste prime tre fattispecie derogatorie, nonché l'ultima riguardante gli interessi legittimi cogenti, non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

luglio 2020, la cd. *Schrems II*, la cui denominazione origina proprio dal nome del ricorrente ¹¹.

Tuttavia, il travagliato rapporto con gli Stati Uniti in materia di trasferimento dati personali ha una origine più risalente poiché, a seguito del ricorso dello stesso Schrems, la Corte di Giustizia era già intervenuta nel 2015 invalidando la precedente decisione di adeguatezza assunta dalla Commissione europea ed emanata sulla base del cd. *Safe Harbour* ¹². Da siffatta pronuncia ne è derivato quindi un successivo accordo, il *Privacy Shield*, in forza del quale la Commissione europea ha adottato la decisione di esecuzione (UE) 2016/1250 del 12 luglio 2016, dichiarata invalida dalla Corte di Giustizia il 16 luglio 2020 proprio con la sopra citata *Schrems II*.

Quest'ultima sentenza è particolarmente rilevante in materia poiché delinea i principi fondamentali in tema di protezione transnazionale dei dati personali definendone i contorni, soprattutto per quanto concerne il profilo relativo all'acquisizione di tali dati da parte di autorità pubbliche del paese terzo ¹³.

Invero, il fulcro della decisione fa perno su una particolare questione caratterizzante l'ordinamento giuridico americano, os-

¹¹ Questa decisione è stata sin da subito criticata da alcuni studiosi americani ritenendola un atto di imperialismo giudiziario e di ipocrisia europea: S. BAKER, *How Can the U.S. Respond to Schrems II?*, *Lawfare*, 21 July 2020; altri operatori del settore hanno sostenuto, in modo suggestivo ma fallace, che la decisione della CGUE non costituirebbe un problema in quanto i dati trasferiti in America, siccome provenienti da una società americana situata in Europa, non rientrerebbero nei programmi di sorveglianza di cui all'art. 702 FISA e E.O. 12333; in questo senso, A. C. RAUL, *Why Schrems II Might Not Be a problem for EU-U.S. Data transfers*, *Lawfare*, 21 Dec. 2020.

¹² Già questa prima pronuncia della Corte ha dato ampio spazio a dibattiti e critiche. C. KUNER, *Reality and illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, vol. 18, 2017, 4, pp. 882-918, si è espresso in senso critico sostenendo che « *EU data protection law (...) maintains the illusion that it can provide seamless, effective protection of EU personal data transferred around the world, a view that the Schrems judgment affirms. This is a beautiful illusion, at least to European eyes, because it envisions a world where the reach of EU data protection law extends globally; where attempts by foreign intelligence agencies to access the data of Europeans are repelled through the use of procedural mechanisms; and where DPAs*

police the Internet and quash attempts to misuse European data ». Secondo l'A. questa illusione è stata confermata dalla stessa sentenza *Schrems* e da una sua successiva applicazione pratica che si è rivelata "limitata" e che non impedisce quelle conseguenze che invero vuole evitare: « *Procedural mechanisms may satisfy formal requirements of data protection law, but they cannot provide protection against the intelligence surveillance that the Schrems case involved. Data localization attempts to minimize or avoid the transfer of personal data to third countries, but cannot protect data transfers on a broad scale. DPAs have a crucial role to play in the protection of personal data, but have a limited ability and willingness to enforce the law across borders, as shown by the fact that there has been very little enforcement related to the Schrems judgment* ».

¹³ A seguito della sentenza *Schrems II* l'EDPB, il 10 novembre 2020, ha pubblicato le "raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza". Con tale documento ha quindi coniato le seguenti quattro garanzie: (a) il trattamento deve basarsi su regole chiare, precise e accessibili; (b) devono essere dimostrate la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti; (c) dovrebbe esistere un meccanismo di controllo indipendente; (d) la persona deve poter accedere a mezzi di ricorso efficaci.

sia l'accesso ai dati europei da parte dei servizi di *intelligence* nell'ambito di appositi programmi di sorveglianza.

La sentenza della Corte enuncia principi sia per l'ambito di applicazione dell'art. 45 del Regolamento, sia per l'ambito di cui all'art. 46, poiché la vicenda giudiziaria è originata quando non era ancora stato raggiunto l'accordo del *Privacy Shield* e la Corte si è quindi pronunciata in merito a più questioni giuridiche.

Come si legge nella stessa sentenza, in base alle informazioni sull'ordinamento giuridico degli Stati Uniti, ivi incluse le dichiarazioni e gli impegni del governo americano, la Commissione aveva ritenuto che «l'ingerenza nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello scudo, compiuta dall'autorità pubblica statunitense per esigenze di sicurezza nazionale, (...) si limitino a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace»¹⁴. Sul punto la Corte di giustizia è stata di contrario avviso, soprattutto sulla base del principio di proporzionalità desumibile dalla Carta UE.

3.1. *Sul principio di proporzionalità e sui diritti fondamentali sanciti nella Carta UE.*

Il *Privacy Shield* è stato dichiarato invalido dalla Corte di giustizia principalmente perché dava origine ad una situazione di incompatibilità con la Carta dei diritti fondamentali europea; tra tali principi — tra cui gli artt. 7 e 8 — l'art. 52 della Carta che contempla il principio di proporzionalità.

In altri termini, secondo tale principio, i diritti e le libertà sancite nella Carta possono subire limitazioni, ma al cospetto di precisi presupposti e solo ove necessari; essi devono inoltre rispondere effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui. La limitazione dei diritti al rispetto della vita privata e alla protezione dei dati deve essere perciò sottoposta ad una verifica a doppio binario: è necessario misurare la gravità dell'ingerenza che la limitazione comporta e valutare l'importanza dell'obiettivo di interesse generale perseguito; quest'ultimo elemento deve essere proporzionato rispetto al primo¹⁵.

¹⁴ In questo senso la Sentenza *Schrems II* nel punto (140) del par. 45.

¹⁵ In questo senso la CGUE, C-511/18, C-512/18, C-520/18, *La Quadrature du Net e a. contro Premier ministre e a.*, consultabile su eur-lex.europa.eu. Con tale pronuncia la Corte ha attribuito un significativo

valore all'obiettivo di salvaguardia della sicurezza nazionale, ritenendolo uno scopo che legittimerebbe le limitazioni dei diritti fondamentali e, in una scala gerarchica, sarebbe sovraordinato per rilevanza anche all'obiettivo del contrasto alla criminalità. Tuttavia, tale giustificazione varrebbe fin-

La normativa che pone limitazioni deve prevedere regole chiare e precise che ne disciplinino la portata e l'applicazione della misura; tali regole debbono prevedere requisiti minimi in modo che gli interessati dispongano di garanzie sufficienti a proteggere i loro dati personali contro il rischio di abusi. L'ordinamento degli Stati Uniti, tuttavia, non si conformerebbe a tale principio.

Il *Privacy Shield*, rileva la Corte, prevedeva che l'adesione ai principi ivi stabiliti a protezione dei dati personali, poteva essere limitata per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia. Tali esigenze, dunque, avevano il primato rispetto ai principi stabiliti in materia di protezione dei dati.

È così emerso che i programmi di sorveglianza PRISM e UPSTREAM, che si fondano sull'art. 702 FISA e sull'E.O. 12333, non rispettando il principio di proporzionalità, non garantirebbero un livello di protezione equivalente a quello sancito all'art. 52, par. 1, Carta UE.

Infatti, l'art. 702 FISA non fa emergere alcuna limitazione all'autorizzazione per l'attuazione dei programmi di sorveglianza ai fini di *intelligence* esterne, né risultano garanzie per i cittadini stranieri potenzialmente oggetto di tali programmi.

Inoltre, la PPD-28¹⁶ non conferirebbe agli interessati alcun diritto nei confronti delle autorità statunitensi azionabili giudizialmente. Ciò vale anche per i programmi di sorveglianza basati sull'E.O. 12333.

La Corte rileva, quindi, che una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva sancito all'art. 47 della Carta UE. Quindi, secondo la Corte, il diritto degli Stati Uniti non garantirebbe un livello di protezione sostanzialmente equivalente a quello garantito dall'art. 47 della Carta.

A tal proposito, non sarebbe neppure sufficiente il meccanismo previsto dal *Privacy Shield* consistente nell'istituzione di un mediatore. Siffatta istituzione, infatti, è stata ritenuta priva del requisito fondamentale dell'indipendenza in quanto risponderebbe direttamente al Segretario di Stato che provvede altresì alla sua designazione, nonché per il fatto che tale organo sarebbe

ché vi siano concrete e valide circostanze che possano far presumere una minaccia grave, reale e attuale alla sicurezza nazionale.

¹⁶ Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities. Questa direttiva, come si legge dal sito uff-

ciale del direttore nazionale di *intelligence* USA « articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes ».

privo di poteri decisorii vincolanti nei confronti dei servizi di *intelligence*.

3.2. *Sui criteri di valutazione del livello di protezione ai sensi dell'art. 46 del Regolamento.*

La Corte di Giustizia ha rilevato che il livello di protezione dei diritti fondamentali richiesto dall'art. 46, par. 1, GDPR deve essere determinato alla luce delle disposizioni dello stesso regolamento, lette in virtù dei diritti fondamentali garantiti dalla Carta.

La valutazione richiesta deve considerare tanto le clausole contrattuali tra il titolare del trattamento e il destinatario del trasferimento (del paese terzo) quanto, in caso di un eventuale accesso delle autorità pubbliche del paese terzo, gli elementi rilevanti di quest'ultimo sistema giuridico.

Gli elementi che devono essere considerati per valutare tale sistema giuridico corrispondono a quelli che, in modo non esaustivo, sono enunciati nel par. 2 dell'art. 45 GDPR¹⁷.

La Corte rileva inoltre che l'art. 46 del Regolamento, facendo parte del capo V, deve essere letto in combinato disposto con l'art. 44 che delinea il principio generale per il trasferimento dei dati. Secondo tale principio, tutte le disposizioni del capo V devono essere applicate senza pregiudicare il livello di protezione garantito dallo stesso Regolamento.

Quindi, la Corte rileva che tale livello di protezione deve 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.

Le clausole tipo di protezione che sono state fatte proprie dal *Privacy Shield*, va da sé, avevano una efficacia di natura obbligatoria, quindi vincolanti solo per i contraenti. Non si prospettava alcuna natura vincolante nei confronti delle autorità pubbliche statunitensi e le clausole che vietano l'accesso legittimo ai dati da parte di autorità pubbliche nell'esercizio delle loro funzioni sono nulle¹⁸. In tal caso, quindi, le circostanze concrete richiederebbero l'adozione di misure supplementari da parte del titolare o del responsabile del trattamento.

¹⁷ Come si è già visto, il riferimento è allo stato di diritto, al rispetto dei diritti umani e delle libertà fondamentali, alla pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come all'attuazione di tale legislazione, alle norme in materia di protezione dei dati, alle norme professionali e alle misure di sicurezza (...); all'esistenza e all'effettivo

funzionamento di una o più autorità di controllo indipendenti nel paese terzo con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati (...); a gli impegni internazionali assunti dal paese terzo in particolare in relazione alla protezione dei dati personali.

¹⁸ L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettiva*, in *Riv. Comm. Int.*, 2021, 3, p. 683.

È lo stesso legislatore europeo che — al considerando 109 del Regolamento — incoraggia i titolari del trattamento a fornire garanzie supplementari che integrino le clausole tipo di protezione dei dati.

3.3. *Sui poteri delle autorità di controllo.*

In mancanza di una decisione di adeguatezza validamente adottata dalla Commissione, l'Autorità di controllo (ai sensi dell'art. 58, par. 2, lett. *f* e *j*) è tenuta a sospendere il trasferimento dei dati personali qualora sulla base delle circostanze proprie del trasferimento, le clausole non siano o non possano essere rispettate nel paese terzo e se la protezione dei dati non possa essere garantita con altri mezzi.

In presenza di una decisione di adeguatezza, invece, stante la loro natura vincolante (*ex art.* 288, par. 4, TFUE) per tutti gli stati membri destinatari, finché la Corte non la dichiari invalida, gli Stati e i loro organi non possono adottare misure contrarie. Tuttavia, la decisione di adeguatezza non impedisce al singolo interessato di ricorrere all'autorità nazionale di controllo, ai sensi dell'art. 77 GDPR. L'autorità in questione potrebbe quindi adire il Tribunale competente e questo, a sua volta, ricorrere con il rinvio pregiudiziale alla Corte di Giustizia europea.

A seguito della sentenza *Schrems II* Stati Uniti e Unione europea hanno intrapreso trattative per giungere ad una intesa che possa portare ad una valida decisione di adeguatezza conformemente ai principi giurisprudenziali delineati.

Le critiche mosse dalla dottrina americana all'orientamento giurisprudenziale europeo (già dalla prima sentenza *Schrems I*) fanno riferimento ad una discutibile discrasia. Si ritiene che l'art. 4, par. 2, TUE, riservando agli stati membri la competenza in materia di sicurezza, renderebbe inapplicabile nei loro confronti la Carta dei diritti fondamentali. Da ciò ne deriverebbe un doppio binario in materia, ossia l'applicabilità di un sistema rigido sul rispetto dei diritti a tutela dei dati per le operazioni di *intelligence* statunitensi rispetto a quello previsto per gli Stati membri UE¹⁹.

Tuttavia, è stato rilevato come una corretta interpretazione della fattispecie renderebbe sempre ammissibile un certo potere di controllo europeo sulla legislazione degli Stati membri ogni qualvolta essa comporti deroghe a diritti connessi e disciplinati dal diritto europeo²⁰. Secondo tale tesi, quindi, l'ambito di applica-

¹⁹ C. KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, cit., p. 881.

²⁰ A. CRISPI, *Sicurezza nazionale e diritti fondamentali alla luce della giurispru-*

denza UE in materia di tutela dei dati personali, in *Riv. Ital. Dir. Pubbl. Comunitario*, 2017, 5, p. 998. L'A. sulla base di giurisprudenza della stessa CGUE, sostiene, p. 1004, che, dato che è « lo stesso trattato

zione della Carta non può essere ancorato a parametri puramente di diritto positivo, bensì all'incidenza del diritto UE e ai suoi scopi ²¹.

4. IL CASO *GOOGLE ANALYTICS*.

Recentemente ha destato l'attenzione di molti operatori del settore anche la decisione assunta dal Garante italiano per la protezione dei dati personali con cui è stata accertata l'illiceità del trattamento dei dati personali degli utenti a mezzo di *Google Analytics* ²². La vicenda ha condotto all'accertamento della violazione degli artt. 5 e 24 GDPR in relazione al principio dell'*accountability*, nonché alla violazione dell'art. 13 in ordine al principio di trasparenza, ossia all'obbligo di rendere edotti gli interessati dell'intenzione di trasferire dati personali a un paese terzo, oltre all'esistenza delle garanzie appropriate.

Il caso ha visto come protagonista una società che si avvaleva della versione gratuita della piattaforma *Google Analytics* per scopi statistici e per l'ottenimento di informazioni aggregate circa l'attività dei propri utenti nel proprio sito web ²³. Lo scopo di avvalersi di tale piattaforma, invero, consiste nel monitoraggio delle campagne di *marketing* sulla base del comportamento e degli interessi dei singoli utenti ²⁴.

In particolare, il Garante ha accertato che i dati raccolti me-

ad attribuire ai paesi membri la competenza in materia di sicurezza (...) l'adozione da parte di questi ultimi di legislazioni interne in tale materia costituisce proprio l'esercizio di una facoltà attribuita loro direttamente dall'UE ed equivale così all'applicazione di una norma comune, il che rende la Carta applicabile nel contesto in esame. (...) Il fatto che la legislazione adottata dagli Stati membri in settori di competenza esclusiva deroghi al diritto UE o possa incidere su quest'ultimo, condizionandone l'applicazione, costituiscono proprio fattori di connessione utili e sufficienti per l'applicazione della Carta ».

²¹ Ivi, p. 1005; M. SAJIAN, *Areas of application of the Charter of fundamental rights of the European Union: fields of conflict?*, in *EUI Working Paper*, 2012, 22, p. 5.

