Flavia Cristiano(*)

IL REGOLAMENTO UE 679/2016 E I TRASFERIMENTI EXTRA UE DEI DATI PERSONALI NEL CONTESTO UNIVERSITARIO

Abstract: This work examines the framework of rules related to the transfer of personal data to non-EU countries and international organizations, focusing on the data processing activities carried out by Italian public universities as part of their institutional purposes. A summary of the guarantees applicable to the processing of personal data is proposed, that considers the balance between the rights to be respected and the laws applicable to the university context. This summary also takes into account the consequences of the recent *Schrems II* ruling of the EU Court of Justice on transfers abroad of personal data processed by entities established in the EU.

1. — *Premessa.*

Con il regolamento UE 679/2016 (nel seguito, GDPR) il bilanciamento tra i due contrapposti diritti, alla protezione dei dati personali e alla loro libera circolazione, realizza un quadro normativo complesso cui il titolare o il responsabile del trattamento dei dati deve attenersi, per ogni attività di trattamento di dati personali che pone in essere.

Come riportato al Considerando 101 GDPR, «I flussi di dati personali

(*) Università degli Studi di Perugia, Università per Stranieri di Perugia.

verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale». L'Unione europea ha investito nella strategia del Mercato unico digitale e riconosce che «l'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali», in particolare per quei trasferimenti di dati verso quei paesi, esterni allo Spazio Economico Europeo[1], che non consentono di garantire alle persone il controllo dei loro dati personali né il rispetto di quei diritti costituzionalmente garantiti nei territori dell'Unione europea.

Focus di questo approfondimento sarà tentare una sintesi delle garanzie applicabili ai trattamenti di dati personali, con uno sguardo particolare a quelli svolti dall'Università statale nell'ambito delle proprie finalità istituzionali, quando tali trattamenti comportano il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale.

Con riguardo alla protezione dei dati personali, andrà tenuto conto del contesto normativo generale a cui l'Università deve attenersi e delle indicazioni normative o di soft law ad essa applicabili per valutare, nei vari contesti dell'attività di trattamento, gli adempimenti da porre in essere.

Un primo studio di questo scenario è stato condotto agli inizi del 2019[2], per mettere a fuoco la presenza di eventuali differenze sostanziali introdotte dal GDPR, rispetto la precedente direttiva 45/96/CE, e fornire spunti operativi utili alla comunità dei DPO universitari che si andava formando. Viene ora ripreso e aggiornato, alla luce delle conoscenze acquisite con il master e delle interpretazioni del GDPR emerse nel corso di questi due anni, con particolare riguardo alle indicazioni dell'European Data Protection Board (EDPB) ed alla sentenza della Corte di giustizia dell'Unione europea (CGUE) che si è pronunciata, a luglio dello scorso anno, invalidando la decisione di adeguatezza del *Privacy Shield* per i trasferimenti dei dati verso gli USA.

---

[1] Corrispondente all'UE assieme a Norvegia, Liechtenstein, Islanda.

[2] Il lavoro è stato svolto dalla scrivente nell'allora sottogruppo di lavoro del gruppo GLAT del Codau. È stato pubblicato nel forum dei DPO universitari per essere liberamente utilizzabile da chiunque avesse voluto condividerlo nella propria università, come poi in effetti avvenuto da parte di alcuni Atenei che lo hanno pubblicato nel proprio sito web.

2. — *Contesto normativo.*

Ogni persona ha diritto alla protezione dei dati personali. Questo diritto è tutelato su più livelli, in quanto previsto dal diritto europeo[3], da fonti di diritto interno e costituzionali[4], e dal diritto internazionale/pattizio/consuetudinario.

L'art. 7 della Carta dei diritti fondamentali dell'Unione Europea (nel seguito Carta o CDFUE) garantisce ad ogni persona il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni, mentre l'art. 8, § 1 della Carta, riconosce esplicitamente a ogni persona il diritto alla protezione dei dati personali che la riguardano.

La tutela delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale, non assoluto, da considerare alla luce della sua funzione sociale[5]; va quindi contemperato[6] con altri diritti fondamentali tra i quali, di interesse per il contesto di questo approfondimento, la libertà di pensiero, di espressione e di informazione, la libertà delle arti e della ricerca scientifica e, non ultime, la libertà personale e la libertà accademica[7].

Il contesto normativo applicabile ai trattamenti di dati personali va pertanto analizzato alla luce del bilanciamento dei vari diritti tutelati dalla CDFUE e al netto di eventuali compressioni all'esercizio degli stessi diritti e libertà, che possono essere possibili solo se previsti da norme di legge. Nel rispetto del principio di proporzionalità, alcune leggi possono infatti apportare limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale, riconosciute dall'Unione, o all'esigenza di proteggere i diritti e le libertà altrui (art. 52 CDFUE). È

---

[3] Ricordiamo l'art. 8, § 1 della Carta dei diritti fondamentali dell'Unione Europea e l'art. 16, § 1 del Trattato sul funzionamento dell'Unione Europea (TFUE), che il regolamento UE 679/2016 richiama al Considerando 1.

[4] Art. 2 Cost., letto alla luce dei diritti contemplati nella CDFUE.

[5] Cfr. CGUE, 16 luglio 2020 su causa C-311/18 (*Schrems II*), in *curia.europa.eu/juris*, spec. § 172, che riprenderemo in seguito.

[6] Cfr. Considerando 4 GDPR.

[7] Previste rispettivamente queste ultime dagli art. 13 Cost., 6 CDFUE e 13 CDFUE.

questo ad esempio quanto avvenuto nel periodo dell'emergenza sanitaria dovuto alla pandemia da Covid-19.

L'Università statale italiana è una istituzione pubblica di alta cultura, i cui fini primari sono la ricerca scientifica, il trasferimento dei suoi risultati e la formazione superiore, obiettivi considerati tra loro inscindibili al fine di promuovere la valorizzazione delle conoscenze a vantaggio dei singoli e della società.

È dotata di autonomia didattica, scientifica, organizzativa, finanziaria e contabile[8] e, essendo intesa quale amministrazione pubblica[9], si applicano ad essa i princìpi e le norme previsti, per la Pubblica amministrazione, sia dalla Costituzione sia da tutte le disposizioni legislative, anche emanate in recepimento di normative o direttive europee, tra cui: le leggi finanziarie; le norme in materia di informatizzazione e digitalizzazione delle amministrazioni pubbliche; le norme in materia di riuso dei dati personali; le norme in materia di procedure amministrative e di diritto di accesso; la normativa in materia di trasparenza e anticorruzione; la normativa in materia di protezione dei dati personali; la normativa in materia di lavori pubblici, di appalti pubblici e forniture di beni e servizi; la normativa in materia di privativa industriale.

Il trattamento di dati personali, anche particolari, necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, può basarsi esclusivamente su una norma di legge o, nei casi previsti dalla legge, di regolamento[10].

Nel quadro normativo previgente all'entrata in vigore sia del GDPR sia del d.lgs. 101/2018, in base agli artt. 20 e 21 del d.lgs. 196/2003 (c.d. Codice Privacy) le PA potevano trattare i dati sensibili o giudiziari solo dotandosi di

---

[8] Art. 6, l. 168/89.

[9] Art. 1, 2° comma del d.lgs. 165/2001 e Costituzione italiana, Parte II, Titolo III, Sezione II («La Pubblica Amministrazione»).

[10] Artt. 6, § 3, 9, § 2 e 10 GDPR e artt. 2-*ter*, 2-*sexies*, 2-*septies* e 2-*octies* del d.lgs. 196/2003: l'interesse pubblico è utilizzabile anche da un soggetto privato, ad esempio concessionario o società in house di un ente pubblico o che svolge servizio pubblico, ma il focus del documento sarà specifico per l'università statale.

un atto di natura regolamentare adottato in conformità al parere espresso dall'Autorità Garante per la protezione dei dati personali. A novembre 2005, la Conferenza dei Rettori delle Università Italiane (CRUI) aveva ottenuto il necessario parere positivo del Garante sullo schema tipo di «Regolamento sul trattamento dei dati sensibili e giudiziari»[(11)]. Esso riporta numerose norme di legge, per ciascun ambito dell'attività di trattamento, che legittimano gli utilizzi dei dati ora definiti particolari e giudiziari, ancora utile per individuare la norma applicabile al loro utilizzo, nello specifico contesto dell'attività di trattamento.

La conoscenza del complesso delle norme europee e nazionali risulta quindi indispensabile per comprendere se l'attività di trattamento dei dati personali, che richiede il trasferimento degli stessi oltre i confini europei, nel perseguire una finalità istituzionale dell'Università rispetti il principio di liceità di cui all'art. 5, § 1, lett. *a)* GDPR. Mancando la base giuridica, verrebbe meno il presupposto giuridico, l'*an* dell'attività di trattamento e, nel caso comportasse il trasferimento dei dati personali all'estero, sarebbero invalide anche le condizioni di garanzia applicate al trasferimento, oggetto di questo studio.

L'Università pone in essere molteplici attività di trattamento nell'ambito delle attività istituzionali dell'Ateneo, anche diverse dalla didattica, ricerca e terza missione; si pensi ad esempio alle attività svolte per la gestione amministrativa dell'Università o per la tutela del suo patrimonio. Con particolare riguardo alle attività di ricerca e di didattica innovativa, ad esse strettamente correlate, nel contesto normativo occorrerà considerare anche l'art. 165 e il Titolo XIX del Trattato sul Funzionamento dell'Unione europea» («Ricerca e sviluppo tecnologico e spazio»), all'interno dei quali si collocano sia la realizzazione di uno spazio europeo di ricerca sia numerosi progetti dell'UE volti alla mobilità internazionale e non solo transfrontaliera[(12)]. Il

---

(11) Rinvenibile in *garanteprivacy.it/web/guest/home*.

(12) Anche il recentissimo programma Erasmus+ 2021-2027 dell'UE si pone, quale obiettivo generale «sostenere, attraverso l'apprendimento permanente, lo sviluppo formativo, professionale e personale degli individui nel campo dell'istruzione, della formazione, della gioventù e dello sport, in Europa e nel resto del mondo» (2021 Erasmus+ Guida al

loro scopo è favorire lo sviluppo della competitività europea, anche attraverso la «promozione della cooperazione in materia di ricerca, sviluppo tecnologico e dimostrazione dell'Unione con i paesi terzi e le organizzazioni internazionali»[13].

L'Università impronta la propria azione a principi di indipendenza, autonomia e responsabilità, riconoscendo la propria appartenenza allo Spazio europeo della ricerca e dell'istruzione superiore e garantendo, a sua volta, libertà di insegnamento e di ricerca scientifica ai professori universitari (cfr. Statuto Università di Perugia e di altri Atenei, in recepimento art. 7 d.P.R. 372/80 e art. 33 Cost.).

Il Capo III del GDPR («Diritti dell'interessato») pone infine bene in evidenza che il diritto alla protezione dei dati personali è inscindibile dal diritto all'autodeterminazione informata, diritto questo di rango inter-costituzionale in virtù degli artt. 2, 13 e 32 Cost. e degli artt. 1, 2 e 3 CDFUE.

3. — *Trasferimento dei dati personali. Quadro degli adempimenti.*

Da un primo confronto tra il Capo IV della direttiva 95/46/CE e il Capo V del GDPR, l'architettura delle norme sui trasferimenti internazionali sembra non subire modifiche rilevanti per gli Stati membri dell'UE[14].