²² Il riferimento è al provvedimento del GPD del 9 giugno 2022, consultabile su [garanteprivacy.it](https://www.garanteprivacy.it).

²³ *Google Analytics* è stato al centro dell'attenzione di diverse Autorità Garanti europee come quella austriaca, francese e danese. A fronte di un'uniformità decisionale da parte delle Autorità citate, nel mese di gennaio 2023 si è pronunciato anche il

Garante spagnolo discostandosi dalla linea delle altre Autorità e rigettando il reclamo proposto. Il provvedimento, emesso ad esito del procedimento E/10529/2021, è consultabile su www.aepd.es/. Con il provvedimento in questione l'Autorità spagnola ha accertato che il Titolare del trattamento, poco dopo essere venuta a conoscenza della sentenza *Schrems II*, ha cessato di utilizzare lo strumento *Google Analytics*. Il Garante ha altresì accertato che il Titolare non ha mai utilizzato le informazioni allo scopo di identificare gli utenti del suo sito web. In base a quanto accertato e alle informazioni disponibili, il titolare non avrebbe, quindi, utilizzato lo strumento in questione.

²⁴ Sulle criticità in termini di *privacy* derivanti dall'utilizzo di sistemi come *Google Analytics*, sia nell'ambito dell'ordinamento statunitense, sia in quello europeo, sebbene non focalizzandosi nello specifico sulla tematica del trasferimento dei dati personali, si era espressa già nel 2010 parte della dottrina americana: R. LIEBER, K. CHANEY, *Google Analytics: Analyzing the Latest Wave of Legal Concerns for Google in the US and the EU*, in *Buffalo Intellectual Property Law Journal*, 2010, 7, p. 135. È stato rilevato come « *the future of web analytics*

dante *cookies* consistono in « identificatori online unici che consentono sia l'identificazione del browser o del dispositivo dell'utente che visita il sito web, sia del gestore stesso del sito (attraverso l'ID account Google); indirizzo, nome del sito web e dati di navigazione; indirizzo IP del dispositivo utilizzato dall'utente; informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata, nonché a data e ora della visita al sito web ». Nel caso in cui l'utente effettuasse l'accesso mediante l'*account* Google, ai suddetti dati andrebbero aggiunti tutti quelli già contenuti nell'*account* di riferimento.

L'autorità di controllo, quindi, accertato che i suddetti dati erano oggetto di trasferimento in un paese terzo, ovvero gli Stati Uniti, per il tramite di Google Ireland Limited quale responsabile del trattamento, si è interrogata sull'esistenza di adeguate misure supplementari volte ad ottenere una adeguata protezione dei dati personali.

A tal proposito, è stato rilevato come le misure supplementari di natura tecnica, nel caso di specie, non fossero adeguate. Infatti, il meccanismo utilizzato consisteva nella cifratura dei dati, la quale tuttavia non si dimostrava sufficiente in quanto il sistema giuridico statunitense consente alle autorità pubbliche l'accesso non solo ai dati personali importati, bensì anche alle chiavi crittografiche necessarie alla loro decodificazione.

Pertanto, dal momento che la disponibilità della chiave di cifratura è detenuta dall'importatore Google LLC, le autorità statunitensi sarebbero in grado di rendere intellegibili anche i dati cifrati. Ciò renderebbe evidente l'inadeguatezza delle misure attuate dal titolare del trattamento.

L'assenza di idonee misure tecniche, inoltre, comporterebbe, secondo il Garante, la conseguente inadeguatezza anche delle ulteriori misure di natura contrattuale e organizzativa ²⁵.

— as a tool and as an industry — will continue to evolve as behavioral targeted marketing and social media become more commonly utilized by companies, organizations, and governments. In addition, Google Analytics's widespread use in the industry will likely continue unabated, thanks in part to its open source status and relative ease of use. But as we have discussed, privacy advocates will continue to raise concerns in the United States, the European Union, and Germany ». Tra le soluzioni proposte, oltre a una sensibilizzazione e formazione dell'utente sull'importanza di un corretto uso dei propri dati personali, vengono fatte proprie anche delle raccomandazioni di organizzazioni statunitensi se-

condo cui: « (...) the providers of measurement tools must build their products to higher privacy standards than what currently exists in the commercial sector. Agencies must craft robust policies to ensure that data collected for measurement purposes is adequately safeguarded. And the [] policies on persistent tracking technologies must be adapted to continue to establish the highest levels of privacy protection while accounting for recent technological advances ».

²⁵ A tal proposito l'Autorità fa rinvio a quanto contenuto nella Raccomandazione EDPB 1/2020 relativa alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di prote-

La decisione del garante è stata dirompente nel mercato delle piattaforme che acquisiscono, elaborano e trasferiscono dati personali e, sebbene sia stata superata dalla nuova decisione di adeguatezza che si vedrà successivamente, potrebbe rappresentare un precedente che delinea principi applicabili in un'ottica futura o presente per altri Stati.

5. L'ATTUALE SITUAZIONE DEI TRASFERIMENTI DEI DATI PERSONALI VERSO GLI U.S.A.

È un dato pressoché indiscusso che la sentenza della CGUE *Schrems II* abbia una portata storica, soprattutto alla luce dell'interdipendenza geopolitica degli stati membri dell'UE rispetto agli Stati Uniti, la quale “non consentirebbe” la sospensione del trasferimento (reciproco) di dati ²⁶.

Il panorama normativo e giurisprudenziale delineato ci pone l'interrogativo su quale sia la situazione attuale dopo le storiche sentenze della Corte di Giustizia e quali sarebbero — al netto della nuova decisione di adeguatezza della Commissione europea n. 1795/2023 — le possibili soluzioni, visto che il sistema composto dalle clausole tipo di protezione non può considerarsi sufficiente per la loro natura non vincolante nei confronti delle autorità pubbliche ²⁷. Molti operatori digitali, inclusa la società protagonista della vicenda *Schrems II*, hanno insistito con l'utilizzo delle clausole tipo nonostante i principi stabiliti dalla Corte di Giustizia europea sul punto, senza adottare alcuna misura supplementare a protezione dei dati personali.

Una delle soluzioni prospettata in letteratura, va da sé, è rappresentata dalla riforma della legislazione americana in tema di sorveglianza e di servizi di *intelligence* ²⁸.

zione dei dati personali dell'UE, 18 giugno 2021, par. 53 secondo cui « le misure contrattuali e organizzative, da sole, non riescono in genere a evitare l'accesso ai dati personali da parte delle autorità pubbliche del paese terzo in forza di una legislazione e/o di prassi problematiche. Vi saranno infatti situazioni in cui solo misure tecniche adeguatamente attuate potrebbero impedire o rendere inefficace l'accesso ai dati personali da parte delle autorità pubbliche dei paesi terzi, in particolare a fini di sorveglianza. In tali situazioni, le misure contrattuali o organizzative possono integrare le misure tecniche e rafforzare il livello generale di protezione dei dati, ad esempio introducendo controlli ed eliminando automatismi in relazione ai tentativi delle autorità pubbliche di accedere ai dati in modo non conforme alle norme dell'Unione ».

²⁶ M. ZALNIERIUTE, *Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security*, in *Vanderbilt Journal of Transnational Law*, vol. 55, 2022, 1, p. 47. L'A. sottolinea il dilemma attuale che vivono gli esportatori di dati, ovvero se trattare i dati personali all'interno dell'Unione europea oppure sollecitare le istituzioni americane ad attuare riforme strutturali in materia che possano rendere il livello di protezione equivalente a quello europeo.

²⁷ G. CHURCHES, M. ZALNIERIUTE, “Contracting Out” *Human rights in International Law: Schrems II and The Fundamental Flaws of U.S. Surveillance Law*, in *Harvard International Law Journal Online*, 2020.

²⁸ B. PROPP, P. SWIRE, *After Schrems II: A Proposal to Meet the Individual Re-*

Tuttavia, secondo alcuni, la riforma della legge statunitense sulla sorveglianza sarebbe difficile ²⁹ o comunque improbabile ³⁰, sebbene sembri essere la soluzione ideale. Una proposta alternativa (poi effettivamente utilizzata) prevederebbe l'uso di ordini esecutivi, sebbene essi siano *deboli* e suscettibili di revoca o modifica dallo stesso Presidente o dal suo successore ³¹.

In ogni caso, gli Stati Uniti, negli ultimi anni, hanno dato segnali positivi, dando vita ad iniziative normative per un quadro legislativo che si avvicina all'approccio europeo del GDPR ³². Sono stati introdotti tre disegni di legge al Congresso americano: a) *the consumer online privacy Act*, del 2019; b) *the consumer Data Privacy and Security Act*, del 2020; c) *the Safe Data Act*, del settembre 2020.

Quest'ultimo, introdotto a seguito della *Schrems II*, sancirebbe alcuni principi che si avvicinano a quelli europei come il diritto di accesso ai dati nonché la richiesta di un consenso esplicito perché si possano acquisire e trasferire dati personali ³³.

Alcuni Stati americani, peraltro, stanno tentando di procedere autonomamente con riforme normative in materia di *privacy*. La California è probabilmente lo Stato più attivo e ambizioso che, con il *California Consumer Act* del 2018 — in vigore dal gennaio del 2020 — prevede, ispirandosi al modello del GDPR, alcune rilevanti novità per i diritti ai consumatori. Tra questi v'è un più pregnante diritto di informazione, il diritto alla cancellazione dei dati personali e il diritto di agire per la tutela dei propri interessi presso il Procuratore Generale della California ³⁴.

Tuttavia, l'iniziativa legislativa più importante è rappresentata dall'*American Data Privacy and Protection Act*, il quale sta facendo discutere perché creerebbe vere e proprie antinomie con

dress Challenge, in *lawfare.com*, 2020, « after Schrems II, the endgame inevitably will include some modification to U.S. surveillance law and practice, specifically to address the clear concerns expressed by the CJEU about lack of individual redress. (...) Any future attempt by the United States to successfully address this perceived deficiency in judicial redress thus must have two dimensions: a credible fact-finding inquiry into classified surveillance activities in order to ensure protection of the individual's rights, and the possibility of appeal to an independent judicial body that can remedy any violation of rights should it occur ».

²⁹ L. CLARKE, *After a Year of Limbo a EU-US Data Privacy Agreement Still Hangs in the Balance*, in *Tech Monitor*, 2021, consultabile su *techmonitor.ai*.

³⁰ M. BURGESS, *Europe's Move Against Google Analytics Is Just the Beginning*, *WIRED*, Jan. 19, 2022, consultabile su *wired.com*.

³¹ W. VOSS, *Transatlantic Data Transfer Compliance*, in *B.U. J. Sci. & Tech. L.*, 2022, 28, p. 177.

³² D. CALIA, *Schrems II: the EU's influence on U.S. data protection and privacy laws*, in *Washington University Global Studies Law Review*, 2022, 21, p. 266.

³³ *Ivi*, p. 268. L'A. pone in dubbio che tali interventi possano portare ad una equivalenza rispetto al diritto europeo.

³⁴ E. TEROLLI, *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in questa rivista, 2021, 1, pp. 63-64.

le vigenti leggi statali, tra tutte la più restrittiva normativa californiana sopra accennata.

I trasferimenti transnazionali di dati sono una delle questioni più complesse nel campo della *privacy*. Tuttavia, come suggerito da parte della dottrina, si tratta anche di un settore in cui è probabile che si verifichino grandi cambiamenti nel medio termine viste le nuove opportunità che saranno dischiuse dalle tecnologie emergenti. Una delle soluzioni è individuata nel “modello dei dati in possesso dell'utente” oltre ad altre opzioni quale ad esempio il progetto europeo di Gaia-X, per « un ecosistema digitale aperto, trasparente e sicuro, in cui i dati e i servizi possono essere resi disponibili, raccolti e condivisi in un ambiente di fiducia »³⁵. Vi sono poi altre soluzioni prospettate come si vedrà qui di seguito.

5.1. Data localization come possibile soluzione?

Una delle soluzioni prospettate in tema di trasferimento dei dati personali verso gli USA a seguito della sentenza della Corte di Giustizia europea è semplice e consiste nel localizzare i dati all'interno dei confini europei. Tale soluzione viene ritenuta l'unica possibile dallo stesso Max Schrems³⁶.

Nella letteratura americana, tuttavia, v'è chi ritiene che tale soluzione non sia adeguata, anzi sarebbe dannosa³⁷. Secondo l'A., anche se i dati non venissero trasferiti negli Stati Uniti, questi ultimi sarebbero comunque in grado, loro stessi o per mezzo di collaborazioni con altre agenzie di *intelligence*, di effettuare operazioni di spionaggio come hanno testimoniato ad esempio le rivelazioni di Edward Snowden. Si sostiene altresì che se i dati rimanessero all'interno dei confini europei, sarebbero comunque soggetti a operazioni di *intelligence* da parte degli apparati dei vari stati membri dell'UE le quali, stando a tale teoria, non sarebbero meno invasive e sarebbero quantitativamente maggiori.

³⁵ P. JURCYS, M.C. COMPAGNUCCI, M. FENWICK, *The Future of International Data Transfers: Managing New Legal Risk with a 'User-Held' Data Model*, in *the Computer Law and Security Review*, Vol. 46, 2022, p. 25. Il modello dei dati in possesso dell'utente consisterebbe in una architettura tecnologica in cui gli individui possono raccogliere e collegare varie fonti di dati alla propria “nuvola di dati personali”. Questi dati possono provenire dagli account online di un individuo o dai dati raccolti da tracker di attività indossabili e dispositivi IoT (come smartwatch, anelli intelligenti, elettrodomestici intelligenti, ecc.). Tale nuvola sarebbe, quindi, un archivio in cui gli individui possono mettere in comune i loro dati

paragonabile a un portafoglio digitale in cui è conservata una copia principale dei dati personali. L'accesso alla nuvola di dati personali sarebbe poi consentito solo al singolo consumatore; i terzi potrebbero accedere a specifici frammenti di dati solo previa autorizzazione dell'individuo.

³⁶ Concludono nello stesso senso C. CHURCHES, M. ZALNIERIUTE, *op. cit.*; viene menzionata come opzione anche da A. MONTERIN, *Dell'incertezza nei trasferimenti di dati personali verso gli Stati Uniti*, in *NGCC*, 2021, 1, p. 160.

³⁷ A. CHANDER, *Is data localization a Solution for Schrems II?*, in *Journal of International Economic Law* 23, 2020, 3, pp. 771-784.

Inoltre, la cd. *data localization* comporterebbe dei costi di transizione maggiori a carico delle piccole società, duplicazioni infrastrutturali e complicazioni relative ad aggiornamenti dei sistemi nonché in tema di *cybersecurity*; oltre a creare tensioni tra Stati che sono tra loro *partner* commerciali.

Tale tesi, tuttavia, appare discutibile sotto molti aspetti poiché, al netto di questioni piuttosto politiche o di opportunità, tralascia il fulcro dei principi delineati dalla sentenza *Schrems II*. Con tale pronuncia si è sottolineata l'inadeguatezza del sistema giuridico del paese terzo non tanto per operazioni di *intelligence* in sé per sé, bensì per l'assenza di rimedi giuridici azionabili dall'interessato, nonché di una autorità indipendente in grado di vigilare ed emettere decisioni vincolanti nei confronti degli apparati statali in caso di violazioni di legge. Tale sistema, per contro, è presente negli Stati europei. Le attività di *intelligence* oltreoceano, inoltre, sono state valutate non rispondenti al principio di proporzionalità che, viceversa, costituisce un cardine degli stati membri UE sancito nella carta europea dei diritti fondamentali e consente di operare un controllo affinché le operazioni dei vari apparati siano limitate e sottoposte a specifiche regole stabilite *ex lege*.

Va da sé che la portata pratica della misura di *Data Localization* sarebbe tutta da verificare, ovvero se possa rivelarsi efficace solo in contesti isolati e non di larga scala³⁸. La questione delicata, che rimane aperta, non sembrerebbe essere solo di natura giuridica ma anche geopolitica, visti i rapporti esistenti tra gli Stati UE e gli USA.