---

programma – Obiettivi generali) evidenziando quanto la didattica e ricerca debbano ormai avere una dimensione internazionale.

[13] Art. 179, 2° comma e art. 180, lett. *b)* TFUE.

[14] Si v. sul punto, in aggiunta al GDPR: per la dottrina, E. Pelino, L. Bolognini, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. Rossi, *Il confine del futuro. Possiamo fidarci dell'intelligenza artificiale?*, Milano, 2019; con riferimento alla prassi, EDPB, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, in *edpb.europa.eu/our-work-tools*; Id., *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*, in *edpb.europa.eu/our-work-tools*; Id., *Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a), e paragrafo 3, lettera b), del regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e di paesi non appartenenti al SEE*, in *edpb.europa.eu/our-work-tools*; Id., *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, in *edpb.europa.eu/our-work-tools*; Comm. europea, *Comunicazione n. 43 del 24.1.2018*, in *eur-lex.euro-*

Ai fini delle garanzie da porre in essere, affinché con il trasferimento risultino impregiudicati i livelli di protezione delle persone fisiche, garantite nello spazio economico europeo, il GDPR ne chiarisce di certo meglio l'applicazione, formalizza e amplia il numero di strumenti di trasferimento possibili, come ad esempio le clausole contrattuali tipo e le norme vincolanti d'impresa.

Alcune Organizzazioni internazionali sono totalmente autonome e indipendenti nello scenario internazionale ed il loro operato non è riferibile ad alcuno Stato in particolare. Nel GDPR sono equiparate ai paesi terzi, così che il livello di tutela della protezione dei dati personali debba riguardare anche i trasferimenti verso di esse.

Estendendo poi lo sguardo sia all'ampliamento della portata territoriale della normativa, soprattutto per l'art. 3, §§ 1 e 2 GDPR, sia alle modifiche che, con il passaggio dalla direttiva al regolamento, sono state apportate alla normativa nazionale di recepimento della norma europea, l'entità del cambiamento risulta considerevole con riguardo ai trasferimenti, specialmente nelle restrizioni introdotte.

Osserviamo ad esempio che la direttiva abrogata riportava, al Considerando 20, la sola "opportunità" che, nel caso di trasferimenti verso un paese estero, «i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva».

La normativa italiana di recepimento della direttiva, che per l'appunto disciplinava i trattamenti dei dati (il d.lgs. 196/2003 ante riforma, introdotta poi dal d.lgs. 101/2018), all'art. 43 del Titolo VII («Trasferimento dei dati all'estero») legittimava tutte le deroghe previste all'art. 26 della direttiva, sen-

---

pa.eu; Gruppo WP29, *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995 del 25 novembre 2005 – WP114*, in *garanteprivacy.it/home*; Id., *Clausole contrattuali tipo - WP47*, in *garanteprivacy.it/web/guest/home*; CGUE, 6 ottobre 2015 su causa C-362/14 (*Schrems I*), in *eur-lex.europa.eu/legal-content*; CGUE, 6 novembre 2003 (*Lindqvist*), in *privacy.it/archivio*.

za alcuna limitazione rispetto la quantità dei dati trattati né la frequenza dei trasferimenti posta in essere[15].

Quelle stesse condizioni, ritenute nel nostro scenario nazionale applicabili sempre e in ogni ambito di attività, sono ora rinvenibili all'art. 49 GDPR quali deroghe cui è possibile ricorrere solo in situazioni eccezionali, in taluni casi solo con trasferimenti "occasionali e non ripetitivi", dovendosi ordinariamente individuare nelle altre garanzie, previste al Capo V del GDPR, le sole utilizzabili al fine di assicurare agli interessati quei diritti effettivi ed azionabili tutelati dal GDPR stesso.

Inoltre, l'individuazione della garanzia al trasferimento di dati, quale misura organizzativa di sicurezza, deve ora tener conto anche di quanto indicato all'art. 32 GDPR, ossia «della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche».

Abrogato l'art. 43 del Codice ad opera del d.lgs. 101/2018 di recepimento del GDPR, compete quindi ora esclusivamente al titolare o al responsabile del trattamento, in virtù dell'art. 44, § 1 e dell'*accountability* di cui all'art. 5, § 2 GDPR, la determinazione sia dei criteri di garanzia al trasferimento dei dati personali sia di come applicarli, affinché il livello di protezione delle persone fisiche garantito dal GDPR non venga pregiudicato.

È alla luce di queste rilevanti novità introdotte dal GDPR che analizzeremo insieme gli adempimenti da porre in essere per i trasferimenti extra UE, soggetti sempre al rispetto di almeno una delle condizioni di garanzia previste al Capo V del GDPR, con l'approfondimento di alcuni scenari specifici del contesto universitario.

Si riportano alcune definizioni relative a termini che saranno utilizzati nel seguito:

a) adeguatezza: nel caso dei trasferimenti, indica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione ma che tale paese assicuri ef-

[15] In effetti, il GDPR recepisce molte delle considerazioni del WP26, espresse nel citato WP114.

fettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri. Agli interessati dovrebbero inoltre essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale[16];

b) autorità di controllo: ai sensi dell'art. 51 GDPR, è l'autorità pubblica indipendente, istituita da uno Stato membro per controllare l'applicazione del GDPR, allo scopo di tutelare i diritti e le libertà fondamentali delle persone fisiche, con riguardo al trattamento dei dati personali, e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. L'autorità di controllo competente per l'Italia è l'Autorità Garante per la Protezione dei Dati Personali (c.d. Garante Privacy o GPDP, nel seguito semplicemente Garante);

c) comunicazione: è definita dal 4° comma dall'art. 2-*ter* del d.lgs. 196/2003 come il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

d) decisione di adeguatezza: è la decisione della Commissione Europea, assunta a valle di una valutazione dell'adeguatezza del livello di protezione dei dati, che un paese terzo, un territorio, uno o più settori all'interno di un territorio o un'organizzazione internazionale garantiscono un livello di protezione adeguato per il trattamento dei dati personali;

e) diffusione: è definita dal 4° comma dall'art. 2-*ter* del d.lgs. 196/2003 come il dare conoscenza dei dati personali a soggetti indeterminati, in

[16] V. Considerando 104 GDPR.

qualunque forma, anche mediante la loro messa a disposizione o consultazione;

f) EDPB (European Data Protection Board) o Comitato europeo per la protezione dati: è l'organismo dell'UE, individuato alla Sezione 3, artt. da 68 a 76 GDPR, composto dalla figura di vertice di un'autorità di controllo per ciascun stato membro e dal garante europeo della protezione dati (o rispettivi rappresentanti). Subentra al precedente Gruppo WP29 nel compito principale di garantire l'applicazione uniforme del GDPR negli stati a cui si applica (SEE). Nel seguito sarà riferito anche come "comitato";

g) esportatore: il titolare o il responsabile del trattamento *ex* art. 28 GDPR, che pone in essere il trasferimento dei dati personali verso un altro titolare, responsabile o destinatario in un paese estero;

h) organizzazione internazionale: ai sensi dell'art. 4, § 26 GDPR, è un'organizzazione o un organismo di diritto internazionale pubblico a essa subordinato o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati;

i) paese terzo: è uno Stato non appartenente all'UE o allo Spazio Economico Europeo, quest'ultimo comprendente anche la Norvegia, l'Islanda e il Liechtenstein. Nel seguito, verrà utilizzato, insieme a paese estero, per indicare un paese terzo o un'organizzazione internazionale;

j) registro: un documento (scritto, in formato cartaceo o elettronico) in cui sono annotati con regolarità determinati elementi o particolari, oppure un elenco ufficiale riportante una serie di nomi o elementi (Merriam Webster Dictionary, Oxford dictionary 2018);

k) registro delle attività di trattamento: è uno degli obblighi introdotto dal GDPR, all'art. 30, per documentare tutte le attività di trattamento svolte sotto la propria responsabilità, sia da parte del titolare che del Responsabile del trattamento;

l) responsabile: ai sensi dell'artt.4, § 8 e art. 28 GDPR, è la persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo che tratta i dati "per conto" del titolare del trattamento. Ad esempio un fornitore di servizi cloud per la memorizzazione di dati raccolti attraverso un progetto universitario è un responsabile dei trattamenti rispetto all'Università. L'U-

niversità può a volte essere responsabile di attività di trattamento svolte per conto di altri enti, ad esempio nell'ambito di attività conto terzi o progetti di ricerca;

m) titolare: è la persona fisica o giuridica (nelle molteplici forme elencate all'art. 4, § 7 GDPR) che determina le finalità e i mezzi del trattamento di dati personali. L'Università lo è per tutte le attività di trattamento che effettua nell'ambito delle sue finalità istituzionali e, in quanto tale, assume in sé tutte le responsabilità relative alla loro conformità alla normativa sulla protezione dei dati personali;

o) trasferimento: è una forma di trattamento, posto in essere se i dati personali trattati dal Titolare, soggetto alle disposizioni del GDPR, sono oggetto di un qualsiasi trattamento in un paese terzo o sono destinati ad esserlo dopo il trasferimento verso un altro titolare, responsabile o destinatario stabilito fuori dell'ambito di applicazione del GDPR. Un ulteriore chiarimento del termine è riportato nel seguito;

p) trasferimento occasionale e non ripetitivo[17]: si configurano tali quei trasferimenti che: *i.* possono ripetersi ma: solo in circostanze non ordinarie *e* ad intervalli di tempo arbitrari; *ii.* sono conseguenti al manifestarsi di condizioni casuali o ignote e pertanto non hanno sicuramente cadenza regolare;

q) trattamento: è definito dall'art. 4, § 2 GDPR come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Notiamo che il GDPR non fornisce direttamente la nozione di trasferimento, che è inserito tra i trattamenti quale «forma di comunicazione tra-

[17] Cfr. EDPB, *Linee guida 2/2018 EDPB sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, cit., p. 4.

mite trasmissione»[18], considerando inoltre trasferimento «anche l'accesso remoto da parte di un'entità di un paese terzo a dati situati nel SEE»[19].

Nel caso Lindqvist la Corte fu chiamata a stabilire, tra altri questioni, se l'inserimento su una pagina internet di dati personali costituisse trasferimento di dati verso un paese terzo, per il solo fatto di rendere tali dati accessibili a persone che si trovano in paesi terzi.

Essa concluse che l'inserimento di dati personali in una pagina web di un fornitore di servizi (web provider) stabilito in uno Stato membro, effettuato da parte di una persona che si trova in uno Stato membro, non costituisce trasferimento di dati personali ai sensi dell'art. 44 GDPR. La formulazione data induceva già a ritenere che si configurasse un trasferimento di dati nell'ipotesi in cui il fornitore fosse stabilito invece in un paese terzo, come poi è stato recentemente confermato dal EDPB, essendoci un trasferimento dei dati dall'UE e un trattamento svolto extra UE per la gestione degli stessi dati da parte del *web provider*[20].

È poi ampliata temporalmente la protezione del dato nel caso di trasferimenti all'estero perché, secondo le previsioni all'art. 44, per configurarsi un trasferimento di dati verso paesi terzi non è necessario che essi vengano trattati contemporaneamente al trasferimento, essendo sufficiente che essi siano destinati ad un trattamento nella fase successiva al trasferimento o in eventuali trasferimenti, successivi al primo, verso un altro paese estero.