5.2. La soluzione del controllo delle attività di *intelligence*.

Un'altra soluzione che è stata prospettata, in un'ottica *de iure condendo* e relativa al sistema statunitense, interviene anche in merito al sistema di controllo delle operazioni compiute dagli apparati americani che la Corte di giustizia ha valutato insufficiente bocciando altresì l'istituzione del Mediatore. Essa consiste nel concepire un sistema di rimedi per l'interessato a fronte di casi di abusi nell'attività di sorveglianza in cui un primo accertamento

³⁸ C. KUNER, *op. cit.*, p. 914, sostiene che una tale misura non possa essere considerata in grado di fornire una protezione completa in relazione all'accesso da parte dei servizi di *intelligence*. Come emerso dalle rivelazioni di E. Snowden, esiste un'ampia condivisione di dati tra i servizi di *intelligence* dell'UE e quelli di Paesi terzi, in particolare i servizi statunitensi e quelli della rete di condivisione di *intelligence* "Five Eyes". Ciò suggerisce che la condivisione dei dati è condotta su vasta scala tra le agenzie di *intelligence* di molti Paesi e che

una volta che i dati sono accessibili da un'agenzia, possono essere resi disponibili a quelle di altri Paesi, in modo che il luogo del server in cui i dati sono memorizzati può essere in gran parte irrilevante per l'accesso ai servizi di *intelligence*. Inoltre, l'A. sottolinea come non sia chiaro se il luogo di archiviazione dei dati influisca sulle capacità tecniche dei servizi di *intelligence* di paesi terzi di accedere ai dati archiviati nell'UE, data la natura globale del trattamento dei dati.

— con precisi *standard* validi sia per i cittadini statunitensi che europei — potrebbe essere condotto dagli attuali organismi preposti a tutela della privacy³⁹, ossia i *civil liberties officers* (PCLO)⁴⁰, oppure coinvolgendo il *Privacy and Civil Liberties Oversight Board* (PCLOB)⁴¹.

Tuttavia, allo stato attuale, tali organi non possiedono le caratteristiche di indipendenza richieste essendo legate al ramo esecutivo; pertanto, le decisioni delle agenzie andrebbero poi sottoposte al vaglio di un giudice federale indipendente⁴². Un meccanismo di ricorso come quello prospettato, tra l'altro, deve garantire una più semplice legittimazione ad agire rispetto al sistema attuale; in questo senso, viene suggerito un meccanismo simile a quello che viene attualmente utilizzato nell'ambito del *Freedom of Information Act* (FOIA) statunitense in forza del quale ogni individuo può chiedere a un'agenzia di produrre documenti senza dover dimostrare di aver subito un particolare pregiudizio. Al pari delle altre decisioni del FISC, si dovrebbe concedere poi di ricorrere al *Foreign Intelligence Surveillance Court of Review* e infine alla Corte Suprema degli Stati Uniti.

5.3. Il modello ibrido.

Una ulteriore opzione prospettata dalla dottrina americana risiede nel creare un modello ibrido attraverso una cooperazione internazionale che combini un approccio fondato sul rischio nel trasferimento dei dati con un sostanziale e istituzionale controllo sulla sorveglianza statunitense⁴³.

Tale modello dovrebbe giungere, sulla base di specifici criteri di valutazione, alla creazione di differenti gruppi che consentano una classificazione in base al rischio di esportazione dei dati; a seconda del gruppo di appartenenza dovrebbero quindi essere adottate differenti politiche e misure da parte dell'esportatore e

³⁹ In questo senso, K. PROPP, P. SWIRE, op.cit., *lawfare.com*, 2020.

⁴⁰ Tali organi hanno già la responsabilità statutaria di indagare e affrontare i reclami sulle violazioni della *privacy* e delle libertà civili.

⁴¹ Si tratta di una piccola agenzia federale attualmente incaricata di proteggere tali interessi in relazione ai programmi antiterrorismo statunitensi e hanno accesso ai *database Top Secret* e ad altri *database* classificati. Tuttavia, la normativa vigente limita l'idoneità del PCLOB per lo svolgimento di questo compito. Infatti, le sue funzioni riguardano solo la supervisione e la politica a livello programmatico, non le indagini sulle singole denunce già condotte dai

PCLO. Inoltre, il suo mandato è limitato al solo terrorismo, non includendo il controspionaggio, altri tipi di minacce dello Stato nazionale e altri aspetti della sicurezza nazionale.

⁴² Gli autori individuano nella *Foreign Intelligence Surveillance Court* (FISC) il giudice più adeguato a tale controllo grazie alla sua competenza specialistica nella legge sulla sorveglianza degli Stati Uniti e alle procedure consolidate per trattare questioni classificate.

⁴³ I. RUBINSTEIN, P. MARGULIES, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the search for Common Ground*, in *Connecticut Law Review*, Vol. 54, 2022, 4, p. 395.

dell'importatore⁴⁴. Una possibile classificazione, secondo gli autori, potrebbe fondarsi su quattro gruppi con diverso grado di rischio. Nel primo, sarebbero inclusi quegli Stati per i quali è stata adottata una decisione di adeguatezza; nel secondo, quegli Stati che stanno tentando di giungere ad una decisione di adeguatezza o che comunque hanno adottato una robusta normativa a tutela dei dati personali simile a quella del GDPR; nel terzo, quegli Stati che adottano una differente politica in tema di *privacy*, come gli Stati Uniti, ma dove v'è rispetto per i diritti umani e un consolidato stato di diritto; infine, nel quarto gruppo, quegli Stati come Cina, Corea del Nord e Iran che si caratterizzano per un debole assetto normativo in tema di *privacy*, lontano dagli *standard* europei o comunque con un sistema debole sotto il profilo della tutela dei diritti umani e dello stato di diritto. Sicché, per quegli Stati con basso o medio rischio vi sarebbe una presunzione di conformità, sino all'ultima categoria per i quali ci sarebbe una presunzione di esclusione.

La seconda parte di tale modello, invece, prevede un riassetto amministrativo e normativo dell'attuale sistema statunitense sulla base dei principi e divieti stabiliti dalla CGUE. Viene quindi esaminata la possibilità di prevedere un sistema indipendente per i ricorsi in tema *privacy* dei cittadini europei, proponendo una nuova *Algorithmic Rights Court* (ARC); una riforma dell'autorità di sorveglianza degli affari esteri prevista nella sezione 702 e l'introduzione di una presunzione di legge contro la sorveglianza dei dipendenti stranieri delle aziende statunitensi che lavorano all'estero e di una codificazione del PPD-28⁴⁵.

Infine, nei rapporti tra gruppi aziendali, il modello ibrido proposto verrebbe completato con le deroghe di cui all'art. 49 GDPR basate sul consenso o sull'esecuzione di un contratto⁴⁶.

6. LA DEROGA DEL CONSENSO DI CUI ALL'ART. 49, LETT. A), GDPR COME BASE PER IL TRASFERIMENTO.

In letteratura v'è chi sostiene che i metodi alternativi per il trasferimento dei dati rappresentati dalle clausole *standard* contrattuali, dalle norme uniformi d'impresa e dalle deroghe previste dall'art. 49 GDPR, sebbene costosi e lunghi, consentirebbero agli Stati Uniti di delineare un quadro giuridico in materia secondo quelle che sono le proprie condizioni, onorando la propria storia. Invece di rivedere le leggi sulla protezione dei dati e sulla *privacy*,

⁴⁴ *Ivi*, p. 445-447.

⁴⁵ *Ivi*, p. 447. Il PPD-28 dovrebbe ricevere una regolamentazione precisa poiché tale strumento consente di limitare le operazioni di sorveglianza ad alcuni ambiti

come terrorismo o spionaggio, tuttavia, qualunque Presidente potrebbe eliminarli estendendolo senza alcun limite.

⁴⁶ *Ivi*, p. 454.

gli Stati Uniti potrebbero incoraggiare l'uso delle SCC, delle norme vincolanti d'impresa e delle deroghe all'art. 49 attraverso programmi governativi volti ad assistere le imprese nella loro conformità ⁴⁷.

Molti responsabili del trattamento dei dati vorrebbero utilizzare il consenso degli interessati per trasferire i dati in paesi al di fuori dello Spazio economico europeo ⁴⁸.

Come accennato nel §2, nel 2018 l'EDPB ha emanato le linee guida per tutte le ipotesi derogatorie previste dall'art. 49 GDPR, inclusa la deroga del consenso dell'interessato ⁴⁹. Sebbene per il trasferimento dei dati verso un paese terzo fondato sul consenso esplicito e specifico non sia richiesto l'elemento dell'occasionalità come in caso di contratto o sede giudiziaria (art. 49, par. 1, lett. b) c) ed e), il Comitato europeo conclude rilevando che i requisiti richiesti, in associazione alla possibilità per l'interessato di revocare il consenso in qualunque momento, fanno sì che il consenso possa rivelarsi una soluzione inapplicabile nel lungo periodo per i trasferimenti verso paesi terzi ⁵⁰.

Nelle stesse linee guida viene specificato che anche « le deroghe non espressamente limitate ai trasferimenti “occasional” e “non ripetitivi” devono essere interpretate in modo da non contraddire la natura delle deroghe stesse, ossia eccezioni alla regola secondo la quale i dati personali possono essere trasferiti verso paesi terzi soltanto se il paese di destinazione offre un livello adeguato di protezione dei dati oppure, in alternativa, se sono messe in atto adeguate garanzie » ⁵¹.

Il consenso di cui alla lett. a) dell'art. 49 deve essere esplicito e specifico. Con il primo elemento si intende che deve essere necessario un elevato livello di controllo individuale dei dati personali come avviene in caso di trattamento di categorie particolari di dati e di decisioni automatizzate. L'elemento della specificità lo rende pari al consenso informato. Siffatto elemento fa sì che non sia possibile ottenere un preventivo consenso per un trasferimento futuro al momento in cui avviene la raccolta dei dati ⁵².

⁴⁷ D. CALIA, *op. cit.*, p. 271.

⁴⁸ S. FABER, *Does the GDPR Allow for the Use of Consent for the International Transfer of Data?*, in *National Law Review*, Vol. IX, 2022, consultabile su nat-lawreview.com. L'A. conclude che sebbene il GDPR sia più permissivo rispetto alla precedente dottrina in termini di utilizzo del consenso come base giuridica per i trasferimenti internazionali di dati, i requisiti per un consenso valido a questo scopo e il diritto di revocare tale consenso generano una situazione complessa e macchinosa. I responsabili e gli incaricati del trattamento

dei dati, conclude l'autore, dovrebbero procedere con cautela prima di ricorrere a una “falsa soluzione” e affidandosi quindi al consenso per i trasferimenti internazionali.

⁴⁹ EDPB, Linee guida 2/2018 sulle deroghe di cui all'art. 49 del regolamento 2016/679.

⁵⁰ *Ivi*, p. 8.

⁵¹ *Ivi*, p. 5.

⁵² *Ivi*, p. 7. Il Comitato europeo, argomentando il requisito della specificità, puntualizza che se le circostanze specifiche e il trasferimento stesso non fossero noti al momento in cui è richiesto il consenso, non

Tra le informazioni che debbono essere rese all'interessato al fine di ottenere un valido consenso per il trasferimento dei dati personali verso Stati terzi, devono essere specificati tutti i destinatari o tutte le categorie di destinatari dei dati e tutti i paesi verso i quali sono trasferiti i dati; devono specificare che il consenso rappresenta il fondamento giuridico per il trasferimento e che il paese terzo verso cui saranno trasferiti i dati non offre un livello adeguato di protezione dei dati sulla base di una decisione della Commissione europea. Come disposto dalla norma stessa, è necessario fornire informazioni sui possibili rischi per l'interessato derivanti dalla mancanza di un'adeguata protezione nel paese terzo e dall'assenza di garanzie appropriate. Questo avviso « che potrebbe essere standardizzato, deve includere ad esempio una menzione della possibile assenza nel paese terzo di un'autorità di controllo e della possibilità che non siano previsti principi sul trattamento dei dati o diritti dell'interessato »⁵³.

Nonostante alcuni timidi tentativi in dottrina volti ad ammettere una simile soluzione, dagli orientamenti del principale organismo europeo in materia di dati personali se ne ricava che la base giuridica del consenso — benché non sia limitata a trasferimenti occasionali al pari di altre deroghe normative —, per i precisi presupposti richiesti, sarebbe difficilmente utilizzabile per quei trasferimenti massivi di dati ripetuti nel tempo come usualmente avviene da parte di quelle *big tech* come nel caso oggetto della sentenza *Schrems II*.

7. IL *TRANS-ATLANTIC DATA PRIVACY FRAMEWORK* E LA NUOVA DECISIONE DI ADEGUATEZZA.

Le più importanti aziende tecnologiche statunitensi hanno insistito a lungo affinché si giungesse all'adozione di un nuovo accordo che potesse superare la fase di stallo creatasi a seguito dell'ultimo intervento della CGUE⁵⁴. Nel corso del 2022, quindi,

sarebbe possibile verificarne l'impatto sull'interessato. Viene perciò riportato l'esempio « in cui un'azienda UE raccolga i dati dei propri clienti per una finalità specifica (consegna merci) senza prevedere, in quel momento, il trasferimento di tali dati a terzi al di fuori dell'Unione. Si ipotizzi che alcuni anni dopo l'azienda sia rilevata da una società di un paese terzo, che intende trasferire i dati personali dei clienti a un'altra azienda di un paese terzo. Perché il trasferimento sia valido in applicazione della deroga, l'interessato deve prestare il proprio consenso per quel trasferimento specifico al momento in cui si prospetta tale operazione. Il consenso fornito all'atto della raccolta dei

dati da parte dell'azienda dell'Unione ai fini della consegna non è sufficiente a giustificare il ricorso a questa deroga ai fini di un trasferimento di dati personali al di fuori dell'UE prospettatosi in un secondo momento. L'esportatore deve quindi assicurarsi di ricevere un consenso specifico prima di mettere in atto il trasferimento, anche se ciò avviene dopo la raccolta dei dati. Tale requisito è correlato alla necessità di un consenso informato ».

⁵³ *Ivi*, p. 8.

⁵⁴ W. VOSS, *op. cit.*, p. 177. L'A. specifica che « (...) Google seeks a replacement Privacy Shield agreement, without modifications to U.S. surveillance legislation, even

si sono poste le basi per giungere ad una nuova decisione di adeguatezza relativa agli Stati Uniti. Il percorso è stato intrapreso nel mese di marzo allorché la Presidente della Commissione europea e il Presidente degli Stati Uniti hanno annunciato un nuovo accordo, il c.d. *Trans-Atlantic Data Privacy Framework* di cui non si conosceva molto al di là di principi e obiettivi generali.

Tale accordo è stato poi recepito negli Stati Uniti il 7 ottobre 2022 attraverso un ordine esecutivo del Presidente (E.O. 14086) e poi per mezzo dei regolamenti del procuratore generale.

Il 13 dicembre 2022, perciò, è stata pubblicata la bozza di decisione di adeguatezza, tempestivamente trasmessa all'EDPB per il suo parere (già adottato). A seguito di un parere dell'EDPB la Commissione, il 10 luglio 2023, ha adottato la decisione n. 1795/2023 nella sua formulazione definitiva, senza alcuna modifica. La decisione sarà sottoposta a revisioni periodiche; la prima, ad un anno dalla sua adozione.

In base al nuovo accordo, le società statunitensi saranno sottoposte ad una serie di obblighi come la cancellazione dei dati personali quando non sono più necessari per lo scopo per il quale sono stati raccolti, e per garantire la continuità della protezione quando i dati personali sono condivisi con terzi. Saranno garantite ai cittadini dell'UE diverse possibilità di ricorso nel caso di trattamento dei dati personali in violazione dell'accordo quadro dinanzi a organismi indipendenti di risoluzione delle controversie e un collegio arbitrale.

Inoltre, il quadro giuridico statunitense prevederebbe una serie di limitazioni e garanzie riguardanti l'accesso ai dati da parte delle autorità pubbliche, in particolare in materia penale e per finalità di sicurezza nazionale. L'accesso ai dati europei da parte delle agenzie di *intelligence* statunitensi sarebbe perciò limitato a quanto necessario e proporzionato per la protezione della sicurezza nazionale; i cittadini europei avranno la possibilità di ottenere un risarcimento in merito alla raccolta e all'utilizzo dei propri dati da parte delle agenzie di *intelligence* statunitensi dinanzi a un meccanismo di ricorso indipendente e imparziale che comprende un Tribunale di revisione per la protezione dei dati di nuova creazione.

La decisione contempla una particolarità rispetto alle precedenti. È previsto, all'art. 1, che gli Stati Uniti garantiscono un adeguato livello di protezione per i dati personali trasferiti dal-

though, paradoxically, it works with Big Tech colleagues at Amazon, Apple, Dropbox, Evernote, Google, Facebook (Meta), Microsoft, Snap, Inc., Twitter, Yahoo and Zoom in a Reform Government Surveillance (RGS)

coalition that "strongly believes that current surveillance laws and practices must be reformed," and be made "consistent with established global norms of privacy, free expression, security, and the rule of law"».

l'UE alle organizzazioni americane ricomprese nella lista del *Data Privacy Framework* (DPF)⁵⁵. Questo elemento, perciò, sta a significare che solo per quegli enti ricompresi nella lista gestita e pubblicata dal dipartimento del commercio degli Stati Uniti (DoC) sarà applicabile la decisione di adeguatezza, mentre per i restanti si dovranno applicare i meccanismi sussidiari di cui agli artt. 46 e ss. del GDPR.

La stessa decisione prescrive che ogni volta che la competente autorità degli stati membri esercita i poteri previsti dall'art. 58 GDPR in riferimento a quanto previsto dall'art. 1 della decisione, lo stato membro è tenuto ad informare senza indugio la Commissione europea. Quest'ultima è chiamata ad un costante monitoraggio del quadro normativo oggetto della decisione di adeguatezza, incluse le condizioni in cui vengono effettuati i trasferimenti successivi, le modalità di esercizio dei diritti individuali e i casi di accesso da parte delle autorità pubbliche statunitensi ai dati trasferiti.

7.1. *I principi in materia di Privacy nel quadro dell'intesa UE-USA.*

Nella decisione della Commissione europea, dalla cui lettura si evince a chiare lettere l'*influenza* della sentenza *Schrems II*, si specifica il principio secondo cui il trattamento dei dati personali deve essere improntato a canoni di liceità e correttezza; che i dati devono essere acquisiti per uno scopo specifico e quindi utilizzati compatibilmente a tale scopo. Questo verrebbe garantito da vari principi, tra cui l'integrità dei dati e la limitazione delle finalità, analogamente a quanto sancito nell'art. 5, par. 1, lett. b), GDPR.

L'utilizzo dei dati personali per una nuova finalità material-

⁵⁵ L'accordo tra UE-USA si fondebbe su un sistema di certificazione con cui le organizzazioni statunitensi si impegnano a rispettare una serie di principi in materia di *privacy* - i "EU-U.S. Data Privacy Framework Principles" adottati dal Dipartimento del Commercio degli Stati Uniti (DoC) e contenuti nell'allegato I della decisione. Per poter ottenere la certificazione, un'organizzazione deve essere soggetta ai poteri d'indagine della *Federal Trade Commission* (FTC) o del *Department of Transportation* (DoT) degli Stati Uniti. Tutte le organizzazioni certificate, inoltre, sono tenute a certificare annualmente la loro adesione ai Principi in questione. Per certificarsi ai sensi del DPF UE-USA, le organizzazioni sono tenute a dichiarare il loro impegno a rispettare i Principi, a rendere disponibili le loro politiche sulla *privacy* e ad attuarle piena-

mente. Come parte della loro domanda di (ri)certificazione, le organizzazioni devono presentare al DoC informazioni su, *inter alia*, il nome dell'organizzazione in questione, una descrizione degli scopi per i quali l'organizzazione tratterà i dati personali, nonché i dati personali che saranno coperti dalla certificazione, il metodo di verifica prescelto, il relativo meccanismo di ricorso indipendente e l'organismo legale che ha la giurisdizione per far rispettare i Principi. Il DoC è tenuto a monitorare costantemente l'effettivo rispetto dei principi da parte delle organizzazioni DPF UE-USA attraverso diversi meccanismi. In particolare, effettuerà "controlli a campione" su organizzazioni selezionate in modo casuale, così come i controlli *ad hoc* di organizzazioni specifiche quando vengono segnalati da terzi.

mente diversa ma compatibile con la finalità originaria, o la divulgazione di dati a terzi, sono subordinati alla concessione di un diritto di opposizione a favore degli interessati attraverso un meccanismo chiaro e prontamente disponibile. In ogni caso, un diverso e incompatibile trattamento sarebbe vietato. In caso di dati personali *particolari*, invece, si prevede la necessità di un esplicito consenso da parte dell'interessato.

I dati devono essere accurati e, se necessario, aggiornati. Devono essere adeguati, pertinenti e non eccessivi in relazione alle finalità perseguite; non devono essere conservati più a lungo di quanto sia necessario per le finalità per le quali sono trattati. Viene altresì stabilito l'elemento della sicurezza, sempre garantita nel processo di trattamento. In tal senso, devono essere adottate misure tecniche e organizzative adeguate a tutela di potenziali minacce ⁵⁶.

In tema di trasparenza è previsto l'obbligo di informare in modo chiaro gli interessati su (i) la partecipazione dell'organizzazione al DPF, (ii) il tipo di dati raccolti, (iii) le finalità del trattamento, (iv) il tipo o l'identità dei terzi a cui possono essere comunicati i dati personali e le relative finalità, (v) i loro diritti individuali, (vi) le modalità di contatto con l'organizzazione e (vii) i rimedi giurisdizionali previsti.

Gli interessati godono di determinati diritti che possono essere fatti valere nei confronti del responsabile del trattamento o dell'incaricato del trattamento; in particolare, è previsto il diritto di accesso ai dati, il diritto di opporsi al trattamento ⁵⁷ e il diritto alla rettifica e alla cancellazione dei dati ⁵⁸.

Il diritto di accesso può essere limitato solo in circostanze eccezionali, ovvero, quando i diritti di altri soggetti verrebbero violati dall'accesso in questione; quando l'onere o il costo di fornire l'accesso sarebbe sproporzionato rispetto ai rischi per la *privacy* dell'individuo. Qualsiasi rifiuto o limitazione di un diritto di accesso deve essere necessario e motivato.

Per quanto riguarda i trasferimenti di dati successivi verso terzi Stati, essi possono avvenire solo (i) per scopi limitati e specifici, (ii) sulla base di un contratto tra l'organizzazione facente parte del DPF UE-USA e la terza parte (o di un accordo analogo all'interno di un gruppo societario) e (iii) solo se tale contratto

⁵⁶ Tali misure devono essere valutate tenendo conto dello stato dell'arte, dei costi correlati e della natura, ambito, contesto e finalità del trattamento.

⁵⁷ Quando i dati personali sono utilizzati per finalità di *marketing* diretto, le persone hanno il diritto di opporsi al trattamento in qualsiasi momento.

⁵⁸ Viene specificato che i Principi non affrontano specificamente il tema delle de-

cisioni che riguardano l'interessato basate esclusivamente sul trattamento automatizzato dei dati personali. Tuttavia, per quanto riguarda i dati personali raccolti nell'Unione, qualsiasi decisione basata su un trattamento automatizzato sarà di norma presa dal responsabile del trattamento nell'Unione — che ha un rapporto diretto con l'interessato — ed è pertanto direttamente soggetta al Reg. (UE) 2016/679.

prevede che il terzo fornisca lo stesso livello di protezione garantito dai Principi.

Nella decisione si specifica che per garantire un livello adeguato di protezione dei dati nella pratica, dovrebbe essere istituita un'autorità di vigilanza indipendente dotata di poteri volti a monitorare e a far rispettare le norme sulla protezione dei dati.

Le organizzazioni aderenti al DPF devono essere soggette alla giurisdizione delle autorità statunitensi competenti — la FTC⁵⁹ e il DoT — che hanno i poteri investigativi e di intervento necessari a garantire il rispetto effettivo dei Principi *privacy*.

7.2. *Le azioni e i rimedi previsti nel DPF.*

In tema di rimedi, nella nuova decisione è previsto che gli interessati possano ricorrere innanzi ad un organismo indipendente designato dalla stessa organizzazione, al DPAs, al DoC oppure al FTC. Nel caso in cui la controversia non venga risolta attraverso questi meccanismi, sarebbe possibile attivare il procedimento di arbitrato previsto all'allegato I della decisione di adeguatezza. Ad eccezione di quest'ultimo procedimento, che richiede il preventivo esperimento di alcuni strumenti prima della sua instaurazione, gli interessati sono liberi di perseguire uno o tutti i meccanismi di ricorso previsti e non sono obbligati a scegliere un meccanismo piuttosto che un altro o a seguire una sequenza specifica.

7.2.1. *Il ricorso innanzi un organismo indipendente designato.*

Ciascuna organizzazione nella propria informativa deve comunicare chiaramente e, quindi, individuare internamente o esternamente all'organizzazione l'organismo che si occuperà della gestione dei reclami. Al ricevimento del reclamo presentato direttamente dall'interessato, o a seguito di un rinvio da parte di un'autorità di protezione dei dati, l'organizzazione deve fornire una risposta entro 45 giorni. Allo stesso modo, le organizzazioni sono tenute a rispondere tempestivamente alle indagini e alle altre

⁵⁹ La FTC è un'autorità indipendente composta da cinque commissari nominati dal Presidente con il parere del Senato. Essi sono nominati per un mandato di sette anni e possono essere rimossi dal Presidente solo per inefficienza, negligenza o inadempienza. La FTC non può avere più di tre Commissari del medesimo partito politico e i Commissari non possono, durante il loro incarico, intraprendere altre attività o impieghi.

La FTC può indagare sull'osservanza dei Principi e sulle false dichiarazioni di adesione ai Principi o di partecipazione al DPF UE-USA da parte di organizzazioni; può emettere provvedimenti e nel caso in cui le organizzazioni non si conformino ad essi, la FTC può chiedere sanzioni e altri rimedi, anche per eventuali danni causati dalla condotta illecita. La FTC manterrà un elenco online delle organizzazioni soggette agli ordini della FTC o di un tribunale in materia.

richieste di informazioni da parte di un'autorità di protezione dei dati.

Gli interessati possono anche presentare un reclamo direttamente all'organismo indipendente di risoluzione delle controversie (negli Stati Uniti o nell'Unione) designato dall'organizzazione per indagare e risolvere i reclami individuali — a meno che non siano palesemente infondati o futili — e per fornire un ricorso adeguato e gratuito all'individuo. Le sanzioni e i rimedi imposti da tale organismo devono essere sufficientemente rigorosi per garantire il rispetto dei Principi da parte delle organizzazioni e devono essere in grado di disporre l'annullamento o la correzione da parte dell'organizzazione degli effetti della “non conformità” ai principi e, a seconda delle circostanze, la cessazione dell'ulteriore trattamento dei dati personali in questione e/o la cessazione del trattamento dei dati personali. Gli organismi indipendenti sono tenuti a pubblicare le informazioni rilevanti e i servizi che forniscono in base all'accordo UE-USA e, a cadenza annuale, a pubblicare un rapporto che fornisca statistiche aggregate sui servizi offerti.

7.2.2. *I ricorsi alle autorità indipendenti nazionali (DPA).*

Gli interessati possono anche presentare i loro reclami innanzi a un'autorità nazionale per la protezione dei dati dello stato membro di riferimento. Le organizzazioni sono tenute a collaborare alle indagini e alla risoluzione di un reclamo da parte di tale autorità, sia quando questo riguarda il trattamento dei dati relativi alle risorse umane raccolti nell'ambito di un rapporto di lavoro, sia quando la rispettiva organizzazione si è volontariamente sottoposta alla sorveglianza delle autorità di protezione dei dati. In particolare, le organizzazioni devono rispondere alle richieste di informazioni, conformarsi ai consigli forniti dall'autorità di protezione dei dati, anche per quanto riguarda le misure correttive o compensative.

Per facilitare la cooperazione per una gestione efficace dei reclami, sia il DoC che la FTC istituiscono un punto di contatto dedicato, responsabile del collegamento diretto con le DPA. Questi punti di contatto assistono le DPA nelle richieste di informazioni relative alla conformità di un'organizzazione ai Principi in materia di *privacy*.

Il parere fornito dai DPA viene emesso dopo che ad entrambe le parti in causa sia stato garantito il contraddittorio. Il gruppo di esperti può emettere il parere con la massima rapidità consentita dal requisito del giusto processo e, di norma, entro 60 giorni dal ricevimento del reclamo. Se un'organizzazione non si adegua entro 25 giorni dalla trasmissione del parere e non offre spiegazioni ragionevoli per il ritardo, la questione può essere sottoposta alla FTC. In tal caso si può giungere ad un'azione esecutiva

basata sulla Sez. 5 del *FTC Act*. In alternativa, si potrà informare il DoC che considererà il rifiuto dell'organizzazione di conformarsi al parere del DPA come una persistente inadempienza che può portare alla rimozione dell'organizzazione dall'elenco DPF se la DPA a cui è stato indirizzato il reclamo non ha intrapreso alcuna azione o ha intrapreso un'azione insufficiente per risolvere la questione.

Il DoC si è impegnato a ricevere, esaminare e fare il possibile per risolvere i reclami relativi alla non conformità di un'organizzazione ai Principi *privacy*. A tal fine, il DoC prevede procedure speciali che consentono alle DPA di indirizzare i reclami a un punto di contatto dedicato, di tenerne traccia e di seguire le organizzazioni per facilitarne la risoluzione. Per accelerare il trattamento dei singoli reclami, il punto di contatto si relaziona direttamente con la rispettiva autorità di protezione dei dati sulle questioni di conformità e, in particolare, la aggiorna sullo stato dei reclami entro un periodo non superiore a 90 giorni dal deferimento. Ciò consentirebbe agli interessati di presentare reclami di non conformità da parte delle organizzazioni del DPF UE-USA direttamente alla propria DPA nazionale e di farli pervenire al DoC in quanto autorità statunitense che amministra il DPF UE-USA.

Qualora, sulla base delle verifiche d'ufficio, dei reclami o di qualsiasi altra informazione, il DoC concluda che un'organizzazione non abbia rispettato i Principi, può rimuovere tale organizzazione dall'elenco DPF. Il rifiuto di conformarsi a una decisione finale di un organismo di autoregolamentazione della *privacy*, di risoluzione indipendente delle controversie o di un ente governativo, compresa una DPA, verrebbe considerato come un'inadempienza persistente.

7.2.3. *Il procedimento di arbitrato.*

In "ultima istanza", nel caso in cui nessuna delle altre vie di ricorso disponibili abbia risolto in modo soddisfacente le doglianze di un individuo, l'interessato può instaurare il procedimento di arbitrato del Gruppo di esperti UE-U.S. *Data Privacy Framework Panel*.

Il *panel* DPF UE-USA è costituito da un gruppo di almeno dieci arbitri che vengono designati dal DoC e dalla Commissione in base alla loro indipendenza, integrità ed esperienza in materia di *privacy* e di diritto dell'Unione europea in materia di protezione dei dati.

Per ogni singola controversia le parti selezionano da questo elenco un gruppo di uno o tre arbitri. La gestione degli arbitrati spetta all'*International Centre for Dispute Resolution* (ICDR) e alla divisione internazionale dell'*American Arbitration Association* (AAA). I procedimenti saranno disciplinati da una serie di

regole concordate e da un codice di condotta applicabile agli arbitri nominati. Il sito web dell'ICDRAAA fornisce informazioni chiare e concise ai singoli individui sul meccanismo di arbitrato e sulla procedura per presentare la domanda di arbitrato.