Alcune condizioni per il trasferimento, come si vedrà, possono essere utilizzate solo per quelli caratterizzabili come "occasionali" o "non ripetitivi"; a solo titolo d'esempio, non potranno considerarsi occasionali i trasferimenti di dati personali da un Titolare ad un importatore nell'ambito di un rapporto stabile, per esempio per la gestione di buste paga dei dipendenti, o quando l'importatore, situato extra UE, può accedere direttamente alla banca dati mediante un'interfaccia applicativa (qual è ad esempio un

---

[18] Cfr. sentenza *Schrems II*, cit.

[19] Cfr. 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*, cit., nt. 22.

[20] Per approfondimenti: *eur-lex.europa.eu/legal-content*.

programma accessibile via web tramite credenziali), indipendentemente da quante volte la utilizzi.

Le violazioni delle disposizioni sui trasferimenti extra UE, artt. da 44 a 49, sono annoverate tra quelle soggette alle sanzioni amministrative pecuniarie più elevate, previste all'art. 83, § 5 GDPR e comportano, fatti salvi i principi di proporzionalità, importi fino a € 20.000.000 e, nei casi di cui all'art. 167, 3° comma del d.lgs. 196/2003, da uno a tre anni di reclusione.

Ciò conferma ulteriormente la necessità di adottare, dopo un'attenta analisi degli scenari di rischio, le adeguate misure di garanzia al trasferimento dei dati.

Il trasferimento di dati personali, come ogni trattamento, deve innanzitutto essere conforme alle disposizioni generali della disciplina in materia di protezione dei dati personali. Occorre quindi verificare che il trasferimento sia effettivamente necessario e i dati trasferiti siano adeguati, pertinenti e non eccedenti in relazione alle finalità per le quali il trasferimento verrà effettuato. Inoltre il trattamento: *a)* deve essere eseguito nel pieno rispetto dei princìpi elencati all'art. 5 GDPR e, in generale, di tutte le disposizioni pertinenti alla specifica attività previste nel GDPR e nelle altre normative applicabili ai trattamenti di dati personali o atti di soft law; *b)* deve essere fondato su una base giuridica tra quelle previste all'art. 6, § 1 e, nel caso di dati particolari o giudiziari, all'art. 9, § 2 o all'art. 10 GDPR, ricordandosi sempre dell'esigenza della minimizzazione dei dati rispetto lo stretto necessario; *c)* deve essere inserito nel Registro delle attività di trattamento, riportando i paesi terzi o le organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati. In particolare, occorre riportare nel registro anche la descrizione delle garanzie attuate per il trasferimento, individuate sulla base della valutazione dei rischi inerenti il trasferimento; *d)* deve essere inserito nell'informativa per l'interessato, riportando quali siano i paesi terzi destinatari e le motivazioni per cui ha luogo il trasferimento. Deve inoltre essere riportata la valutazione del Titolare in merito alla scelta dello strumento di garanzia adottato, come riportato nel Registro di cui al punto precedente; *e)* deve essere attuato nel rispetto delle misure di sicurezza di cui all'art. 32 GDPR e sottoposto alla valutazione d'impatto di cui all'art. 35 GDPR,

qualora la valutazione del rischio evidenzi un rischio medio/alto o l'attività rientri in quelle per le quali la valutazione d'impatto è obbligatoria[21].

In assenza di una decisione di adeguatezza della Commissione Europea, sia la valutazione del rischio del trattamento che il titolare deve costantemente effettuare ai sensi dell'art. 24 GDPR[22], sia l'adeguatezza della tutela offerta da un paese terzo vanno considerate in funzione dell'ambito di applicazione, del contesto e delle finalità del trattamento, della natura dei dati personali, della quantità dei dati trasferiti, della modalità, della frequenza e durata del trasferimento, dei tempi di conservazione dei dati ed eventuali utilizzi per ulteriori finalità nonché di eventuali trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.

In relazione alle misure di sicurezza, ad esempio, come indicato sempre dall'EDPB, nel caso di trasferimenti di dati particolari potrebbero essere adottate ulteriori misure di garanzie che prevedano o specifichino meglio, tra le altre: eventuali restrizioni per l'accesso ai dati particolari (definendo profili differenziati di accesso, autenticazione a tre fattori, tracciamento degli accessi, etc.); limitazioni delle finalità di utilizzo dei dati; il divieto di trasferimento ulteriore dei dati; la formazione specifica del personale addetto ai trattamenti; l'adozione di algoritmi crittografici per la conservazione dei dati; misure supplementari per assicurare la disponibilità continuativa dei dati, ad esempio se sussistono motivi di cura della salute.

4. — *Condizioni di garanzia per il trasferimento.*

Fermo restando il rispetto degli adempimenti appena richiamati, il trasfe-

---

[21] Cfr. Garante Privacy, *Valutazione di impatto sulla protezione dei dati (DPIA)*, in *garanteprivacy.it/regolamentoue/dpia.*

[22] Il concetto di "misure adeguate per garantire ed essere in grado di dimostrare", di cui all'art. 24, implica che sia sempre svolta una valutazione dei rischi, diversamente non potendosi dimostrare l'adeguatezza delle misure adottate, contrariamente al principio dell'*accountability* che comporta la dimostrabilità di ogni scelta operata dal titolare.

rimento dei dati verso paesi extra UE è possibile se, e solo se, sussiste almeno una delle seguenti condizioni di garanzia di cui al Capo V del GDPR. Esse mirano da un lato ad escludere che il Titolare ricorra a trattamenti effettuati in paesi terzi per eludere la normativa UE, dall'altro a garantire la possibilità, per gli interessati, di esercitare i diritti previsti dal GDPR, potendo ricorrere con strumenti effettivi in sede giudiziaria qualora tali diritti siano violati.

Le elenchiamo brevemente, riprendendole rispettivamente dagli artt. 45, 46 e 47 GDPR, per descriverle più accuratamente nel seguito:

1) decisione di adeguatezza: la Commissione Europea può decidere che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione, garantiscono un adeguato livello di protezione dei dati personali. In presenza di tale decisione, il trasferimento dei dati è possibile senza altre autorizzazioni specifiche[23];

2) garanzie adeguate: qualora non vi sia decisione di adeguatezza, il trasferimento può essere effettuato in presenza di garanzie adeguate e in forza di condizioni per le quali gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Esse sono costituite alternativamente da: uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; le norme vincolanti d'impresa (BCR), conformemente all'art. 47 GDPR; le clausole contrattuali tipo o standard di protezione dei dati, adottate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, § 2 GDPR; le clausole contrattuali tipo o standard di protezione dei dati, adottate da un'Autorità di Controllo e approvate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, § 2 GDPR; un Codice di Condotta (CC) approvato a norma dell'art. 40 GDPR, unitamente all'impegno vincolante ed esecutivo, da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese terzo, importatore dei dati, di applicare le garanzie adeguate al trattamento dei dati, anche per quanto riguarda i diritti degli interessati; un Meccanismo di Certificazione (MC) approvato a norma dell'art. 42 GDPR, unitamente all'impegno, vincolante ed esigibile da parte del Titolare del trattamento o

[23] Sentenza *Schrems II*, cit., §§ 117 e 118.

del Responsabile del trattamento nel Paese terzo, di applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; (con l'autorizzazione dell'Autorità garante per la protezione dati personali) le Clausole Contrattuali tra il Titolare del trattamento o il Responsabile del trattamento e il Titolare del trattamento, il Responsabile del trattamento o il destinatario dei Dati Personali nel Paese terzo o nell'organizzazione internazionale; (con l'autorizzazione dell'Autorità garante per la protezione dati personali) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati; le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base alla precedente direttiva 95/46/CE, che restano valide fino a quando non vengono modificate, sostituite o revocate dalla medesima autorità di controllo (art. 46, § 5);

3) deroghe in specifiche situazioni: in mancanza di una delle precedenti condizioni di garanzia, è possibile trasferire i dati personali solo se si verifica una delle seguenti situazioni, vincolante per la legittimità del trasferimento. Queste deroghe sono da considerare residuali nel loro utilizzo rispetto quelle riportate in precedenza, in quanto potrebbero contravvenire al diritto dell'interessato di disporre di mezzi di ricorso effettivi e diritti azionabili in caso di violazione dei suoi dati.

Vedremo che non tutte possono essere utilizzate dall'Università, in quanto Pubblica amministrazione, mentre alcune richiedono la concomitante presenza di altri fattori.

4.1. – *Decisioni di adeguatezza.*

La decisione di adeguatezza è la prima tra le condizioni di garanzia utilizzabili e prima elencate. Deve però esistere in relazione al paese terzo di destinazione del trasferimento, essendo un atto di esecuzione della Commissione Europea.

Il concetto di adeguatezza è finalizzato a garantire che le misure di protezione adottate nel paese terzo o organizzazione internazionale siano sostanzialmente equivalenti a quelle poste in essere dal GDPR. In base all'art. 45,

§ 2 GDPR la Commissione deve valutare l'adeguatezza[24] di un paese, ai fini del trasferimento di dati personali, tenendo conto innanzitutto dello stato di diritto, del rispetto dei diritti umani e delle libertà fondamentali tutelate dalla CDFUE, della pertinente legislazione generale e settoriale, anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale, accesso delle autorità pubbliche ai dati personali e norme inerenti il trasferimento successivo dei dati personali verso un altro paese estero, osservate nel paese terzo o organizzazione internazionale. Devono inoltre dimostrare un'efficacia verificabile, il che dovrà necessariamente includere: *a)* la presenza di un impianto sanzionatorio adeguato per la loro eventuale violazione; *b)* la disponibilità per l'interessato di diritti azionabili e mezzi di ricorso effettivi, in sede amministrativa e giudiziaria, quali quelli garantiti nell'ambito territoriale di applicazione del GDPR; *c)* l'esistenza e l'effettivo funzionamento, nel paese terzo, di un'autorità di controllo indipendente e con poteri di esecuzione, per assistere e fornire assistenza agli interessati nell'esercizio dei loro diritti, in cooperazione con le autorità di controllo degli Stati membri.

La decisione di adeguatezza, adottata dalla Commissione europea secondo la procedura d'esame di cui all'art. 93, § 2 GDPR, ha come destinatari tutti gli Stati membri e, ai sensi dell'articolo 288, quarto comma, TFUE, ha per essi un carattere vincolante: si impone pertanto a tutti i loro organi, nella parte in cui produce l'effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo interessato da tale decisione[25]. Per questo motivo, un trasferimento dei dati personali verso un paese terzo, effettuato in base a siffatta condizione, non necessita di altra condizione di garanzia a tutela dei dati. In ogni caso, secondo la giurisprudenza costante della Corte, l'Unione

[24] Al fine di fornire orientamenti alla Commissione europea, in merito la valutazione del livello di tutela dei dati nei paesi terzi e organizzazioni internazionali, il gruppo WP29 ha elaborato il documento WP254 (rinvenibile in *ec.europa.eu/newsroom*) che aggiorna il precedente WP12, alla luce sia del passaggio dalla direttiva al regolamento sia della giurisprudenza della Corte di giustizia dell'Unione europea con riguardo alla c.d. sentenza *Schrems I*. Al cap. 3 descrive principi di contenuto e meccanismi di procedura/applicazione basilari.

[25] Cfr. *Schrems I*, cit., § 51 ss.: in tal caso anche i giudici devono astenersi dall'applicare le norme interne.

è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, con particolare riguardo ai Trattati, ai princìpi generali del diritto nonché ai diritti fondamentali: anche le decisioni della CE sono soggette a tale controllo[26] da parte della CGUE.