Il DPF contiene diverse caratteristiche che migliorano l'accessibilità a questo meccanismo per gli interessati dell'Unione: (i) nella preparazione di un ricorso l'interessato può essere assistito dalla propria autorità nazionale di protezione dei dati; (ii) sebbene l'arbitrato si svolga negli Stati Uniti, i ricorrenti europei possono scegliere di partecipare tramite videoconferenza o conferenza telefonica, senza alcun costo per l'interessato; (iii) benché la lingua utilizzata nell'arbitrato sia l'inglese, l'interpretazione durante l'udienza arbitrale e la traduzione saranno in linea di principio fornite su richiesta motivata e senza alcun costo per il ricorrente; (iv) infine, benché ciascuna parte deve sostenere le proprie spese legali, se rappresentata da un avvocato davanti al collegio, il DoC manterrà un fondo alimentato con contributi annuali dalle organizzazioni DPF UE-USA, che coprirà i costi della procedura di arbitrato fino a un importo massimo stabilito dalle autorità statunitensi in consultazione con la Commissione.

Il collegio arbitrale ha l'autorità di imporre misure correttive specifiche e necessarie per rimediare al mancato rispetto dei Principi. Sebbene il collegio tenga conto di altri rimedi già adottati da altri organismi DPF UE-USA nell'adottare la sua decisione, gli interessati possono comunque ricorrere all'arbitrato se ritengono che questi non siano soddisfacenti. La decisione arbitrale può esser fatta valere presso i tribunali statunitensi dai singoli ai sensi del *Federal Arbitration Act*, garantendo così un rimedio legale nel caso in cui un'organizzazione non si conformi.

L'arbitrato ha comunque un ruolo sussidiario, ovvero non potrebbe essere adito qualora un'autorità di protezione dei dati abbia il potere di risolvere la questione nei confronti dell'organizzazione interessata.

7.3. *I poteri delle agenzie di intelligence secondo il nuovo accordo.*

L'altro profilo fondamentale — in considerazione dei principi enunciati dalla Corte di Giustizia europea — riguarda l'accesso e l'utilizzo di dati personali da parte delle autorità pubbliche statunitensi.

Perciò una prima parte della decisione è dedicata ai poteri e ai limiti delle autorità pubbliche per finalità di polizia e di applicazione della legge penale. La seconda, invece, si focalizza sull'accesso da parte delle autorità pubbliche per motivi di sicurezza nazionale. Quest'ultima riguarda in modo particolare i poteri facenti capo ai servizi di *intelligence*. La parte finale, invece, è dedicata alla supervisione delle autorità *de quibus* e ai rimedi giurisdizionali in caso di abusi da parte delle suddette autorità.

Nella nuova decisione viene evidenziato che le agenzie di *intelligence* statunitensi possono ottenere l'accesso ai dati personali trasferiti per scopi di sicurezza nazionale solo se autorizzate per legge, in particolare in base al *Foreign Intelligence Surveillance Act* (FISA) o a quelle disposizioni di legge che autorizzano l'accesso tramite il *National Security Letters* (NSL).

Il FISA contiene diverse basi giuridiche che possono essere utilizzate per raccogliere (e successivamente trattare) i dati personali dei cittadini europei trasferiti nell'ambito dell'accordo UE-USA (sez. 105 FISA, sez. 302 FISA, sez. 402 FISA, sez. 501 FISA e sez. 702 FISA).

Le agenzie hanno anche la possibilità di raccogliere dati personali al di fuori degli Stati Uniti e tali attività all'estero si basano sull'Ordine esecutivo 12333. Si tratta di quell'E.O. che ha giocato un ruolo centrale nella pronuncia della CGUE del 2020.

La decisione si focalizza sulle operazioni di *Signals Intelligence* (SIGINT), ovvero sulla raccolta di informazioni attraverso l'intercettazione e l'analisi di segnali, emessi tra persone (come segnali di comunicazione COMINT) o tra macchine (ELINT, spionaggio elettronico), oppure con una combinazione delle due operazioni. Le SIGINT possono essere effettuate dalle agenzie di *intelligence* statunitensi sia all'interno degli Stati Uniti — sulla base del FISA — sia durante il transito dei dati verso gli Stati Uniti, sulla base della E.O. 12333.

La novità rispetto al contesto della *Schrems II* risiede nell'adozione dell'E.O. 14086 del 7 ottobre 2022, il quale prevede limitazioni e salvaguardie per tutte le attività di *intelligence* degli Stati Uniti e sostituisce, in larga misura, il PPD-28203 (altra fonte centrale nell'ambito dell'oggetto della *Schrems II*), rafforzando le condizioni, le limitazioni e le salvaguardie che si applicano a tutte le SIGINT, indipendentemente dal luogo in cui si svolgono.

I requisiti stabiliti in questo ordine esecutivo sono vincolanti per l'intera comunità dell'*intelligence*. Essi devono essere ulteriormente attuati attraverso politiche e procedure di agenzia che li traducano in indicazioni concrete per le operazioni quotidiane. A questo proposito, l'E.O. 14086 concede alle agenzie di *intelligence* degli Stati Uniti il termine di un anno per aggiornare le politiche e le procedure esistenti e allinearle ai requisiti sanciti nell'E.O. stesso.

Tali politiche e procedure aggiornate devono essere sviluppate in consultazione con l'*Attorney General*, il *Civil Liberties Protection Officer del Director of National Intelligence* (ODNI CLPO) e il *Privacy and Civil Liberties Oversight Board* (PCLOB), ossia un organo di controllo indipendente autorizzato a rivedere le politiche che dell'*Executive Branch* e la loro attuazione.

7.3.1. *Le limitazioni e le garanzie per la raccolta di dati personali per finalità di sicurezza nazionale.*

L'E.O. 14086 stabilisce una serie di requisiti applicabili a tutte le SIGINT (raccolta, uso, diffusione, ecc. di dati personali). Le attività devono fondarsi su uno statuto o su un'autorizzazione presidenziale. Qualsiasi attività di *intelligence* può essere svolta solo « dopo aver stabilito, sulla base di una valutazione ragionevole di tutti i fattori pertinenti, che le attività sono necessarie per portare avanti una priorità di intelligence convalidata ».

Infine, per garantire il rispetto di questi requisiti generali — che riflettono i principi di legalità, necessità e proporzionalità — le attività di *intelligence* sono soggette ad apposita supervisione. Innanzitutto, i casi per cui i dati possono essere raccolti nell'ambito delle attività di *intelligence* sono limitati in due modi. Da un lato, vengono stabiliti gli obiettivi che possono essere perseguiti dalla SIGINT, ad esempio comprendere o valutare le capacità, le intenzioni o le attività di organizzazioni straniere, comprese le organizzazioni terroristiche internazionali, che rappresentano una minaccia attuale o potenziale alla sicurezza nazionale degli Stati Uniti; proteggere dalle capacità e dalle attività militari straniere; comprendere o valutare le minacce transnazionali che hanno un impatto sulla sicurezza globale, come il clima e altri cambiamenti ecologici, i rischi per la salute pubblica e le minacce umanitarie. D'altro canto, l'E.O. elenca alcuni obiettivi che non devono mai essere perseguiti dalle attività di *intelligence* dei segnali, ad esempio per ostacolare la critica, il dissenso o la libera espressione di idee o di opinioni politiche da parte di individui o della stampa; per svantaggiare persone in base alla loro etnia, razza, genere, identità di genere, orientamento sessuale o religione; o per offrire un vantaggio competitivo alle aziende statunitensi.

Le priorità di *intelligence* vengono prima sviluppate dal Direttore dell'*Intelligence* nazionale (attraverso il cosiddetto *National Intelligence Priorities Framework*) e quindi sottoposte all'approvazione del Presidente. Il Direttore deve — in conformità con la E.O. 14086 — ottenere una preventiva valutazione da parte del funzionario per la protezione delle libertà civili della direzione dell'*Intelligence* nazionale (ODNI CLPO) per ciascuna priorità.

Tale procedimento, si specifica nella nuova decisione, garantirebbe che le considerazioni sulla *privacy* siano prese in considerazione fin dalla fase iniziale di elaborazione delle priorità di *intelligence*.

Dopo aver stabilito la *priorità*, è necessario determinare le modalità operative. Quindi, le agenzie di *intelligence* statunitensi devono considerare l'esistenza, la fattibilità e l'adeguatezza di modalità meno intrusive. Quando, sulla base dei predetti criteri, la raccolta di informazioni è ritenuta necessaria, deve essere “il

più possibile mirata” e “non deve avere un impatto sproporzionato sulla *privacy* e sulle libertà civili”.

La “raccolta massiva”, invece, può essere attuata solo al di fuori degli Stati Uniti sulla base dell’E.O. 12333; e anche in questo caso, ai sensi della E.O. 14086, la raccolta mirata deve avere la priorità. Al contrario, la raccolta massiva è consentita solo quando le informazioni necessarie per portare avanti una priorità di *intelligence* convalidata non possono essere ragionevolmente ottenute con una raccolta mirata. Anche in quest’ultimo caso però si applicano quelle specifiche garanzie previste dalla E.O. 14086. Per portare avanti una priorità di *intelligence* convalidata è necessario attuare metodi e misure tecniche volte a limitare i dati raccolti solo a quelli necessari, riducendo al minimo la raccolta di informazioni non pertinenti.

Inoltre, vengono limitati gli usi delle informazioni raccolte in massa a sei obiettivi specifici, tra cui in tema di terrorismo, di presa di ostaggi e di detenzione di individui da parte o per conto di un governo, di un’organizzazione o di una persona straniera; nell’ambito dello spionaggio, di sabotaggio o di assassinio da parte di stranieri; in tema di protezione contro le minacce derivanti dal possesso o dalla proliferazione di armi di distruzione di massa o di tecnologie e minacce correlate.

Oltre ai requisiti dell’E.O. 14086, le SIGINT trasferite a un’organizzazione negli Stati Uniti è soggetta a limitazioni e salvaguardie specifiche disciplinate dalla Sezione 702 FISA. Per raccogliere informazioni di *intelligence* straniera ai sensi della Sezione 702 della FISA, il Procuratore Generale e il Direttore dell’*Intelligence Nazionale* presentano certificazioni annuali alla *Foreign Intelligence Surveillance Court* (FISC) per identificare le categorie di informazioni di *intelligence* straniera da acquisire. Tali certificazioni devono essere accompagnate da procedure di *targeting*, minimizzazione e interrogazione, anch’esse approvate dal FISC e legalmente vincolanti per le agenzie di *intelligence* statunitensi. Le decisioni assunte dal FISC possono essere appellate al *Foreign Intelligence Surveillance Court of Review* (FISCR) e, in ultima istanza, alla Corte Suprema degli Stati Uniti.

Per quanto riguarda le altre basi giuridiche per la raccolta di dati personali trasferiti a organizzazioni negli Stati Uniti, si applicano limitazioni e garanzie diverse. In generale, la raccolta di dati in blocco è specificamente vietata dalla Sezione 402 della FISA (*pen register* e *trap and trace authority*).

7.3.2. Le modalità di utilizzo delle informazioni raccolte.

Ogni agenzia di *intelligence* deve garantire un’adeguata sicurezza dei dati e impedire l’accesso da parte di persone non autorizzate ai dati personali raccolti tramite lo spionaggio di segnali elettromagnetici.

A questo proposito, diversi strumenti, tra cui leggi, linee guida e *standard*, specificano ulteriormente i requisiti minimi di sicurezza che devono essere messi in atto (ad esempio, l'autenticazione a più fattori, la crittografia, ecc.). L'accesso ai dati raccolti deve essere limitato al personale autorizzato il quale necessita di conoscere le informazioni per svolgere la propria missione. Più in generale, le agenzie devono fornire una formazione adeguata ai propri dipendenti, anche sulle procedure per segnalare e affrontare le violazioni della legge.

In ordine alla conservazione dei dati, l'E.O. 14086 prevede l'applicazione degli stessi periodi di conservazione sia per i cittadini statunitensi che per le persone non statunitensi. Inoltre, i dati personali di cittadini non statunitensi possono essere diffusi solo se riguardano lo stesso tipo di informazioni che possono essere diffuse su persone statunitensi, ad esempio informazioni necessarie per proteggere la sicurezza di una persona o di un'organizzazione (come obiettivi, vittime o ostaggi di organizzazioni terroristiche internazionali). Ogni agenzia di *intelligence* è tenuta a conservare un'adeguata documentazione sulla raccolta di informazioni.

7.3.3. La supervisione delle attività di intelligence.

Le attività delle agenzie di *intelligence* statunitensi sono soggette alla supervisione da parte di diversi organismi. L'E.O. 14086 richiede anzitutto che ogni agenzia conduca da sé una supervisione periodica delle attività di *intelligence* e che garantisca un rimedio per qualsiasi eventuale violazione. Esse devono fornire ai funzionari preposti l'accesso a tutte le informazioni necessarie per svolgere le loro funzioni di supervisione.

A questi ultimi debbono essere garantite le risorse necessarie per adempiere al loro mandato, l'accesso a tutto il materiale e al personale necessario per svolgere le loro funzioni e devono essere informati e consultati sui cambiamenti di politica proposti.

I responsabili per la *privacy* e le libertà civili riferiscono periodicamente al Congresso e al PCLOB, anche in merito al numero e alla natura delle denunce ricevute dal dipartimento/agenzia.

Inoltre, ogni agenzia deve prevedere un ispettore generale indipendente con la responsabilità, tra le altre, di supervisionare le attività di *intelligence* estera. Essi hanno accesso a tutti i registri, ai rapporti, alle verifiche, alle revisioni, ai documenti o altro materiale pertinente. Ancora. L'*Intelligence Oversight Board* (IOB), istituito all'interno del *President's Intelligence Advisory*

Board (PIAB) ⁶⁰, vigila sul rispetto della Costituzione e di tutte le norme applicabili da parte delle autorità di *intelligence* statunitensi. Come già previsto dall'E.O. 12333, i capi di tutte le agenzie sono tenuti a riferire all'IOB qualsiasi attività per la quale vi sia motivo di ritenere che possa essere illegale o contraria a un ordine esecutivo o a una direttiva presidenziale. Per garantire che l'IOB abbia accesso alle informazioni necessarie per svolgere le sue funzioni, l'E.O. 13462 dispone che il Direttore dell'*Intelligence* nazionale e i capi delle agenzie di *intelligence* forniscano tutte le informazioni e l'assistenza che l'IOB ritiene necessarie per svolgere le sue funzioni.

L'IOB è a sua volta tenuto a informare il Presidente sulle attività di *intelligence* che ritiene possano violare la legge degli Stati Uniti e che non vengono affrontate adeguatamente dal Procuratore Generale, dal Direttore dell'*Intelligence* Nazionale o dal capo di un'agenzia.

Le agenzie sono soggette anche alla supervisione del PCLOB, un'agenzia indipendente all'interno del ramo esecutivo composta da un Consiglio di cinque membri nominato dal Presidente. Oltre ai meccanismi di supervisione interni al ramo esecutivo, sono previste specifiche commissioni del Congresso degli Stati Uniti che hanno la responsabilità di supervisionare tutte le attività di *intelligence* estera degli Stati Uniti. I membri di queste commissioni hanno accesso a informazioni classificate, nonché a metodi e programmi di *intelligence*.

7.3.4. I rimedi esperibili secondo il DPF.

L'E.O. 14086 ha istituito un meccanismo di ricorso specifico, integrato al regolamento dell'AC che istituisce il Tribunale per la revisione della protezione dei dati, con lo scopo di gestire e risolvere i reclami degli individui relativi alle attività di *intelligence* degli Stati Uniti.

Qualsiasi cittadino europeo ha il diritto di presentare un reclamo in caso di presunta violazione della legge statunitense che disciplina le attività di *intelligence* (ad esempio, l'E.O. 14086, la sezione 702 del FISA o l'E.O. 12333) che leda i suoi interessi in materia di *privacy* e libertà civili. Il ricorso deve essere presentato innanzi ad un'autorità di controllo di uno Stato membro dell'UE competente per la supervisione dei servizi di sicurezza nazionale e/o del trattamento dei dati personali.

⁶⁰ Organo consultivo dell'Ufficio esecutivo del Presidente, composto da 16 membri, nominati dal Presidente, senza legami con il governo degli Stati Uniti. L'IOB è

invece composto da un massimo di cinque membri designati dal Presidente tra i membri del PIAB.