Secondo la novità introdotta dal GDPR, la decisione può essere revocata tramite un meccanismo di riesame periodico – almeno ogni 4 anni – tenendo conto degli sviluppi che in tali paesi potrebbero incidere sul funzionamento delle decisioni già adottate, modificando uno o più degli aspetti citati che devono essere presi in considerazione. La Corte di Giustizia dell'Ue è competente in via esclusiva a dichiarare l'invalidità di una decisione della Commissione[27], allo scopo di garantire la certezza del diritto mediante l'applicazione uniforme del diritto dell'Unione nei diversi Stati membri.

Ulteriore elemento di novità del GDPR, rispetto la precedente direttiva 95/46/CE, riguarda la possibilità che la decisione di adeguatezza della Commissione Europea (CE) possa essere adottata anche su un territorio o uno o più settori specifici all'interno di un paese estero e non necessariamente sull'interezza di questo.

Sono considerate equiparate a tali decisioni quelle adottate dalla Commissione in base all'art. 25, § 6 della direttiva 95/46/CE e che continuano ad essere valide fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata mediante atti di esecuzione, al pari delle decisioni adottate secondo le previsioni del GDPR.

In presenza di una decisione di adeguatezza validamente adottata, neanche l'Autorità garante può sospendere o vietare il trasferimento dei dati personali verso il paese oggetto della decisione o le aziende di quel paese che vi hanno aderito[28] (tutte le decisioni sono pubblicate sul sito della Commissione e del Garante per la protezione dati nazionale).

È opportuno prendere visione dell'atto di decisione relativo al paese di destinazione in quanto, per essere applicabile al trasferimento, potrebbe pre-

---

[26] Cfr. *Schrems I*, cit., § 60.

[27] Cfr. *Schrems I*, cit., § 61.

[28] Cfr. *Schrems II*, cit., § 156.

vedere delle condizioni cui l'importatore stesso deve aver aderito [29]. In assenza di una decisione di adeguatezza, l'esportatore deve procedere ad individuare quale garanzia deve applicare, di quelle all'art. 46 o se deve ricorrere, in via eccezionale, ad una deroga di cui all'art. 49 GDPR.

4.2. – *Le garanzie dell'art. 46 e la recente sentenza* Schrems II.

Prima di approfondire le ulteriori garanzie per il trasferimento previste dal GDPR, ci soffermiamo sulla sentenza C-311/18 della CGUE di luglio 2020, c.d. *Schrems II*, evidenziandone alcuni aspetti.

La decisione 2000/520 - *Safe Harbour*, della Commissione Europea, riguardava l'adeguatezza della protezione offerta dai principi dell'approdo sicuro agli interessati, con riguardo al trasferimento dei dati personali dall'allora Comunità Europea alle organizzazioni degli Stati Uniti che si conformavano ai principi in essa contenuti. Era stata invalidata ad ottobre 2015 dalla Corte di Giustizia UE (CGUE) con una sentenza detta "Schrems I", relativa ad un rinvio pregiudiziale proposto alla CGUE dalla High Court irlandese.

A seguito di tale sentenza, la Commissione Europea aveva adottato, nel luglio 2016, la decisione di esecuzione (UE) 2016/1250 - *Privacy Shield*, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy.

Nella recente sentenza del 16 luglio 2020, cosiddetta *Schrems II*, relativa ad un ulteriore domanda di pronuncia pregiudiziale propostale sempre dalla High Court irlandese, la CGUE ha dichiarato invalida anche questa, riportando una serie di considerazioni che risultano fondamentali per inquadrare una questione molto complessa come quella dei trasferimenti extra UE e non solo verso gli USA. Essa esplicita anche quali siano i criteri che devono guidare l'esportatore nella scelta delle garanzie da applicare, tra quelle previste all'art. 46, in assenza di una decisione di adeguatezza adottata sul paese terzo destinatario del trasferimento.

[29] Alla pagina *ec.europa.eu/info/law* è descritta la modalità con la quale l'UE determina se un paese terzo sia o meno adeguato.

Se da un lato, infatti, i flussi di dati personali verso e da paesi al di fuori dell'Unione, o da organizzazioni internazionali, sono necessari per la cooperazione internazionale e l'espansione del commercio, al quale guarda con particolare attenzione l'UE anche con la strategia del mercato unico digitale europeo, d'altro lato il livello di tutela delle persone fisiche assicurato nell'Unione dal GDPR non deve essere compromesso quando i dati sono trasferiti a importatori in paesi terzi, considerando anche i casi di eventuali trasferimenti successivi verso altri paesi esteri. Nel rispetto del principio di proporzionalità, le limitazioni ai diritti e alle libertà riconosciuti dalla Carta possono intervenire solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[30].

Una decisione di adeguatezza deve quindi assicurare che le persone, dopo che i loro dati sono stati trasferiti ad un paese terzo, continuino a godere dei diritti e delle libertà fondamentali che sono loro accordati in relazione al trattamento dei dati nell'Unione europea[31].

Nelle sentenze da poco citate, la Corte evidenzia che l'accesso indifferenziato e su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli Stati Uniti verso imprese aderenti ai princìpi del Privacy Shield, non consente di ritenere salva la continuità dei diritti dei cittadini europei, in materia di protezione dei dati personali, nel caso in cui l'invio dei dati avvenga sulla base di tale decisione.

Con la *Schrems I* le considerazioni della Corte erano state analoghe, seppur meno incisive e circostanziate, mentre nella *Schrems II* l'High Court irlandese aveva prodotto alla CGUE, a supporto della richiesta di rinvio pregiudiziale, numerosa documentazione sui programmi di sorveglianza USA, che le autorità statunitensi le avevano fornito nell'ambito del procedimento principale.

Da tali prove emerge chiaramente che l'accesso massivo dell'intelligence americana non si limita a quanto strettamente necessario per perseguire

---

[30] Cfr. *Schrems II*, cit., § 174.

[31] Gruppo WP29, *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995 del 25 novembre 2005 – WP114*, cit., p. 7.

l'obiettivo legittimo della sicurezza nazionale, pertanto è manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Carta dei diritti fondamentali dell'Unione europea. Esistono infatti programmi di sorveglianza – in particolare uno denominato UPSTREAM – che consentono alla National Security Agency l'intercettazione dei dati in transito verso gli Stati Uniti, mediante l'accesso ai cavi sottomarini posti sul fondale dell'Atlantico, nonché di raccogliere e conservare i dati prima che essi giungano negli Stati Uniti e possano essere soggetti a norme specifiche statunitensi[32].

Il parere della Corte è che, affinché le intercettazioni di comunicazioni elettroniche possano essere considerate conformi ai princìpi europei, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale, o della repressione della criminalità, e che esistono garanzie adeguate e verificabili per i cittadini UE[33].

La Corte chiarisce inoltre che gli strumenti dei quali un paese terzo si avvale, per assicurare un livello di protezione dei dati personali adeguato ai requisiti richiesti in UE, possono essere diversi da quelli attuati all'interno dell'Unione per garantire il rispetto del GDPR, ma devono rivelarsi concretamente efficaci nell' assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione, comprendendo la possibilità di un ricorso effettivo per gli interessati.

Su questo aspetto la Corte aggiunge che il Mediatore dello scudo (Ombudsman), figura indipendente dai servizi di intelligence e prevista dal *Privacy Shield*, al fine di creare un nuovo meccanismo di vigilanza sulle ingerenze delle autorità federali per motivi di sicurezza nazionale, seppur nominato in seno al Dipartimento di Stato, a livello di Sottosegretario, non è un organo giurisdizionale ai sensi dell'art. 47 della Carta. Inoltre le possibilità di ricorso, offerte dalla giurisprudenza statunitense anche ai cittadini stranieri, sono limitate. L'istanza di ricorso presentata è infatti irricevibile se non è in grado

[32] Cfr. *Schrems II*, cit., § 63.

[33] Cfr. *Schrems I*, cit., §§ 33 e 74, per quanto al cpv. successivo.

di dimostrare la propria legittimazione ad agire e le stesse possibilità di ricorso non contemplano alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi, il che limita di fatto l'accesso al giudice ordinario[34], in alcuni casi finanche agli stessi cittadini statunitensi.

Per questi, e anche altri motivi, non si può ritenere che il diritto statunitense garantisca ai cittadini dell'Unione un livello di protezione sostanzialmente equivalente a quello garantito nei territori UE né la possibilità di esercitare diritti effettivi e azionabili, in relazione a trattamenti di dati personali che violano i principi di cui all'art. 5 GDPR, tra cui la necessità e proporzionalità.

La recente sentenza *Schrems II* non solo quindi invalida la decisione *Privacy Shield* ma, nell'analisi puntuale che effettua, dimostra una portata ben più ampia che incide, come vedremo, anche su altre condizioni di garanzia. Difatti la questione può presentarsi, allo stesso modo, nei trasferimenti verso un qualsiasi altro paese terzo che abbia un ordinamento giuridico dal quale possano discendere le stesse considerazioni.

Un'altra delle questioni pregiudiziali sottoposte alla CGUE dalla High Court irlandese, chiedeva di chiarire quale dovesse essere il livello di protezione da ricercare e garantire ai dati personali, se essi venivano trasferiti verso un paese terzo utilizzando le clausole contrattuali tipo adottate dalla Commissione europea e non sulla base di una decisione di adeguatezza. In particolare si chiedeva di specificare sia se le clausole contrattuali standard potessero ritenersi ancora valide sia quali fossero i fattori da prendere in considerazione, con riguardo al paese terzo di destinazione, per valutare se il livello di protezione assicurato dall'utilizzo delle clausole soddisfacesse i requisiti richiesti dalla normativa applicabile ai trasferimenti e il rispetto dei diritti tutelati dalla CDFUE.

Per la Corte la risposta è già nel GDPR: i fattori da prendere in considerazione sono tutti quelli previsti all'art. 45, § 2 (elenco degli elementi utilizzati dalla CE per valutare l'adeguatezza del livello di protezione) e che ottemperano all'art. 46, §1. Gli interessati devono disporre di diritti aziona-

[34] Cfr. *Schrems II*, cit., § 45.

bili e mezzi di ricorso effettivi e, se del caso, l'importatore deve collaborare con l'esportatore, obbligandosi a fornire garanzie adeguate al trasferimento. Ciò comporta che anche l'adozione di altre condizioni di garanzia, quali le clausole contrattuali standard adottate dalla Commissione europea, di per sé non può dirsi invalida ma potrebbe da sola non risultare adeguata per taluni trasferimenti di dati.

Le clausole contrattuali tipo, adottate dalla Commissione, hanno infatti il solo scopo di uniformare le garanzie contrattuali che si applicano in tutti i paesi terzi ai titolari del trattamento e ai responsabili del trattamento stabiliti nell'Unione, ma non possono vincolare le autorità pubbliche di paesi terzi, poiché queste ultime non sono parti del contratto[35]. Da ciò l'esigenza di doverle eventualmente integrare con misure supplementari, per garantire il rispetto dell'art. 44 GDPR e come previsto al Considerando 109 GDPR.

Diversamente quindi dalla garanzia "all inclusive", fornita dall'esistenza di una decisione di adeguatezza valida nel territorio extra UE, in sua assenza compete esclusivamente agli *esportatori*, siano essi titolari o responsabili del trattamento, la valutazione del livello di protezione fornito da uno degli strumenti di trasferimento di cui all'art. 46 GDPR, tra cui le clausole contrattuali tipo, o la decisione di avvalersi di una delle deroghe di cui all'art. 49 GDPR.

All'esportatore di dati, titolare o responsabile, ente pubblico o privato che sia, compete inoltre la responsabilità di verificare, caso per caso, l'efficacia della garanzia al trasferimento dei dati, individuata come adeguata, o l'eventuale necessità di integrarla con condizioni aggiuntive, volte a compensare la carenza di garanzie nel paese terzo derivante, ad esempio, da una eccessiva ingerenza delle autorità pubbliche nei flussi di dati internazionali o da elementi rilevanti del sistema giuridico del paese terzo. Per la verifica, se lo ritiene necessario, può avvalersi dell'importatore dei dati.

Sempre in ottemperanza all'*accountability* di cui all'art. 5, § 2 GDPR, all'esportatore di dati compete infine il dovere di rispettare in modo attivo e continuo il diritto alla protezione dei dati degli interessati, attuando le misure

[35] Nel caso del *Privacy Shield*, la decisione di adeguatezza prevedeva che fosse applicabile ai trasferimenti con le imprese statunitensi che vi aderivano e non a tutti i trasferimenti verso gli USA.

giuridiche, tecniche e organizzative che ne garantiscano l'efficacia nel tempo. Egli deve essere in grado di comprovare questi sforzi agli interessati, al pubblico in generale e alle autorità di controllo in materia di protezione dei dati[36].

Di tutti questi elementi, riportati nella sentenza della CGUE, è indispensabile che si tenga conto tutte le volte che, in assenza di una decisione di adeguatezza, occorre individuare uno strumento di garanzia per il trasferimento dei dati extra UE.

L'EDPB ha deciso di esaminare la complessa questione risultante dalla sentenza della CGUE, per venire in aiuto degli esportatori nell'applicare il "principio della responsabilizzazione", nei casi in cui scelgano di avvalersi di uno degli strumenti tra quelli all'art. 46 GDPR per il trasferimento dei dati extra UE. Ha quindi adottato due documenti: le Linee guida 2/2020 sugli artt. 46, § 2, lett. *a)* e 46, § 3, lett. *b)* GDPR, per i trasferimenti di dati personali di cui può avvalersi l'esportatore qualora sia un'autorità o organismo pubblico, che intende trasferire i dati ad un'autorità o organismo pubblico extra UE, e le Raccomandazioni 01/2020 per tutti gli altri strumenti previsti all'art. 46 GDPR.

Entrambe rappresentano una guida per incoraggiare titolari e responsabili dei trattamenti nell'applicazione coerente del GDPR, quando non sia possibile ricorrere ad una decisione di adeguatezza al trasferimento internazionale dei dati.

Le «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» sono corredate da informazioni utili e da riferimenti a possibili fonti di informazione, oltre che da diversi esempi di misure supplementari che potrebbero integrare qualsiasi strumento di trasferimento, tra quelli dell'art. 46 GDPR cui si riferiscono.

Sono strutturate in sei passi e, pur costituendo una base di riferimento importante, la sensazione che si riceve dalla loro lettura è che rispetto ad un

---

[36] 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*, cit., § 3.

problema di disallineamento giuridico, dai quali consegue un minor livello di tutela dei diritti degli interessati, solo il rendere inintelligibili i dati attraverso opportune tecniche, quali ad esempio un'adeguata pseudonimizzazione o la crittografia con chiave nota solo all'esportatore, può costituire una giusta misura di tutela, tanto più doverosa quanto più manchi l'esigenza che i dati esportati debbano essere acceduti in chiaro dall'importatore (è il caso della conservazione dei dati per backup, ad esempio) o la quantità e tipologia dei dati la richieda.

Abbiamo visto che se il trasferimento dei dati personali avviene verso un paese terzo, per il quale la Commissione Europea non ha adottato una decisione di adeguatezza, l'esportatore, titolare o responsabile, può ricorrere ad una delle diverse garanzie previste come adeguate all'art. 46, eventualmente da integrare secondo quanto riportato al paragrafo precedente.

Vedremo che alcune di esse necessitano di autorizzazione specifica da parte di un'Autorità di controllo; le autorizzazioni che sono state rilasciate da uno Stato membro o dall'autorità di controllo in base all'art. 26, § 2 della direttiva 95/46/CE, continuano a rimanere valide fino a quando non saranno modificate, sostituite o abrogate dalla medesima autorità di controllo.

L'ultimo capoverso del Considerando 109 GDPR invita poi i Titolari del Trattamento e i Responsabili del Trattamento a fornire garanzie supplementari attraverso impegni contrattuali che integrino le Clausole tipo di protezione dati, quali quelle proposte dall'EDPB con le Raccomandazioni 01/2020. Allo stesso modo, i Codici di condotta (art. 40) e i Meccanismi di Certificazione (art. 42) costituiscono strumenti validi di garanzia, se accompagnati da un impegno vincolante ed esecutivo, assunto dalla parte stabilita nel paese extra UE, ad attuare garanzie adeguate rispetto ai principi di protezione dati e qualora prevedano sia sanzioni sia meccanismi effettivi di esercizio dei diritti da parte degli interessati. In taluni casi, l'esportatore potrebbe anche ricorrere a formule di attribuzione totale delle responsabilità a suo carico, anche ai fini di un eventuale risarcimento.

Prima di addentrarsi nei diversi strumenti dell'art. 46, è infine importante evidenziare che, qualora il trasferimento dei dati personali, da parte di un titolare o responsabile del trattamento in UE, sia disposto da sentenze di

un'autorità giurisdizionale o dalle decisioni di un'autorità amministrativa di un paese terzo, ai sensi dell'art.48 (e C115) del GDPR queste possono essere riconosciute o assumere un carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, fatti salvi gli altri presupposti al trasferimento di cui al capo V del GDPR. È questo il caso, ad esempio, dell'Accordo tra Unione europea e Stati Uniti in materia di estradizione del 25 giugno 2015 e di altri accordi presenti sulla pagina del Ministero della giustizia – Atti internazionali. Questo perché la presenza di un accordo internazionale (o anche di mutua collaborazione giudiziaria) in vigore tra lo Stato membro e il paese terzo fornisce una garanzia, da parte di questi, di tutela dei principi e dei diritti e delle libertà fondamentali dell'UE. Diversamente, la mera applicazione extraterritoriale di leggi, regolamenti e atti normativi del paese terzo potrebbe creare una situazione contraria al diritto della protezione dati personali applicato in UE, ostativa al trasferimento richiesto.

4.3. – *Trasferimenti di dati tra autorità e organismi pubblici.*

Quando i trasferimenti di dati personali avvengono tra autorità ed organismi pubblici dello Spazio Economico Europeo verso altre autorità pubbliche, organismi pubblici o organizzazioni internazionali con analoghi compiti o funzioni, stabiliti in Paesi terzi, i dati personali possono essere trasferiti, alternativamente, sulla base di: A. uno strumento giuridicamente vincolante e avente efficacia esecutiva [art. 46, § 2, lett. *a)*], quale un accordo amministrativo, di natura internazionale e di ambito bilaterale o multilaterale; B. disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati [art. 46, § 3, lett. *b)*], quali ad esempio i protocolli d'intesa. Queste necessitano di autorizzazione preventiva dell'autorità di controllo competente.

Come per le clausole contrattuali, anche in questo caso l'EDPB ha adottato le «Linee guida 2/2020 sull'art. 46, § 2, lett. *a)* e § 3, lett. *b)* del GDPR». Esse forniscono un'indicazione delle garanzie al trasferimento che entrambi gli strumenti devono attuare per essere valide, anche a seguito della senten-

za *Schrems II* della CGUE; costituiscono inoltre una check list di cui può avvalersi l'esportatore per la predisposizione di tali accordi amministrativi, qualora sia un'autorità o organismo pubblico che intende trasferire i dati ad un'autorità o organismo pubblico extra UE.

Le linee guida devono essere lette congiuntamente ad altri documenti del Comitato e rappresentano una valida bussola per orientare un'autorità o organismo pubblico, quando attua trasferimenti internazionali di dati con organismi pubblici nell'ambito di cooperazioni amministrative, ma anche didattiche o di ricerca.

Gli accordi internazionali stipulati tra soggetti pubblici europei e dei paesi esteri, di cui al punto A, per avere validità non devono incidere sul diritto dell'UE o sul GDPR ossia contraddirlo o limitarne la portata. Inoltre devono essere conclusi da autorità pubbliche o organismi pubblici, devono essere giuridicamente vincolanti e avere efficacia esecutiva sia nel paese estero sia nei territori dell'UE. Se si guarda agli accordi internazionali, dato l'iter di approvazione[37], sembra piuttosto difficile potersene avvalere da parte delle Università.

Lo scopo precipuo dell'accordo è quello di impegnare le parti al rispetto rigoroso della normativa in materia di protezione dei dati personali e di tutelare gli interessati garantendo diritti effettivi e azionabili. Pertanto, secondo una lettura meno rigorosa delle sopra citate Linee guida che, in termini di Data Protection Agreement (DPA) da sottoscrivere tra le parti, trattano allo stesso modo le due diverse tipologie, potrebbe essere sufficiente qualsiasi accordo vincolante tra le parti purché riporti al suo interno una DPA redatta secondo le indicazioni dell'EDPB.

Analogamente è possibile ricorrere a disposizioni specifiche di cui al punto B, da prevedere nei contratti di diritto amministrativo o in accordi amministrativi tra autorità o organismi pubblici, che sono considerate garanzie adeguate se (e solo se) comprendono diritti effettivi e azionabili per gli interessati. Un esempio può essere rappresentato dal Memorandum d'intesa

[37] Si veda, ad es., la circolare 4/2008 del Ministero degli esteri rinvenibile in *esteri.it/mae/resource*.

che, pur non essendo un vero e proprio contratto, è un documento giuridico che esprime una convergenza di interessi fra le parti, indicando una comune linea di azione prestabilita e comune per i diritti effettivi ed azionabili degli interessati.

In questo caso l'accordo che le prevede va subordinato ad autorizzazione dell'autorità garante [prevista nei suoi compiti e poteri, rispettivamente art. 57, § 3, lett. *r)* e art. 58, § 3, lett. *i)*] che deve comunicare tale decisione al EDPB perché possa emettere un parere, secondo il principio di coerenza di cui agli artt. 63 e 64, § 1, lett. *e)* GDPR.

La prima autorizzazione ai sensi dell'art. 46, § 3, lett. *b)*, è stata resa dal Garante il 23 maggio 2019 alla CONSOB, che l'ha richiesta per sottoscrivere un accordo amministrativo per il trasferimento di dati personali tra le autorità di vigilanza finanziaria dello Spazio economico europeo (SEE) e le autorità di vigilanza finanziaria al di fuori del SEE (doc. web n. 9119857).

Volendo prenderla come eventuale riferimento per la redazione di disposizioni, da inserire nell'accordo amministrativo e da sottoporre all'autorizzazione dell'autorità garante, occorre tener conto che è antecedente all'adozione delle Linee guida 2/2020 e pertanto va rivista alla luce delle indicazioni in esse contenute.

4.4. – *BCR o Norme vincolanti d'impresa. Clausole contrattuali tipo.*

Il requisito fondamentale per attingere a tale strumento è l'appartenenza della società "importatrice" ed "esportatrice" al medesimo gruppo societario (anche se situate in due paesi diversi). Anche su di esse gravano le conseguenze della sentenza *Schrems II* che non verranno approfondite, in quanto non sono applicabili in ambito universitario.