La presentazione di un tale ricorso — secondo la nuova decisione della Commissione — è soggetta a pochi requisiti di ammissibilità poiché gli interessati non sono tenuti a dimostrare che i loro dati sono stati effettivamente oggetto di attività di *intelligence*. Allo stesso tempo però è necessario fornire alcune informazioni di base, ad esempio sui dati personali che si ritiene siano stati ragionevolmente trasferiti negli Stati Uniti e sui mezzi con cui si ritiene siano stati trasferiti; sull'identità degli enti governativi statunitensi che si ritiene siano stati coinvolti; sull'identità degli enti governativi statunitensi che si ritiene siano stati coinvolti.

L'indagine iniziale delle denunce presentate a questo meccanismo di ricorso è condotta dal CLPO dell'ODNI, il cui ruolo e i cui poteri, già previsti dalla legge, sono stati ampliati per le azioni intraprese ai sensi della E.O. 14036.

I rimedi che tale organo può adottare consistono in diverse misure come la cessazione dell'acquisizione di dati, la cancellazione di dati raccolti illegalmente, la cancellazione dei risultati di interrogazioni condotte in modo inappropriato su dati altrimenti raccolti legalmente, la limitazione dell'accesso ai dati raccolti legalmente a personale adeguatamente addestrato o il richiamo di rapporti di *intelligence* contenenti dati acquisiti senza autorizzazione legale o che sono stati diffusi illegalmente. Le decisioni del CLPO sono vincolanti per le agenzie di *intelligence* interessate. Esse possono essere impugnate innanzi al DPRC entro 60 giorni dalla notifica del provvedimento ⁶¹. Gli interessati europei possono presentare la loro impugnazione, anche in questo caso, attraverso le autorità nazionali.

7.3.5. *Gli ulteriori strumenti giurisdizionali secondo il DPF.*

La FISA prevede la possibilità per gli individui di intentare un'azione civile per danni contro gli Stati Uniti quando le informazioni che li riguardano sono state utilizzate o divulgate illegalmente e intenzionalmente. È consentito citare in giudizio per il risarcimento dei danni i funzionari del governo degli Stati Uniti che agiscono a titolo personale e contestare la legittimità del programma di sorveglianza nel caso in cui il governo degli Stati Uniti intenda utilizzare o divulgare qualsiasi informazione ottenuta o derivata dalla sorveglianza elettronica contro l'interessato

⁶¹ Il DPRC è un tribunale indipendente istituito dall'*Attorney General* sulla base della EO 14036 e la nomina dei giudici si basa sui criteri utilizzati dal ramo esecutivo per valutare i candidati alla magistratura federale. I ricorsi al DPRC sono esaminati da un collegio di tre giudici. Ogni commissione è assistita da un avvocato spe-

ziale che ha accesso a tutte le informazioni relative al caso, comprese quelle classificate. Il ruolo di quest'ultimo è quello di garantire che gli interessi del ricorrente siano rappresentati e che la commissione della DPRC sia ben informata su tutte le questioni rilevanti di diritto e di fatto.

in procedimenti giudiziari o amministrativi negli Stati Uniti. Inoltre, sono previste diverse possibilità di ricorso contro i funzionari governativi per un accesso o un uso illegale di dati personali da parte del governo, anche per presunti scopi di sicurezza nazionale (ad esempio, *Computer Fraud and Abuse Act*, *Electronic Communications Privacy Act* e *Right of the Information Act*).

Una possibilità di ricorso più generale è offerta dall'APA, che può essere adita da qualsiasi persona che subisca una violazione a causa di un'azione di un'agenzia, o che sia danneggiata o lesa da un'azione dell'agenzia.

Infine, oltre alle vie di ricorso menzionate, ogni interessato ha il diritto di chiedere l'accesso ai documenti esistenti delle agenzie federali ai sensi della FOIA. L'ottenimento di tale accesso può anche facilitare l'avvio di procedimenti dinanzi ai tribunali ordinari, anche per dimostrare la propria legittimazione ad agire.

Le agenzie possono rifiutare informazioni che rientrano in alcune eccezioni elencate, tra cui l'accesso a informazioni classificate sulla sicurezza nazionale e a informazioni riguardanti le indagini delle forze dell'ordine, ma i denunciatori hanno facoltà di contestarla presentando un ricorso amministrativo e, successivamente, giudiziario innanzi ai tribunali federali.

8. IL PARERE DELL'EDPB SULL'ULTIMA DECISIONE DI ADEGUATEZZA RELATIVA AGLI U.S.A.

Non si è fatto attendere l'intervento dell'EDPB che il 28 febbraio 2023 ha pubblicato il proprio parere sulla bozza di decisione della Commissione europea riguardante gli USA ⁶².

Il Comitato si è espresso per alcuni aspetti in senso critico e, per altri, accogliendo favorevolmente alcune novità apportate con il nuovo accordo. Il Parlamento europeo, invece, l'11 maggio 2023 ha adottato la propria risoluzione con cui si è espresso in modo molto critico ⁶³.

In riferimento al parere dell'EDPB, si può notare che una prima parte è dedicata agli aspetti generali e la seconda ai profili

⁶² EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, consultabile su edpb.europa.eu.

⁶³ Risoluzione del Parlamento europeo dell'11 maggio 2023 sull'adeguatezza della protezione offerta dal quadro UE-USA in materia di privacy dei dati (2023/2501(RSP)). Con questa risoluzione il Parlamento — come già accaduto in precedenza — si è espresso in modo molto netto ricor-

dando che, con la risoluzione del 20 maggio 2021, aveva già invitato la Commissione a non adottare alcuna nuova decisione di adeguatezza in relazione agli Stati Uniti, a meno che non fossero state introdotte riforme significative, in particolare a fini di sicurezza nazionale e *intelligence*. Ha ritenuto non significativo l'E.O. 14086 e ha ribadito « che la Commissione non dovrebbe lasciare il compito di proteggere i diritti fondamentali dei cittadini dell'UE alla Corte di giustizia dell'Unione europea in conseguenza di denunce presentate dagli stessi singoli citta-

attinenti alla protezione dei dati personali. Infine, una terza è dedicata all'accesso ai dati da parte delle autorità pubbliche.

Nella prima parte introduttiva il Comitato segnala che i principi del DPF rimangono sostanzialmente invariati rispetto a quelli del *Privacy Shield* e sottolinea la necessità di ricevere maggiori informazioni del contesto normativo americano affinché possa essere compreso nel miglior modo l'interazione tra i principi DPF e l'ordinamento statunitense. Inoltre, viene criticata la struttura degli allegati al DPF piuttosto confusa così come la terminologia utilizzata, sollecitando una maggior coerenza sistematica ⁶⁴.

Nella parte relativa ai profili riguardanti la protezione dei dati personali e i principi ivi stabiliti, l'EDPB pone particolare risalto alle questioni concernenti i diritti degli interessati ⁶⁵, all'assenza di definizioni chiave, alla incertezza sull'applicazione dei principi del DPF agli incaricati del trattamento. L'EDPB ribadisce peraltro che il livello di protezione delle persone i cui dati sono trasferiti non deve essere compromesso da trasferimenti successivi da parte del destinatario dei dati trasferiti.

Ulteriori criticità deriverebbero dalla frammentazione della normativa statunitense in materia di *privacy* a seconda del settore di riferimento; ciò creerebbe differenti livelli di protezione da chiarire. Ancora. Per quanto riguarda i processi decisionali automatici viene sottolineato come dovrebbero essere stabilite garanzie come il diritto dell'individuo di conoscere la logica decisionale sottostante, il diritto di contestare la decisione e di ottenere un intervento umano quando la decisione incide significativamente sull'interessato.

Nella terza parte, invece, dedicata all'accesso ai dati da parte delle autorità pubbliche americane, il Comitato accoglie con più favore le modifiche apportate, riconoscendo un significativo miglioramento rispetto al quadro precedente. Viene tuttavia auspicato che l'adozione della decisione sia preceduta dall'adozione di politiche e procedure aggiornate per l'attuazione dell'E.●. 14086 da parte di tutte le agenzie di *intelligence* statunitensi e che queste

dini». Nella stessa recente risoluzione il Parlamento ha segnalato che i principi del quadro in materia di *privacy* dei dati del Dipartimento del commercio degli Stati Uniti non hanno subito modifiche sufficienti, rispetto al quadro precedente. Dunque, il Parlamento conclude ritenendo che il quadro UE-USA in materia di *privacy* non crea un'equivalenza essenziale del livello di protezione; ha quindi invitato la Commissione a proseguire i negoziati con le sue controparti statunitensi al fine di creare un meccanismo che garantisca tale equivalenza, nonché

l'adeguato livello di protezione richiesto dal diritto dell'Unione in materia di protezione dei dati e dalla Carta secondo l'interpretazione della CGUE; ha invitato la Commissione a non adottare la decisione di adeguatezza finché non saranno pienamente attuate tutte le raccomandazioni formulate nella risoluzione e nel parere dell'EDPB.

⁶⁴ Il Comitato riporta l'esempio della nozione di "processing".

⁶⁵ A titolo esemplificativo, alcune eccezioni al diritto di accesso e i tempi e le modalità del diritto di opposizione.

siano valutate, aggiornate e condivise da parte della Commissione europea.

L'EDPB saluta con favore l'introduzione dei concetti di necessità e proporzionalità nel quadro giuridico statunitense sui *Signals intelligence* oltre al nuovo meccanismo di ricorso stabilito, ritenuto notevolmente migliorato rispetto al precedente ⁶⁶. Viene riconosciuta positivamente la previsione di diritti e garanzie in precedenza escluse, nonché le maggiori garanzie d'indipendenza del DPRC e l'esistenza di poteri più efficaci per porre rimedio alle violazioni di legge.

Tuttavia, sono stati segnalati una serie di punti che richiederebbero ulteriori chiarimenti. Un primo punto riguarda i cc.dd. *temporary bulk collection*, nonché la conservazione e la diffusione dei dati raccolti in massa. Per questi viene sottolineato che sebbene l'E.O. 14086 contenga un elenco di scopi specifici per i quali la raccolta può o non può avvenire, essi potrebbero facilmente essere aggiornati con ulteriori e nuovi obiettivi alla luce di nuovi imperativi di sicurezza nazionale. Un altro aspetto delicato, secondo il Comitato, riguarderebbe l'ipotesi di raccolta di dati in massa ai sensi dell'E.O. 12333, il quale non prevede il requisito dell'autorizzazione preventiva da parte di un'autorità indipendente, come invece richiesto dalla più recente giurisprudenza della Corte europea dei diritti dell'uomo, né tantomeno un riesame sistematico indipendente *ex post* da parte di un tribunale o di un organismo indipendente equivalente. Inoltre, con riferimento all'autorizzazione preventiva e indipendente della sorveglianza ai sensi della Sezione 702 della FISA, l'EDPB si rammarica del fatto che quest'ultima non sia chiamata a verificare preventivamente il programma sulla conformità rispetto all'E.O. 14086 per quelle ipotesi in cui siano coinvolti individui non statunitensi.

Il parere, quindi, si conclude con richieste di approfondimenti e chiarimenti diretti alla Commissione europea.

9. VERSO SCHREMS III?

Si è visto che la circolazione dei dati ha una notevole rilevanza non solo per questioni riguardanti la sfera domestica, ma anche nella definizione di quei rapporti tra attori geopolitici. La costante evoluzione e la pervasività di questo tema dà la misura del valore

⁶⁶ L'EDPB saluta con favore anche le garanzie aggiuntive previste dal nuovo meccanismo di ricorso, come il ruolo dei difensori speciali e l'intervento del PCLOB. Le preoccupazioni riguardano l'applicazione generale della risposta *standard* del DPRC

che notifica all'interessato l'assenza di violazioni e la sua non impugnabilità complessivamente considerata. Data l'importanza del meccanismo di ricorso, il Comitato invita la Commissione a monitorare attentamente il suo funzionamento pratico.

sempre più pregnante di ciò che è in argomento ⁶⁷. La circolazione transfrontaliera dei dati, caratteristica dominante della società moderna, è una questione che impegna le istituzioni in ogni latitudine del globo ⁶⁸.

I fattori geopolitici emergono sotto differenti sfaccettature. Ad esempio, è nota la complementarità tra il tema dei dati personali e quello dello sviluppo di sistemi di intelligenza artificiale sempre più all'avanguardia che, in vero, si avvalgono proprio dei dati per il loro funzionamento ⁶⁹. I primi costituiscono il carburante dei secondi.

Perciò, non desta stupore che il 7 ottobre 2022 gli Stati Uniti hanno, da un lato, adottato l'E.O. 14086 — prodromico all'adozione della nuova decisione di adeguatezza da parte della Commissione europea — e, dall'altro, hanno provveduto ad emanare ulteriori misure restrittive volte a limitare l'esportazione verso la Cina di specifici sistemi *hardware* utilizzati per le operazioni e per lo sviluppo di sistemi di intelligenza artificiale ⁷⁰.

Limitandoci qui ad osservazioni circoscritte al primo tema, si

⁶⁷ Nel 2013 e 2014 le Nazioni Unite hanno adottato due risoluzioni su questioni riguardanti i dati personali e la tutela della "vita privata". Esse sono "The right to privacy in the digital age" ONU, Assemblea generale, A/RES/68/167, New York, 18 dicembre 2013; e ONU, Assemblea generale, "Revised draft resolution on the right to privacy in the digital age", A/C.3/69/L.26/Rev.1, New York, 19 novembre 2014, in risposta allo sviluppo di nuove tecnologie e alle rivelazioni sulla sorveglianza di massa effettuata in alcuni Stati (il riferimento è alle rivelazioni di E. Snowden). Queste risoluzioni condannano fermamente la sorveglianza di massa ed evidenziano l'impatto che tale sorveglianza può avere sui diritti fondamentali alla vita privata e alla libertà di espressione nonché sul funzionamento di una società democratica. Nei successivi anni sono state adottate altre revisioni delle risoluzioni sul tema: ONU, Assemblea generale, "Revised draft resolution on the right to privacy in the digital age", A/C.3/71/L.39/Rev.1, New York, 16 novembre 2016; ONU, Consiglio per i diritti umani, "The right to privacy in the digital age", A/HRC/34/L.7/Rev.1, 22 marzo 2017.

⁶⁸ In Africa sono attualmente in corso negoziati per un protocollo sul commercio digitale nell'ambito dell'*African Continental Free Trade Area* (AFCFTA) per la creazione di un mercato unico nel continente africano che riguarderà anche i flussi di dati transfrontalieri che potrebbero essere regolamentati da tale Protocollo. Si veda a tal proposito A. BEYLEVELD, F. SÜCKER, *Cross-*

border data flows in Africa: policy considerations for the afcfta protocol on digital trade, ottobre 2022, consultabile su ssrn.com. Per il continente africano, inoltre, è interessante quanto emerge dallo studio di T. ROBERTS, A. MOHAMED ALI, M. FARAHAT, R. OLOYEDE, G. MUTUNCU, *Surveillance Law in Africa: a Review of Six Countries*, Brighton: Institute of Development, 2021: la ricerca si focalizza sulle criticità in materia di trattamento dei dati personali che emergerebbero, in modo particolare, in sei stati africani tra cui Egitto, Kenya, Nigeria, Senegal, Sudafrica e Sudan. Le criticità sarebbero dovute alla riforma di leggi che estendono i poteri di sorveglianza dello Stato, alla mancanza di chiarezza normativa e protezione per la *privacy* nella legislazione esistente, al diffondersi delle tecnologie di sorveglianza che consentono sorveglianze illegali, alle agenzie statali che condividono regolarmente attività di sorveglianza al di fuori delle leggi, all'impunità per i trasgressori e alla insufficiente capacità della società civile di riconoscere lo Stato come soggetto responsabile.

⁶⁹ G. GRÖGER, *There Is No AI Without Data*, in *Communications of the ACM*, vol. 64, 2021, 11, pp. 98-108.