Le clausole contrattuali tipo sono accordi contrattuali sottoscritti da ambo le parti, solitamente allegati ai contratti di servizio. Esistono di tre livelli:

a) *Clausole tipo della Commissione Europea [Standard Contractual Clauses o SCC, art. 46, § 2, lett c)]*

Vengono adottate nella forma di decisione della Commissione europea,

secondo la procedura prevista dall'art. 93, § 2 GDPR (in precedenza, art. 25, § 4 della direttiva 95/46/CE). Ad oggi sono di due tipi: una per trasferimenti da un titolare ad un titolare situato extra UE, l'altra per trasferimenti da un titolare ad un responsabile extra UE, tutte reperibili sul sito dell'Autorità garante[38].

Le clausole-tipo solitamente riguardano solo gli aspetti inerenti la protezione dei dati, pertanto vengono incorporate in un contratto più generale di Data Transfer, non ammettono modifiche o correzioni e devono essere sottoscritte da tutte le parti. Vi si possono aggiungere clausole ulteriori purché non in conflitto, direttamente o indirettamente, con quanto in esse contenuto e approvato dalla Commissione europea. Le integrazioni possono ad esempio recepire le raccomandazioni dell'EDPB relativamente alle misure che integrano gli strumenti di trasferimento, di cui abbiamo in precedenza parlato e come consigliato al Considerando 109 GDPR.

Nonostante sia stata confermata dalla CGUE la validità delle SCC tra titolare e responsabile, nei ruoli rispettivamente di esportatore e importatore, adottate con decisione 2010/87/UE della Commissione e modificate dalla decisione di esecuzione UE 2016/2297, la Commissione ha ritenuto necessario predisporre un progetto di decisione per i trasferimenti extra UE, redatto alla luce sia del GDPR sia delle considerazioni della CGUE riportate nella sentenza *Schrems II*, dovendo assicurare che ai dati personali trasferiti sia concesso un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione.

Il progetto è stato sottoposto a consultazione a novembre 2020 e su di esso si sono espresse, con la «Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries»[39] l'EDPB e l'EDPS (Autorità con competenza limitata ai dati trattati dalle istituzioni, organi, uffici e agenzie dell'UE), sollevando alcune perplessità, esprimendo necessità di ulteriore chiarezza in alcuni contesti e fornendo talvolta indi-

[38] Cfr. Garante Privacy, *Trasferimento di dati personali all'estero*, in *garanteprivacy.it/temi/trasferimento-dati-estero*.

[39] Rinvenibile in *edpb.europa.eu/our-work-tools/our-documents*.

cazioni utili al completamento degli scenari che, stando a quanto proposto dalla CE, non appaiono contemplati.

Il progetto proposto è modulare e riguarda le SCC per i trasferimenti di dati personali verso Paesi terzi, coprendo anche i casi di trasferimento «da responsabile UE a titolare extra UE» e «da responsabile UE a responsabile extra UE», non trattati finora da alcuna delle decisioni della Commissione Europea, al fine di venire incontro alle aumentate esigenze derivanti dagli sviluppi dell'economia digitale. La modularità dovrebbe facilitare il compito degli esportatori nell'adattamento delle SCC alle particolarità del caso specifico e comprendono la possibilità che aderiscano al contratto più parti, sin da subito o inserendosi successivamente come esportatori o importatori, previo consenso dei contraenti originari.

Nel pieno rispetto delle condizioni di trasparenza nei confronti degli interessati, questi dovrebbero ricevere copia delle SCC ed essere informati di qualsiasi cambiamento avvenga sia nelle finalità del trattamento sia negli eventuali ulteriori o diversi destinatari dei dati. In tal modo verrebbero informati anche delle modalità di esercizio dei diritti e di indennizzo, che le SCC devono prevedere.

L'importatore deve collaborare con l'esportatore al fine di valutare se le leggi in vigore nel suo paese potrebbero impedirgli di conformarsi ai requisiti previsti dalle SCC; ha altresì la responsabilità di conservare ogni documentazione sulle attività di trattamento e di informare l'esportatore, tempestivamente, qualora non sia più in grado di rispettare le SCC, dando modo all'esportatore di interrompere il trasferimento o risolvere il contratto.

Quando saranno adottate, ci sarà un anno di tempo per passare alle nuove SCC da parte di chi avesse fatto ricorso alle versioni adottate in precedenza e da queste sostituite. In ogni caso, le raccomandazioni 01/2020 dell'EDPB, relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione, se del caso, andranno utilizzate congiuntamente alle nuove Standard Contractual Clauses.

b) *Clausole tipo adottate dalla autorità garante nazionale (novità)*

In base al Meccanismo di coerenza, previsto all'art.63 e all' art. 64.1 lett. *d)* GDPR, il Garante di uno stato membro può proporle come "decisione

di adozione" al Comitato europeo per la protezione dati (EDPB). La Commissione europea potrà adottarle secondo atti d'esecuzione, al fine di garantire un'omogenea applicazione della normativa all'interno di ciascuno stato membro e dell'UE. Potrà quindi utilizzarle un esportatore anche stabilito in uno stato membro diverso da quello dell'autorità proponente.

c) *Clausole contrattuali ad hoc tra le parti o* model clause

Questa condizione di garanzia esplicita un requisito precedentemente più vago e, nel caso in cui le *model clause* siano stipulate tra il titolare o responsabile (esportatore) e l'importatore (altro titolare, responsabile o semplice destinatario extra UE), impone che tali contratti, anche di natura privata, siano sottoposti all'autorità garante nazionale competente. Questa ha il compito di autorizzarne la validità (art. 57, § 1, lett. *r)* e art. 58, § 3, lett. *h)* e di comunicare tale decisione al EDPB perché possa emettere un parere, secondo il principio di coerenza di cui agli artt. 63 e 64, § 1, lett. *e)* GDPR[40].

4.5. – *Deroghe: consenso e necessità.*

I trasferimenti fondati su una deroga non necessitano di alcuna autorizzazione preventiva dell'autorità garante nazionale e presentano rischi maggiori per i diritti e le libertà degli interessati limitando, se non escludendo del tutto, la disponibilità di diritti azionabili e mezzi di ricorso effettivi agli interessati.

Quando i trasferimenti avvengono nell'ambito della normale attività o prassi commerciale, piuttosto che ricorrere alle deroghe devono essere messe in atto garanzie adeguate ai sensi dell'art. 46. Le deroghe non devono costituire una regola nei trasferimenti del Titolare, che deve interpretarle in maniera restrittiva e eccezionale, e può ricorrervi solo entro i limiti dello stretto necessario.

Le condizioni previste nelle deroghe sono, in alternativa: *a)* che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo

[40] Continuano ad essere valide le autorizzazioni nazionali emesse dal Garante, anche in conseguenza di decisioni di adeguatezza della Commissione adottate sulla precedente normativa, riportate all'indirizzo *garanteprivacy.it/home/provvedimenti-normativa.*

essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; *b)* che il trasferimento sia 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; *c)* che il trasferimento sia 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'Interessato; *d)* che il trasferimento sia necessario per importanti motivi di interesse pubblico; *e)* che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; *f)* che il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; *g)* che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri; *h)* se non è applicabile alcuna delle garanzie o deroghe precedenti, solo se (il trasferimento) non è ripetitivo, se riguarda un numero limitato di interessati e se è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'Interessato. Il titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione ha fornito garanzie adeguate relativamente alla protezione dei Dati Personali. In questo caso, il titolare del trattamento informa del trasferimento l'Autorità di Controllo e, in aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il titolare del trattamento informa l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti[41].

Ad esse si aggiunge la condizione prevista all'art. 28, § 3, lett. *a)*, per la

[41] Questa condizione rappresenta un'alternativa molto residuale rispetto le altre riportate ed è applicabile in condizioni particolari. Si nota che nelle linee guida EDPB sui trasferimenti tale condizione è riferita come condizione all'art. 49, § 1, 2° comma; nella versione italiana del GDPR la condizione è riportata dopo la lett. *g)* dello stesso paragrafo.

quale il Responsabile del trattamento può effettuare il trasferimento dei dati verso un paese terzo, pur non avendolo tra le istruzioni del Titolare, quando lo prevede il diritto dell'UE o dello Stato membro cui è soggetto. In tal caso ne informa il Titolare, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico

Con le Linee guida 2/2018 l'EDPB, basandosi sul documento WP114 del gruppo WP29, ha fornito una serie di orientamenti per l'applicazione del meccanismo delle deroghe ai trasferimenti verso paesi terzi o organizzazioni internazionali, tenendo conto del Considerando 111 GDPR e soprattutto ponendo la "necessità" del trasferimento dei dati per una determinata finalità, come presupposto di fondo per il ricorso alle deroghe, con la sola esclusione della prima, fondata sul consenso.

Per comprendere quando sia possibile il ricorso al consenso, che è una base giuridica prevista dal GDPR, è bene riferirsi alle Linee guida 5/2020 EDPB.

Le deroghe di cui all'art. 49, § 1, lett. da *b)* a *f)*, prima elencate, prevedono che «il trasferimento sia necessario». Tale condizione deve essere verificata mediante un test di necessità da parte del Titolare, volto ad evidenziare il nesso stretto e specifico tra i dati personali oggetto del trasferimento e le finalità del trattamento cui si vuole applicare la specifica deroga.

Il trasferimento può avvenire solo se le finalità sono necessarie, concrete e non presunte o possibili, e i dati strettamente pertinenti e necessari allo scopo. La necessità richiede che debba esserci uno stretto e sostanziale legame tra la persona interessata e le finalità per le quali il trasferimento viene ritenuto, appunto, necessario.

Ad esempio, non è necessario per l'esecuzione di un contratto di lavoro in UE che i dati siano trasferiti in territorio extra UE per la gestione della busta paga. In questo caso non è quindi possibile utilizzare la deroga 49, § 1, lett. *b)*, poiché il nesso tra la finalità del trasferimento e la sua necessità, ai fini del contratto di lavoro, non è diretto né oggettivo; può esserlo invece nel caso di un'agenzia di viaggio con riferimento ai trasferimenti ad alberghi o partner commerciali all'estero dei dati dei clienti, ai fini dell'organizzazione del viaggio da questi richiesto. In ogni caso la deroga non può applicarsi alla

trasmissione di informazioni non necessarie ai fini del trasferimento (dati eccedenti la finalità) o a trasferimenti con una finalità diversa dall'esecuzione del contratto, con riferimento sempre alla 49.1.b) dell'esempio[42].

Se quindi le deroghe si giustificano in quanto è necessario rendere compatibile, in talune situazioni, la tutela dei diritti fondamentali delle persone - attraverso la protezione dei dati personali - con la libera circolazione delle informazioni e persone a livello internazionale, il ricorso ad esse non può derogare al rispetto dei diritti fondamentali in quanto ciò ne comporterebbe una violazione.

Il gruppo di lavoro della Commissione europea, già nel 1998[43], riteneva che fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione siano comprese le seguenti: *a)* trasferimenti riguardanti le categorie particolari di dati; *b)* trasferimenti che comportano rischi di perdite finanziarie (ad esempio pagamenti con carta di credito attraverso Internet); *c)* trasferimenti che comportano rischi per la sicurezza personale; *d)* trasferimenti finalizzati all'adozione di una decisione particolarmente importante per la persona interessata (assunzioni, promozioni, concessione di un credito, ecc.); *e)* trasferimenti che rischiano di causare un grave imbarazzo a una persona o di lederne la reputazione; *f)* trasferimenti che possono condurre ad azioni specifiche che costituiscono un'ingerenza grave nella vita privata della persona; *g)* trasferimenti ripetuti che riguardano grandi volumi di dati (per es. dati su transazioni elaborati su reti di telecomunicazioni, Internet, etc.); *h)* trasferimenti che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti "cookies" di Internet), cui potrebbe oggi aggiungersi l'utilizzo diffuso di

---

[42] EDPB, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, cit., e Gruppo WP29, *Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995 del 25 novembre 2005 – WP114*, cit., § 2.2.

[43] Cfr. Comm. europea – Gruppo di lavoro "Tutela delle persone fisiche con riguardo al trattamento dei dati personali", *Trasferimento di dati personali verso paesi terzi: applicazione degli artt. 25 e 26 della direttiva europea sulla tutale dei dati – DG XV D/5025/98 WP12*, in *garanteprivacy.it*.

servizi in cloud anche per la gestione dei dati dei lavoratori o per lo scambio di dati per attività di lavoro e ricerca.

I rischi per i diritti e le libertà delle persone fisiche, di cui tenere conto, sono ulteriormente elencati ai considerando 75 e 76 del GDPR.

Come anticipato, non tutte le deroghe sono utilizzabili senza la contemporanea esistenza o assenza di altre condizioni. Per rappresentare gli scenari ammessi, viene riportata una schematizzazione delle condizioni di applicazione delle deroghe di cui all'art. 49, § 1. Si ribadisce che sono da considerare residuali nel loro utilizzo e che anche le deroghe non espressamente limitate ai trasferimenti "occasionali" e "non ripetitivi", devono essere interpretate come eccezionali rispetto alla regola[44].

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
a. Che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'Interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)		Consenso come base giuridica, che deve essere esplicito, informato e specifico, indicando i paesi di destinazione, i destinatari o le categorie di destinatari, i possibili rischi derivanti dall'assenza, nel paese terzo, di un'autorità di controllo e la possibilità che non siano previsti principi di legittimità del trattamento e diritti per l'interessato mancando un parere di adeguatezza.	Essendo possibile la revoca in qualsiasi momento non è utilizzabile per trasferimenti di lungo periodo, in termini di frequenza. Il consenso deve essere esplicito, dopo minuziosa informazione dei possibili rischi, nel pieno rispetto delle condizioni agli artt.4.11, 7, 13 e 14, dei C32, C33, C42 e C44 GDPR e delle linee guida sul consenso WP259 del WP29. La specificità impone che il consenso valga solo per quel trasferimento specifico di cui è informato e le circostanze del trasferimento non siano modificate dopo la prestazione del consenso.

[44] Cfr. EDPB, *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, cit.

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
b. che il trasferimento sia 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;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)	SI	Occasionalità del trasferimento e quale sia il nesso stretto e significativo tra il trasferimento dei dati, i dati trasferiti e le finalità del contratto.	Non utilizzabile per trasferimenti di dati aggiuntivi, non strettamente necessari per l'esecuzione del contratto o delle misure precontrattuali. Nel caso di trasferimenti ripetuti devono essere utilizzate le misure di garanzie art.46.
c. che il trasferimento sia 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'Interessato;	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3)	SI	Come per b)	Come per b)

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
d. che il trasferimento sia necessario per importanti motivi di interesse pubblico;	eccezione descritta ultimo capoverso 5.3 nel caso di richieste da paesi terzi, art.48, descritto nell'annotazione →		Occasionalità del trasferimento e quale sia il nesso stretto e significativo tra il trasferimento dei dati, i dati trasferiti e i motivi di interesse pubblico perseguiti.	Il requisito essenziale è nell'indicazione di necessità del trasferimento dei dati per un importante interesse pubblico, non nella natura dell'organizzazione che trasferisce o riceve i dati, che può essere anche privata (C111, C112) In continuità con l'art.26.1.d della direttiva 95/46/CE, l'art. 48 riporta che il trasferimento può avvenire solo qualora sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, deducibile dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, anche in virtù della reciprocità per la cooperazione internazionale sottoscritta tramite accordo o convenzione internazionale. Nel WP114 del 25 novembre 2015 il WP29 afferma che "questa deroga può essere utilizzata solo se il trasferimento è nell'interesse delle autorità stesse di uno Stato membro dell'Ue e non unicamente nell'interesse di una o più autorità di un paese terzo".

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
e. che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;		SI		Poiché il trasferimento deve essere effettuato nell'ambito del procedimento, è necessario un nesso stretto tra i dati trasferiti e il procedimento specifico relativo alla situazione in questione, non la mera possibilità che occorrano a tale scopo. I procedimenti devono avere un fondamento giuridico e possono includere la fase preprocessuale, l'apertura di un contenzioso o la richiesta di approvazione di una fusione. Nel diritto nazionale di alcuni Stati esistono i "blocking statutes" che impediscono o limitano i trasferimenti di dati personali verso autorità giudiziarie o talvolta organismi pubblici di paesi terzi. Occorrerebbe prima verificare se possano essere utilizzati dati anonimi o pseudonimizzati
f. che il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;	SOLO quando l'interessato è nell'incapacità fisica o giuridica di prestare il consenso			Se c'è capacità decisionale ed è possibile dare il consenso la deroga non è applicabile. Il trasferimento deve essere correlato all'interesse individuale dell'interessato o di un'altra persona e, nel caso di dati sanitari, deve essere necessario ai fini di una diagnosi essenziale. È esclusa p.e. la ricerca medica che produrrà risultati solo in futuro. Il grave rischio imminente deve essere superiore rispetto le preoccupazioni connesse alla protezione dei dati

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
g. che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri;	Non può riguardare la totalità dei dati né intere categorie di dati personali contenuti nel registro (non solo per la PA).			La deroga si applica a dati contenuti in registri aventi la finalità di trasmettere informazioni al pubblico, non ai registri privati. Si tratta di registri che possono essere consultati dal pubblico, in generale, o da chiunque sia in grado di dimostrare un legittimo interesse (registri delle imprese, di condanne penali o casellario giudiziale, registri catastali, pubblici registri automobilistici, …). Se il registro è costituito per legge per essere consultato da persone che hanno un legittimo interesse, il trasferimento può avvenire su loro richiesta o se ne sono destinatarie (quindi non tramite pubblicazione *erga omnes*), tenendo conto degli interessi e dei diritti fondamentali dell'interessato.

Deroghe art. 49 GDPR	Eccezioni per la PA	Solo se occasionali?	Cosa aggiungere nell'informativa o al Registro dei trattamenti	Riferimenti e annotazioni
h. se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'Interessato; il titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei Dati Personali. Il titolare del trattamento informa del trasferimento l'Autorità di Controllo. In aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il titolare del trattamento informa l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti.	Non utilizzabile nell'esercizio di pubblici poteri (art.49.3) (è la condizione dal secondo capoverso lett. g, che nel testo originale del GDPR è il secondo comma §1)	SI	Il titolare deve informare l'interessato. Vanno descritti i legittimi interessi cogenti e i seri motivi per i quali non è stato possibile tutelare il trasferimento con garanzie adeguate o alcuna delle altre deroghe previste, inserendo i paesi destinatari. Devono essere indicate nel Registro dei trattamenti sia la valutazione delle circostanze relative al trasferimento sia le garanzie adeguate fornite a seguito della valutazione.	È prevista come extrema ratio, applicabile solo nel caso in cui non è possibile basare il trasferimento su una disposizione art. 45 o 46 né su alcuna delle deroghe sopra elencate; ai sensi del C113, deve riguardare un numero limitato di interessati ed è subordinato alla concomitante sussistenza delle condizioni espressamente elencate nell'intero capoverso riportato dopo la lett. g) § 1 art. 49. L'interesse legittimo deve essere cogente poiché non vi rientrano tutti i possibili interessi di cui all'art.6, § 1.f); deve esserne informato il GDPD

Particolare importanza riveste l'informativa dovuta all'interessato che, ancor più nel ricorso ad una deroga, dovrà riportare i possibili rischi derivanti dal trasferimento dei dati verso un paese che non fornisce una protezione adeguata ed effettuato in assenza di misure di salvaguardia per la protezione dei dati e l'esercizio dei diritti.

Nelle FAQ del Garante Privacy, relative alle conseguenze sui trasferimenti extra UE derivanti dalla sentenza *Schrems II* (v. § 4.2), si conferma l'utilizzabilità delle deroghe purché siano rispettate tutte le condizioni di cui all'art. 49, da interpretare in maniera restrittiva.

Nel caso del ricorso alla deroga «per importanti motivi di interesse pubblico», che devono essere riconosciuti nella legislazione UE o dello Stato membro, il requisito essenziale è che il trasferimento sia fondato su tali importanti motivi, non che sia deducibile dalla natura del soggetto coinvolto nel trasferimento. Inoltre, sebbene tale deroga non sia limitata ai trasferimenti di dati aventi natura "occasionale", ciò non significa che i trasferimenti di dati sulla base della deroga per importanti motivi di interesse pubblico possano configurarsi su larga scala e in modo sistematico.

Resta fermo che le deroghe previste all'art. 49 non dovrebbero mai trasformarsi di fatto in una regola, essendo limitate a situazioni specifiche e condizionate ad un rigoroso test di necessità.

Il § 5 dell'art. 49 pone infine una deroga alle deroghe, lasciando possibilità all'Unione o agli Stati membri, in assenza di una decisione di adeguatezza, di fissare limiti al trasferimento di categorie specifiche di dati verso paesi esteri per importanti motivi di interesse pubblico, notificandolo alla Commissione.

5. — *Brexit.*

A partire dal 1° gennaio 2021 il Regno Unito è un Paese terzo rispetto l'Unione europea.

L'accordo commerciale raggiunto tra le parti prevede un periodo transitorio, che si estende fino a tutto giugno 2021, durante il quale il trasferimento di dati tra paesi UE e Regno Unito non sarà considerato verso un paese

terzo. Potranno quindi essere applicate, al trasferimento, le stesse condizioni di garanzia utilizzate fino al 31 dicembre 2020, a condizione che rimanga in vigore negli UK l'attuale regime di protezione dei dati personali che ha nell'Information Commissioner's Office (ICO) il suo organismo di vigilanza indipendente.

Se entro tale periodo la Commissione europea, impegnata a lavorare con il governo inglese, non riuscirà ad adottare una decisione di adeguatezza, tutti i trasferimenti potranno essere effettuati solo in presenza di garanzie adeguate, di cui agli artt. 46, 47 o 49, ferme restando tutte le valutazioni finora riportate in relazione alla loro utilizzabilità.

La Commissione europea ha in effetti pubblicato, il 19 febbraio 2021, la bozza della decisione di adeguatezza sulla protezione dei dati personali relativa al Regno Unito, su cui l'EDPB, con l'Opinion 14/2021, ha espresso parere favorevole; dovrà ora essere approvata secondo l'iter previsto dal GDPR. Una volta completata questa procedura, la Commissione europea potrà adottare definitivamente e ufficialmente la decisione di adeguatezza a favore del Regno Unito.

È necessario che ogni titolare individui già da ora quali siano i trattamenti effettuati che richiedono trasferimenti di dati verso gli UK, provvedendo quanto prima ad aggiornare i documenti interni (p.e. Registro dei trattamenti, nel quale va indicato se l'attività comporta trasferimenti extra UE) e ad integrare le informative relative a tali attività di trattamento in quanto, indipendentemente dalle condizioni di garanzia che potranno essere adottate dopo il 31 giugno, i trasferimenti verso gli UK sono già, a tutti gli effetti, trasferimenti extra UE.