⁷⁰ Già nel 'Final Report' del *National Security Commission on Artificial Intelligence* del marzo 2021 si legge che « *we must win the AI competition that is intensifying strategic competition with China. China's plans, resources, and progress should concern all Americans. It is an AI peer in many areas and an AI leader in some applica-*

può osservare come la nota sentenza *Schrems II* abbia prodotto risultati incoraggianti e altri più deludenti che si scontrano con le dinamiche di *realpolitik*. Infatti, tra questi ultimi, v'è un risultato non troppo positivo in tema di certezza del diritto, ossia che, nonostante il chiaro tenore della sentenza, le dinamiche riguardanti la circolazione transfrontaliera dei dati non hanno visto un vero e proprio adeguamento o ridimensionamento pratico; la società Meta ha infatti continuato a trasferire dati sulla base delle clausole contrattuali tipo senza adottare alcuna misura supplementare atta a dimostrare una protezione equivalente a quella europea e il DPC irlandese è intervenuto, ma a distanza di quasi tre anni dalla sentenza *Schrems II*, ossia con la decisione del 12 maggio 2023⁷¹. Tuttavia, seppur a distanza di anni, con la sua decisione il DPC si è adeguato alla pronuncia della CGUE dichiarando che l'ordinamento americano non garantisce un livello di protezione equivalente a quello europeo e ha affermato, a chiare lettere, *inter alia*, che « *in making the Data Transfers, Meta Ireland is infringing Article 46(1) GDPR* »⁷².

La pronuncia della Corte ha portato, però, anche a risultati positivi, di talché negli USA — sebbene con qualche travagliata dinamica tra Stati e amministrazione federale — si è intrapresa un'opera legislativa che si avvicina timidamente agli *standard* europei sebbene le più recenti novità che hanno portato alla proroga della discussa sezione 702 FISA possano scoraggiare⁷³.

Tutto ciò, in ogni caso, ha permesso di giungere al nuovo accordo tra UE e USA e a una nuova decisione di adeguatezza con specifiche peculiarità che ha già impegnato l'EDPB e, si può ipotizzare, un giorno, anche la CGUE.

Dagli scenari che si sono venuti a realizzare, l'auspicio, va da sé, è quello di un superamento della fase di stallo creatasi, a beneficio della certezza del diritto, delle imprese e degli utenti dei vari servizi, soprattutto nel mercato digitale. È necessario altresì definire il margine di operatività dell'attività di *intelligence* estera che alcuni sostengono, in modo controverso, essere inevitabile⁷⁴.

tions. We take seriously China's ambition to surpass the United States as the world's AI leader within a decade », p. 2.

⁷¹ "Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. Further to an own-volition inquiry under Section 110 of the Data Protection Act 2018", consultabile al sito edpb.europa.eu

⁷² *Ivi*, p. 212, § 10.2. Perciò, il DPC ha ordinato di sospendere, secondo una precisa tabella temporale, il trasferimento dei dati personali verso gli Stati Uniti. Ha inol-

tre escluso l'applicabilità, da parte di Meta, della deroga del consenso di cui all'art. 49 GDPR per procedere con i trasferimenti dei dati.

⁷³ L'estensione di quattro mesi della Sezione 702 del *Foreign Intelligence Surveillance Act* (FISA) è il frutto della recente approvazione del *National Defense Authorization Act* (NDAA), ossia l'ultima legge statunitense sulla politica di difesa americana. A fronte di una vigenza della predetta Sezione fino al 31 dicembre 2023, è stata approvata una proroga sino al 19 aprile 2024.

⁷⁴ A. LUBIN, *'We Only Spy on Forei-*

A tal proposito, però, la nuova decisione per gli U.S.A. — come già risaltato dall'EDPB — non è esente da criticità. Sicché il dibattito potrebbe riguardare differenti profili. Si può prevedere un'analisi focalizzata su quelle regole sancite a definizione dei limiti dei diritti e delle libertà degli individui, ovvero, verificando se siano sufficientemente chiare e precise in virtù del principio di proporzionalità. Ci si chiede, dunque, se (nell'ambito dei programmi di sorveglianza) le regole di riferimento siano sufficienti nella individuazione delle categorie di persone potenzialmente destinatarie delle misure; nell'individuazione del limite di durata della misura; nell'indicazione della procedura per l'esame, utilizzo e conservazione dei dati ricavati ⁷⁵.

Peraltro, l'ordine esecutivo del 7 ottobre 2022, sebbene circoscriva a determinate ragioni e limiti l'attività di *intelligence*, non impedisce di certo l'attività di *Signals Intelligence* e non impedisce la c.d. *bulk collection*, ossia la raccolta massiva di dati personali riguardanti cittadini di Stati stranieri. Questo profilo, invero, è stato già segnalato in senso critico dal DPC irlandese con la succitata decisione del 12 maggio 2023 ⁷⁶.

Al di là di quanto espresso dall'autorità irlandese, tra le ragioni che legittimano l'attività di *Signal Intelligence* ve ne sono alcune piuttosto vaghe, tanto da far dubitare sulla conformità rispetto a quella proporzionalità a cui si riferisce la CGUE, che rimane un principio concettualmente diverso rispetto a quello oltreoceano. L'ordine esecutivo, a titolo esemplificativo, prevede tra queste ragioni — al fine di proteggere la sicurezza nazionale degli Stati Uniti e dei suoi alleati e *partner* — quello di comprendere o valutare le capacità, le intenzioni o le attività di un governo o esercito straniero, di una regione di una nazione straniera, di un'organizzazione politica con sede all'estero o di un'entità che

gners': *The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, in *Chicago Journal of International Law*, Vol. 13, 2018, 2, pp. 502 e ss. sostiene che un diritto universale alla privacy è un falso mito, nonché la legittimità di una distinzione tra norme che prevedono *standard* di tutela più elevate per i cittadini di uno Stato e meno elevati per chi risiede oltre confine.

⁷⁵ CEDU, *Weber and Saravia v. Germany*, 54934/00, consultabile su hudoc.echr.coe.int.

⁷⁶ Cfr. *Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act cit.*, § 2.61, p. 25. L'Autorità irlandese si è espressa in modo critico sull'E.O. 14086 — sebbene in epoca antecedente all'adozione della nuova decisione di adeguatezza — anche su altre questioni riguardanti i rimedi ivi previsti;

cfr. pp. 21-25. La critica principale riguardava la circostanza che l'Ordine esecutivo contempla, come rimedio processuale, un ricorso la cui legittimazione sarebbe spettata ai soli Stati designati come *Stati qualificati* e, tra questi non compariva ancora alcuno Stato europeo. La questione è stata poi superata allorché, in data 30 giugno 2023, il Procuratore generale del dipartimento di giustizia americano ha designato « *the EU, Iceland, Liechtenstein, and Norway as qualifying states for purposes of eligibility for the redress mechanism established in section 3 of Executive Order 14086* »; la designazione in questione è diventata efficace a partire dal 11 luglio 2023, vale a dire, a seguito dell'adozione della decisione di adeguatezza n. 1795/2023 della Commissione europea. Il documento del Procuratore generale è consultabile al sito justice.gov

agisce per conto o sotto il controllo di un governo, di un esercito, di una regione o di un'organizzazione politica straniera;⁷⁷ oppure, altrettanto vaga sarebbe l'attività volta a comprendere o valutare le minacce transnazionali che hanno un impatto sulla sicurezza globale, tra cui il cambiamento climatico e altri cambiamenti ecologici, i rischi per la salute pubblica, le minacce umanitarie, l'instabilità politica e le rivalità geografiche⁷⁸; oppure, per proteggere dalle minacce al personale degli Stati Uniti o dei suoi alleati o *partner*⁷⁹. Quest'ultimo obiettivo riguarderebbe anche l'attività di *bulk collection*.

Sebbene l'ordine esecutivo restringa gli scopi per la raccolta di dati in massa, tale sistema rispecchierebbe in larga parte quei limiti e quei contorni già stabiliti nel PPD-28 che hanno suscitato critiche e condotto alla storica *Schrems II*⁸⁰. Va da sé che, però, l'ordine esecutivo presenta elementi positivi di novità, tra cui la previsione di un medesimo livello di tutela per tutte le persone, precedentemente garantito ai soli cittadini statunitensi.

In tema di conservazione dei dati personali da parte delle agenzie di *intelligence* l'ordine esecutivo prevede infatti che la conservazione (a) delle informazioni personali di individui non statunitensi, raccolte attraverso l'*intelligence* dei segnali può avvenire solo se la conservazione di informazioni analoghe riguardanti persone statunitensi fosse consentita dalla legge sottopo-

⁷⁷ L'ordine esecutivo così testualmente stabilisce: « (i) *Legitimate objectives*. (A) *Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives: (1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners* ».

⁷⁸ « *Understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry* ».

⁷⁹ L'ordine esecutivo si limita a prevedere: « *protect against threats to the personnel of the United States or its allies or partners* ». Con il termine *personnel*, l'ordine esecutivo precisa che deve intendersi qualsiasi membro attuale o ex membro delle Forze Armate degli Stati Uniti, qualsiasi funzionario attuale o precedente del Governo degli Stati Uniti e qualsiasi altra per-

sona attualmente o precedentemente impiegata o che lavora per conto del Governo degli Stati Uniti, nonché qualsiasi membro attuale o ex delle Forze Armate, funzionario attuale o ex, o altra persona attualmente o precedentemente impiegata o che lavora per conto di un alleato o *partner*.

⁸⁰ Con la PPD-28 si prevedeva che l'attività di *bulk collection* potesse avvenire per (1) spionaggio e altre minacce e attività dirette da potenze straniere o dai loro servizi di *intelligence* contro gli Stati Uniti e i loro interessi; (2) minacce agli Stati Uniti e ai loro interessi derivanti dal terrorismo; (3) minacce agli Stati Uniti e ai loro interessi derivanti dallo sviluppo, dal possesso, dalla proliferazione o dall'uso di armi di distruzione di massa; (4) minacce alla sicurezza informatica; (5) minacce alle Forze armate statunitensi o alleate o ad altro personale statunitense o alleato; e (6) minacce transnazionali, compresa la finanza illecita e l'elusione delle sanzioni connesse. In nessun caso l'*intelligence* dei segnali raccolta in massa avrebbe potuto essere utilizzata allo scopo di reprimere o appesantire le critiche o il dissenso; svantaggiare le persone in base alla loro etnia, razza, sesso, orientamento sessuale o religione; offrire un vantaggio competitivo alle aziende statunitensi e ai settori commerciali statunitensi.

nendo tali informazioni agli stessi periodi di conservazione applicabili a cittadini statunitensi; (b) delle informazioni personali di persone non statunitensi raccolte attraverso l'*intelligence* dei segnali per le quali non è stata presa una decisione definitiva sulla conservazione agli stessi periodi di conservazione temporanea che si applicherebbero a informazioni comparabili riguardanti persone statunitensi; e prevede (c) la cancellazione delle informazioni personali di persone non statunitensi raccolte attraverso l'*intelligence* dei segnali che non possono più essere conservate, al pari della cancellazione di informazioni riguardanti cittadini statunitensi.

Il principio di minimizzazione dei dati e la loro conservazione da parte delle agenzie di *intelligence* nella realtà dei fatti, però, come testimoniato da episodi concreti, richiedono un più difficile controllo⁸¹. Ancora. Si può osservare come l'ordine esecutivo in tesi non si applicherebbe a quei dati a cui le autorità pubbliche accedono attraverso altri strumenti come, ad esempio, attraverso il *US Cloud Act* o il *US Patriot Act*, mediante operazioni di tipo commerciale o accordi volontari di condivisione di dati.

Nondimeno, un profilo che potrà rilevare emerge anche a seguito di una importante pronuncia della CGUE del 4 luglio 2023 (CGUE C-252/21). Infatti, nell'allegato I, sez. III, della decisione di adeguatezza si fa menzione dell'aspetto riguardante i dati sensibili (o "dati particolari" stando al lessico del GDPR) e si specifica che l'organizzazione non è obbligata a ottenere il consenso esplicito dell'interessato per i dati sensibili in determinate circostanze, tra cui l'ipotesi in cui l'interessato abbia reso manifestamente pubblici i dati in questione. Ebbene, tale formula piuttosto generica, deve essere criticamente letta in combinato con i principi stabiliti dalla Corte di giustizia con la sentenza del 4 luglio. Infatti, questa ha stabilito precisi parametri perché si possa ritenere che un utente abbia reso manifestamente pubblici i propri dati, ai sensi di detto articolo 9, paragrafo 2, lettera e), GDPR. Nella sentenza si legge testualmente che l'articolo 9, par. 2, lettera e), GDPR deve essere interpretato nel senso che:

« un utente di un social network online, allorché consulta siti Internet oppure applicazioni correlati a una o più delle categorie menzionate all'articolo 9, paragrafo 1, di detto regolamento, non rende manifestamente pubbliche, ai sensi della prima di tali disposizioni, i dati relativi a tale consultazione, raccolti dall'operatore di detto social network online mediante cookie o simili tecnologie di registrazione.

Quando inserisce dati in tali siti Internet o applicazioni nonché

⁸¹ Si veda il 'Memorandum and opinion order' della *Foreign Intelligence Surveillance Court* del 26 aprile 2017, consultabile su dni.gov

quando attiva pulsanti di selezione integrati in questi ultimi, come i pulsanti « Mi piace » o « Condividi » o i pulsanti che consentono all'utente di identificarsi su un sito Internet o su un'applicazione utilizzando gli identificativi di connessione collegati al suo account di utente del social network, il suo numero di telefono o il suo indirizzo di posta elettronica, tale utente rende manifestamente pubblici, ai sensi di detto articolo 9, paragrafo 2, lettera e), del RGPD, i dati così inseriti o risultanti dall'attivazione di tali pulsanti soltanto se abbia esplicitamente espresso preliminarmente, se del caso sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone ».

Un altro aspetto del nuovo accordo UE-USA potrebbe riguardare la portata vincolante di quei poteri facenti capo agli organi statunitensi chiamati a valutare eventuali violazioni. Su quest'ultimo punto si può osservare come le modifiche apportate potrebbero essere valutate favorevolmente per i soggetti privati che raccolgono i dati personali. Invero, il sistema dell'iscrizione alla lista delle organizzazioni aderenti al DPF come presupposto per l'applicazione della decisione di adeguatezza fa sì che il potere di espellere dalla lista in questione una determinata organizzazione ritenuta "colpevole", unitamente ad altre possibili misure, possa essere di per sé un valido rimedio.

Gli altri temi, molto probabilmente, riguarderanno l'effettiva indipendenza degli organi chiamati a svolgere indagini e pronunciarsi sui ricorsi⁸², nonché la natura e la portata del provvedimento che ha in gran parte consentito di giungere al nuovo progetto di decisione.

In riferimento alla prima questione, sembrerebbero ancora esistenti le criticità sollevate dalla *Schrems II*, considerato che alcuni degli organi presi in considerazione dall'Ordine esecutivo (in particolare il DPRC) appartengono al ramo esecutivo. In riferimento alla seconda questione, invece, l'ordine esecutivo può essere ritenuto *debole*, nel senso che lo stesso non rientra tra le fonti legislative ed è facilmente modificabile o revocabile dallo stesso o da un successivo Presidente. Perciò, l'attività di monitoraggio da parte della Commissione e delle rispettive Autorità garanti degli Stati membri, e i tempi di intervento, giocherebbero un ruolo essenziale.

⁸² Molti di questi organi sono stati "proposti" nella già citata letteratura statunitense di cui al § 5.2 che ha segnalato come possibili enti competenti il PCLO e il PCLOB che, sebbene non possiedano le caratteristi-

che di indipendenza rispetto al potere esecutivo, potrebbero essere sottoposte al vaglio di un giudice federale indipendente come il FISC e il FISCR in caso di impugnazione, per giungere infine alla Corte suprema.

Quanto appena analizzato riguarda il panorama statunitense che, sebbene sia mutato, presenta ancora sostanziali criticità ⁸³.

D'altro canto, il piano di riforme inglese, invece, sembrerebbe andare nella direzione opposta e, infatti, la decisione riguardante il Regno Unito, con tutte le dinamiche geopolitiche del caso, potrà suscitare ampi dibattiti e imponderabili sviluppi, inclusi quelli di natura giurisdizionale. Nella materia in questione il c.d. effetto Bruxelles ha, quindi, generato in molti casi risultati positivi e, in altri — stante la complessità del meccanismo stabilito nel GDPR — ha creato incertezza e *impasse* che devono essere necessariamente superate. Questo risultato può essere ottenuto solo mediante sforzi più profusi tra gli attori geopolitici coinvolti.

10. LA DECISIONE DI ADEGUATEZZA PER IL REGNO UNITO.

La Commissione europea — lo si è accennato nel precedente paragrafo — ha recentemente adottato una decisione di adeguatezza anche per il Regno Unito a seguito del noto procedimento di recesso dall'UE che nel gergo comune è stato denominato *brexit* ⁸⁴. Anche tale decisione ha le sue peculiarità sotto vari aspetti ⁸⁵.

Da un lato, l'analisi su cui la decisione si fonda si è rivelata più agevole per la Commissione poiché la normativa vigente in quei territori ricalca strutturalmente la normativa europea, tanto da essere denominato il GDPR del Regno Unito. L'ulteriore dato che ha agevolato l'adozione della decisione risiede nell'adesione del Regno Unito alla CEDU e alla convenzione 108 ⁸⁶, nonché il suo assoggettamento alla giurisdizione della Corte europea dei diritti dell'uomo.

Dall'altro lato, si consideri che sono attualmente in corso dibattiti in seno al parlamento inglese sul tema riguardante le modifiche alla disciplina dei dati personali e ciò prelude a importanti riforme. È per tale ragione che la decisione presenta una vera e

⁸³ Il sistema si presenta ancora piuttosto fragile rispetto ad un modello di decisione di adeguatezza come quello relativo al Giappone in cui v'è la designazione di un'Autorità indipendente e un meccanismo molto stringente di accesso ai dati per finalità di sicurezza nazionale. USA e Giappone, però, si differenziano in termini di postura strategica.

⁸⁴ La decisione di adeguatezza è stata adottata il 28 giugno 2021.

⁸⁵ A. CHOROMIDOU, *EU data protection under the TCA: the UK adequacy decision and the twin GDPRs*, in *International Data Privacy Law*, Vol. 11, 2021, 4, p. 388.

⁸⁶ la Convenzione 108 è vincolante per

gli Stati contraenti. Essa non è soggetta al controllo giudiziario della Corte EDU, ma è stata tenuta in considerazione nella giurisprudenza della Corte nel quadro dell'art. 8 della CEDU. Nel 2001 è stato adottato un Protocollo addizionale alla Convenzione 108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti e l'istituzione obbligatoria delle autorità nazionali di controllo per la protezione dei dati. Tale Convenzione è stata di recente oggetto di un processo di modernizzazione. Questo processo è stato completato il 18 aprile 2018 con l'adozione del protocollo di modifica della Convenzione 108 (Protocollo CETS No. 223).

propria scadenza a giugno 2025 che comporterà un'analisi *ex novo* dell'intero assetto normativo da parte della Commissione. A tal proposito, infatti, il Parlamento europeo con la sua risoluzione alla bozza di decisione di cui si discute prendeva atto « della strategia nazionale del Regno Unito in materia di dati, aggiornata il 9 dicembre 2020, che suggerisce un passaggio dalla protezione dei dati personali a un uso e una condivisione maggiori e più ampi dei dati »; rilevava « che tale posizione secondo cui la mancata comunicazione dei dati può avere un impatto negativo sulla società, come enunciata nella strategia, non è compatibile con i principi di minimizzazione dei dati e limitazione della finalità ai sensi dell'RCPD e del diritto primario »⁸⁷.

L'altra peculiarità della decisione, sebbene la formulazione sia stata ritenuta troppo vaga dall'EDPB, risiede nel fatto che la stessa non riguarda i dati personali trasferiti per finalità di controllo dell'immigrazione da parte del Regno Unito o che rientrano nell'ambito di applicazione dell'esenzione rispetto a determinati diritti degli interessati ai fini di mantenimento dell'effettivo controllo dell'immigrazione.

L'altro elemento risaltato riguarda anche qui il profilo delle *intelligence*, e quindi, i poteri delle autorità pubbliche nell'accesso ai dati personali per motivi di sicurezza nazionale. Le agenzie inglesi, al pari di quelle statunitensi, godono notoriamente di ampi poteri in tal senso e le loro attività sono già state oggetto di importanti pronunce come la sentenza CEDU *Big Brother Watch*⁸⁸. Su questo tema la Corte ha sancito importanti principi anche nel caso *Centrum för rättvisa c. Svezia*⁸⁹.

⁸⁷ European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)).

⁸⁸ *Case of Big Brother Watch and Others v. United Kingdom, Applications 58170/13, 62322/14 and 24960/1, Judgment*. Il 25 maggio 2021 si è pronunciata la Grande Camera stabilendo che « 1. La sorveglianza di massa sulle comunicazioni, come disciplinata dal diritto britannico, non è soggetta ad una verifica di necessità e proporzionalità (che assicuri, ad esempio: che le intercettazioni siano soggette all'autorizzazione di un organo indipendente; che l'oggetto e l'ambito di applicazione delle misure di sorveglianza siano ben definite; che vi sia controllo, *ex ante* ed *ex post*, da parte di un organismo indipendente). Sebbene gli stati godano di un ampio margine di apprezzamento nel decidere quali misure di sorveglianza siano più adatte a difendere la propria sicurezza nazionale, vi è una violazione dell'art. 8 CEDU. 2. La disciplina britan-

nica che consente lo scambio di informazioni con i servizi di intelligence stranieri non viola l'art. 8 CEDU. Infatti, la supervisione e la possibilità di review da parte di organi indipendenti su queste operazioni appaiono adeguate. 3. La disciplina britannica che governa l'acquisizione dai dati dai service providers viola l'art. 8 CEDU, perché le circostanze che rendono possibile l'acquisizione non sono "stabilite per legge". 4. La disciplina britannica sulla sorveglianza di massa viola l'art. 10 CEDU, nella misura in cui non sono previste garanzie speciali quando viene in gioco materiale che richiede specifica confidenzialità — ad esempio materiale giornalistico confidenziale », consultabile su hudoc.echr.coe.int.

⁸⁹ Con questa pronuncia del 25 maggio 2021, n. 35252/08, la Corte EDU (Grande Camera), ha stabilito che « 1) Alla luce del proliferare delle minacce alla sicurezza nazionale e dell'ampio uso che i terroristi fanno di Internet, agli Stati deve essere riconosciuto un alto margine di apprezzamento nel

Peraltro, anche l'EDPB nel parere che ha preceduto l'adozione della decisione di adeguatezza ha avanzato le sue perplessità⁹⁰. Tra le sue varie osservazioni, nell'ambito delle intercettazioni massive di dati da parte delle *intelligence* — i c.d. *bulk power* — ha sottolineato come i dati raccolti massivamente, secondo la legislazione inglese, possono essere conservati per lunghi periodi in modo da essere disponibili per un ulteriore e futuro accesso. La disciplina dell'IPA del 2016 — con margini piuttosto ampi — prevede solo la distruzione delle copie dei dati raccolti e solo se la loro conservazione non sia necessaria nell'interesse della sicurezza nazionale o per altri motivi che rientrano nell'ambito di applicazione della sezione 138, par. 2, dell'IPA 2016. È stato così sottolineato come il riferimento sia rivolto alla distruzione delle sole copie.

Il Comitato, perciò, invitava la Commissione a fornire ulteriori chiarimenti e valutazioni sulle intercettazioni di massa, in particolare sulla loro selezione, per chiarire in che misura l'accesso ai dati personali soddisfi quei principi stabiliti dalla CGUE e quali salvaguardie siano previste per proteggere i diritti fondamentali delle persone i cui dati sono intercettati in questo ambito, anche per ciò che riguarda i periodi di conservazione dei dati.

È ancora più netto il Parlamento europeo là dove nella risoluzione citata si pronuncia in merito ad alcune attività di *intelligence* britannica tra cui, in particolare, il programma *Tempora* gestito dal *Government Communications Headquarters* (GCHQ — quartier generale delle comunicazioni del governo) del Regno Unito con il quale vengono intercettate le comunicazioni in tempo reale attraverso i cavi in fibra ottica della dorsale internet e si registrano i dati in modo che possano essere trattati e consultati in un momento successivo; un'attività di sorveglianza di massa del

decidere quali sono le misure migliori per proteggere la sicurezza dei loro cittadini. Pertanto, la scelta di disporre misure di sorveglianza che intercettino le comunicazioni su Internet non è, di per sé, contraria all'art. 8 CEDU. 2) Nondimeno, nel disciplinare le proprie misure di sorveglianza, gli Stati non possono sottrarsi alle basiche garanzie sottese al principio di proporzionalità. Ad esempio, l'intercettazione deve essere soggetta all'autorizzazione di organismi indipendenti; l'oggetto e l'ambito di applicazione delle misure di sorveglianza deve essere ben definito; le operazioni devono essere svolte sotto la supervisione di un organo indipendente e deve esserci possibilità di controllo *ex post*. 3) Il regime di sorveglianza svedese non rispetta pienamente questi requisiti. In particolare, vi sono tre criticità. Primo, non vi sono regole

chiare che riguardino la distruzione del materiale intercettato; secondo, non viene imposto che, quando il materiale intercettato è condiviso con i servizi di intelligence stranieri, debba essere fatta una valutazione anche alla luce delle esigenze della vita privata e familiare, oltre che di quelle della sicurezza nazionale; terzo, non vi è effettiva possibilità di controllo *ex post* sulle misure poste in essere». La pronuncia in questione rileva anche perché dichiara legittima l'adozione di un diverso regime giuridico per la sorveglianza domestica e quella straniera. Sentenza consultabile al sito hudoc.echr.coe.int.

⁹⁰ EDPB, 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.

contenuto e dei metadati delle comunicazioni che, sottolinea il Parlamento UE, avviene indipendentemente dalla sussistenza di sospetti specifici o di particolari obiettivi⁹¹. Sul tema della sorveglianza, quindi, l'istituzione europea invitava gli Stati membri a concludere accordi di “non spionaggio” con il Regno Unito e invitava la Commissione a utilizzare le sue interlocuzioni con le controparti britanniche per rappresentare che, se le leggi e le pratiche di sorveglianza del Regno Unito non fossero modificate, l'unica opzione percorribile per facilitare le decisioni di adeguatezza sarebbe la conclusione di accordi di “non spionaggio” con gli Stati membri.

Dunque, già lo stato di fatto del quadro normativo inglese genera di per sé perplessità in tema di quella adeguatezza richiesta dal GDPR; a ciò si aggiunga il processo di riforme in discussione proprio in quelle latitudini. Il *Data Protection and Digital Information Bill* così come proposto nel luglio scorso⁹² prevedeva importanti modifiche normative che si discostavano dal GDPR, tra cui quelle relative alla definizione di “dati personali” in termini di “identificabilità” dell'interessato, così come in relazione ai processi decisionali automatizzati prevedendo una riduzione dei limiti al ricorso a tali operazioni⁹³. Ulteriori modifiche riguarderebbero poi proprio l'ambito del trasferimento transna-

⁹¹ Nella risoluzione si legge, quindi, che il Parlamento: « ritiene inaccettabile che i progetti di decisione di adeguatezza non tengano conto dell'assenza di restrizioni all'utilizzo da parte del Regno Unito dei poteri sui dati in blocco, né dell'effettivo ricorso alle operazioni di sorveglianza del Regno Unito e degli Stati Uniti, come descritto da Edward Snowden, compreso il fatto che: a) l'ICO o gli organi giurisdizionali non effettuano un controllo sostanziale efficace sul ricorso all'esenzione per la sicurezza nazionale prevista dalla legislazione del Regno Unito relativa alla protezione dei dati; b) le restrizioni di utilizzo dei poteri su dati in blocco da parte del Regno Unito non sono previste dalla legge stessa, come richiesto dalla CGUE (ma sono invece lasciate alla discrezione dell'esecutivo soggetta a un “rispettoso” controllo giurisdizionale); c) la descrizione di “dati secondari” (metadati) nei progetti di decisione è gravemente fuorviante e non precisa che tali dati possono contenere molte informazioni ed essere altamente invasivi, e che sono soggetti a sofisticate analisi automatizzate (come dichiarato dalla CGUE nella causa “Digital Rights Ireland”) ma che tuttavia, ai sensi della legislazione britannica, i metadati non sono adeguatamente protetti dall'accesso indebito, dalla raccolta in blocco e dall'analisi

basata sull'intelligenza artificiale da parte delle agenzie di intelligence del Regno Unito; d) le “Five Eyes Agencies”, in particolare il GCHQ e l'Agenzia nazionale per la sicurezza (NSA), condividono nella pratica tutti i dati di intelligence ».

⁹² S. WILKINSON, *UK data protection and digital information bill explained*, in *Journal of Data Protection & Privacy*, Vol. 5, 2022, 3, pp. 242-253; I. LLOYD, *Moving UK Data Protection Law Away from EU Standards - Legislative Focus Areas in 2022 - New Directions Forward or Steps Backwards in UK Data Protection and Digital Information Bill?*, in *Computer Law Review International*, 2022, 6, pp. 180 e ss.

⁹³ In connessione con il tema dei dati personali, peraltro, nel Regno Unito è stato recentemente proposto, per scopi di sicurezza e tutela dei minori, il disegno di legge *Online Safety Bill*, attualmente all'esame del parlamento inglese. Tale disegno di legge non è andato esente da critiche, soprattutto da parte di operatori del mercato in tema di comunicazioni private e sicure. Infatti, *Signal* ha recentemente palesato la possibilità di abbandonare il mercato inglese in caso di approvazione di tale disegno di legge poiché, secondo alcuni, indebolirebbe la *privacy* garantita dai sistemi delle piattaforme tramite la nota crittografia *end-to-end*. L'af-

zionale dei dati personali verso un sistema più favorevole ad una “circolazione” internazionale dei dati personali. Da ultimo, insieme ad altre modifiche, la riforma avrebbe previsto anche il mutamento — in senso meno restrittivo — del profilo riguardante *cookie* e altre tecnologie di tracciamento, utilizzabili senza il consenso dell'interessato ⁹⁴.

A fronte di un piano di riforma sostanzialmente modificativo dell'impianto giuridico in materia di dati personali, più di recente si è assistito ad una sua “sospensione” volta a considerare nuovamente il progetto. Il motivo principale che ha condotto a riconsiderare l'intervento normativo (fino ad una nuova versione del testo annunciata nei primi mesi del 2023) ⁹⁵ riposa proprio sulla preoccupazione di possibili ripercussioni sulla decisione di adeguatezza adottata dalla Commissione europea nel 2021. Pertanto, alcuni membri del governo britannico hanno espresso l'intenzione di riflettere un quadro normativo in materia di *privacy* che possa garantire un'adeguatezza rispetto alla normativa europea al pari di quanto è avvenuto con altri Stati come Giappone, Corea del Sud, Canada e Nuova Zelanda. Questo è l'effetto Bruxelles.

Abstract

This paper analyses the rules laid down in Regulation no. 679/2016 on General Data Protection concerning the transfers of personal data to third countries. This topic has long been the subject of scholarly debates and legislative initiatives, in particular with regard to those importing States where public authorities have broad powers of access to the data in question. According to the principles laid down by the European Court of Justice, therefore, it is necessary to assess on a case-by-case basis whether protection equivalent to European protection is guaranteed, with particular focus on the proportionality principle and fundamental rights. The newest developments, addressed in this paper, concern the United Kingdom and the United States of America.

fievolimento delle tutele deriverebbe da un dovere di scansione dei messaggi della rete volte a scovare comunicazioni di matrice pedopornografica e terroristica.

⁹⁴ Ciò sarebbe consentito, a titolo esemplificativo, per finalità legate al miglioramento del servizio, sito web o app, oppure per consentire l'adattamento delle funzioni del servizio alle preferenze dell'utente.

⁹⁵ L'8 marzo 2023 il governo britannico ha annunciato una nuova versione del *Data Protection and Digital Information Bill* ritenendola una iniziativa legislativa che favorisce le imprese e allo stesso tempo garantisce un'elevata protezione dei dati personali. Fonte normativa consultabile su gov.uk.