Nel censire tali trasferimenti, il titolare dovrà tenere conto anche di servizi realizzati su server collocati in territori nazionali o europei, cui il fornitore di servizi (o il partner della ricerca) può accedere dal Regno Unito, considerando che le considerazioni della CGUE nella sentenza *Schrems II* fanno sì che anche tali trattamenti debbano essere annoverati nei trasferimenti di dati extra UE. Un riguardo particolare andrà in tali casi dato all'*access right*, affinché sia limitato ai soli diritti necessari all'erogazione del servizio e ai soli dati strettamente necessari a fornirlo.

Si rimanda al sito del Garante Privacy per ogni ulteriore approfondimento[45].

6. — *Il programma Erasmus+*.

Il programma Erasmus+ è istituito con regolamento (UE) 1288/2013 del Parlamento Europeo e del Consiglio dell'11 dicembre 2013, quale programma dell'Unione per l'istruzione, la formazione, la gioventù e lo sport. Esso subentra al precedente programma Erasmus, partito 27 anni prima, recependone l'esperienza positiva al fine di contribuire ancor più al conseguimento di vari obiettivi, compresi quelli in materia di istruzione, formazione e promozione dei valori europei, attraverso molteplici "azioni chiave" del programma europeo. Tra queste ultime, alcune sono volte a sostenere la mobilità degli studenti e del personale per esperienze di apprendimento e/o professionali in altri paesi, anche tramite partenariati strategici transnazionali e internazionali.

Nell'ambito del programma Erasmus+, gli accordi di mobilità possono essere stipulati anche con atenei collocati in paesi terzi per: *a)* scambio di visite di docenti e ricercatori impegnati nell'attività di ricerca o organizzazione congiunta d'incontri, seminari, corsi di formazione e attività di docenza; *b)* scambio di dottorandi, dottori di ricerca, assegnisti di ricerca e giovani ricercatori; *c)* scambio di studenti; *d)* altre forme di cooperazione: progetti comuni di ricerca, sostegno all'avvio di una struttura di ricerca o progetti di sviluppo, tirocini curricolari ed extracurricolari, etc.

Tali accordi possono avere la forma di "accordi quadro" all'interno dei quali stipulare, di volta in volta, accordi inerenti una delle specifiche situazioni tra quelle appena citate. In ogni caso, prevedono la stipula di convenzioni tra gli enti partecipanti, successivamente alla sottoscrizione degli accordi contrattuali richiesti ai partner dall'UE per la partecipazione al bando.

Venendo alle finalità di approfondimento del trasferimento dei dati, i trat-

[45] Cfr. Garante Privacy, *Trasferimento di dati personali all'estero*, cit.

tamenti sono effettuati ai sensi dell'art. 6, lett. *e)* GDPR ossia «il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» e ai sensi dell'art. 6, lett. *c)*. Difatti il programma Erasmus+ è definito nell'ambito dei pilastri UE, è approvato dal Parlamento europeo e l'Ateneo deve veder approvata la sua candidatura alla partecipazione al programma per poter attivare i bandi a livello locale, nell'ambito delle finalità istituzionali universitarie. L'adesione al programma Erasmus+ comporta notevoli obblighi a carico dell'Ateneo, tra cui quelli per il controllo dei finanziamenti UE.

La responsabilità ultima del regolare funzionamento del Programma Erasmus+ spetta infatti alla Commissione europea, che ne gestisce il bilancio e ne stabilisce costantemente priorità, obiettivi e criteri. Il programma ha un'estensione pluriennale di circa 7 anni e da poco è stato approvato il programma Erasmus+ 2021-2027.

A livello europeo, l'Agenzia esecutiva per l'istruzione, gli audiovisivi e la cultura (Agenzia esecutiva) è responsabile, in particolare, dell'attuazione delle azioni centralizzate del Programma Erasmus+. Molte altre azioni sono decentrate e, in particolare, la Commissione europea affida le funzioni di esecuzione del bilancio alle Agenzie nazionali: per l'Italia, è l'Agenzia Indire.

Le Agenzie nazionali promuovono e realizzano il Programma a livello nazionale e fungono da tramite tra la Commissione europea e le organizzazioni partecipanti a livello locale, regionale e nazionale. Di norma, i partecipanti ai progetti Erasmus+ devono risiedere in uno dei paesi aderenti al Programma, tra cui ci sono anche paesi esterni all'UE.

I trattamenti dei dati dei candidati al programma avvengono quindi da parte di molti titolari: gli Atenei, l'Agenzia nazionale e quella esecutiva[46].

[46] L'indirizzo riporta il riferimento al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, ora sostituito dal regolamento UE 1725/2018. I trattamenti svolti da questi ultimi sono descritti all'indirizzo *ec.europa.eu/programmes/erasmus-plus/programme-guide* e integrano i trattamenti dei dati effettuati dall'ateneo, per i quali è dovuta dagli stessi atenei l'informativa al momento della candidatura dello studente. Per la trasparenza, i successivi trattamenti andrebbero almeno citati, riportando i riferimenti delle ulteriori informative.

Come avviene per altre tipologie di contratti o convenzioni, l'individuazione degli Atenei che sottoscrivono la convenzione come Titolari autonomi, o Contitolari, dipende dall'impostazione data circa le finalità e modalità dei trattamenti che sono oggetto dell'accordo.

Il nuovo bando Erasmus+ è il primo successivo all'entrata in vigore del GDPR. Nel pieno rispetto di quei principi del regolamento (e non più direttiva) sulla protezione dati e dei meccanismi di coerenza previsti dal regolamento stesso, è plausibile che lo stesso programma Erasmus+ debba indicare quali siano gli impegni che gli enti partner extra UE debbano sottoscrivere, all'atto dell'adesione al programma, per l'applicazione delle garanzie al trasferimento dei dati dei cittadini UE che partecipano ai bandi di mobilità (siano essi studenti, docenti o personale tecnico amministrativo delle istituzioni scolastiche e universitarie). Se ciascun ente partner UE dovesse provvedere in proprio, si creerebbe in UE una disparità di trattamento dei dati, e quindi dei diritti, dei circa quattro milioni di partecipanti al programma dei diversi stati membri, in contrasto con lo scopo perseguito con il GDPR, espresso in particolare al Considerando 10.

Si attende quindi nei mesi di giugno e luglio 2021 la pubblicazione degli *agreement* che dovranno essere sottoscritti tra i partner UE ed extra UE al fine di assicurare, ai trasferimenti dei dati personali, un livello di protezione adeguato e uniforme per tutti i trasferimenti dei dati personali dai vari stati membri.

È ipotizzabile che, salvo l'esistenza di una decisione di adeguatezza adottata e applicabile all'ente ospitante, occorra seguire una delle seguenti strade:

a) aggiungere all'accordo la sottoscrizione di una clausola contrattuale tipo (SCC) adottata in base alla Decisione della Commissione europea. Come indicato nella sezione dedicata alle SCC, si attende che la CE adotti il progetto di decisione modulare delle clausole, recependo le indicazioni della "joint opinion" del EDPB ed EDPS. Nel frattempo, può essere adottata, ad esempio quella del 27 dicembre 2004 (2004/915/CE)[47] – che modifica

[47] Il documento che riporta in allegato la clausola, composta da tre elementi, è rinvenibile in *eur-lex.europa.eu*.

la decisione 2001/497/CE – per il trasferimento di dati personali a titolare stabilito in un paese terzo. Essendo state adottate prima dell'entrata in vigore del GDPR, occorre intervenire nella terminologia (Titolare al posto di Responsabile, dati particolari anzichè dati sensibili…) oltre a integrarle con quanto necessario per l'applicazione al caso concreto, seguendo le indicazioni delle Raccomandazioni 01/2020 prima citate, senza intervenire su di esse in modalità incompatibile con il contenuto delle SCC. Può essere utilizzata anche la clausola contrattuale adottata con decisione 2001/497/CE, che è stata modificata e affiancata, ma non sostituita, da quelle proposte in nota;

b) utilizzare la base di garanzia prevista all'art. 46, § 3, lett. *b)*, ossia "disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli Interessati", che possono essere predisposte dall'Ateneo ma devono essere sottoposte all'autorizzazione preventiva del Garante;

c) in termini di "*accountability*", è possibile il ricorso alla deroga di cui all'art. 49, § 1, lett. *d)* "trasferimento necessario per importanti motivi di interesse pubblico", da ritenersi comunque come eccezione alla regola, secondo quanto già riportato in precedenza. Il trasferimento supera il test di necessità, per i soli dati personali comuni necessari e sufficienti a consentire alla persona interessata di svolgere l'attività presso la sede richiesta con la sua candidatura al bando e di essere rimborsata delle spese, nelle modalità previste sempre dal bando. Lo scopo del trasferimento rientra negli importanti motivi di interesse pubblico del programma Erasmus+[(48)] riconosciuti dall'Unione Europea, e anche nelle finalità istituzionali dell'Ateneo, che si candida al programma per ricevere i finanziamenti per le borse da assegnare ai candidati vincitori dei bandi. In considerazione della partecipazione volontaria dei candidati ai diversi bandi di mobilità, in taluni casi verso organizzazioni internazionali anche segnalate direttamente dai potenziali candidati (per esempio la Croce Rossa internazionale) nel bilanciamento dei diritti è possibile tenere conto di quelli dell'interessato, di fruire di un'opportunità didattica e esperienziale diversa la cui importanza è riconosciuta a livello

[(48)] Per approfondimenti sul punto, si v. la pagina *ec.europa.eu/programmes/erasmus-plus*.

UE, chiaramente espressi con la domanda di partecipazione.

In una prima ipotesi appariva possibile anche il ricorso al consenso dell'interessato che, alla luce degli approfondimenti condotti, si ritiene difficilmente applicabile al caso. Difatti l'Università aderisce al programma Erasmus+ contribuendo spesso alla copertura delle spese, anche se in misura diversa tra gli atenei, per consentire agli studenti, e al personale che vi partecipa, lo svolgimento di attività che siano attinenti o al percorso formativo dello studente, per il riconoscimento dei crediti formativi, o all'ambito didattico/lavorativo di coloro in ateneo che chiedono di parteciparvi. Le motivazioni sono sempre quindi nel campo della formazione e didattica di qualità, miglioramento delle esperienze interpersonali volte all'apprendimento di culture e lingue diverse, meglio esplicitati nell'abbondante documentazione UE su tali programmi, in ogni caso ritenute di rilevante interesse pubblico e rientranti nelle finalità istituzionali universitarie. Anche la domanda di candidatura al bando, effettuata volontariamente da parte degli studenti e del personale di ateneo, in base allo specifico loro diritto, comporta che l'Università ponga in essere ogni attività necessaria per rispondere alla richiesta dell'interessato, nell'esercizio delle sue funzioni istituzionali.

In base all'art. 49, § 3, si esclude quindi la possibilità di ricorso al consenso (che inoltre sappiamo non essere quasi mai ritenuta la corretta base giuridica, per i dipendenti del titolare).

Resta l'obbligo, oltre quanto già rappresentato nel paragrafo sulle deroghe, di dare ampia informativa all'interessato sui rischi potenziali che possono derivare dal trasferimento dei suoi dati, che saranno solo quelli necessari e non eccedenti rispetto lo scopo per cui devono essere comunicati, al fine di dare attuazione alla sua richiesta. Come già accennato, l'informativa dovrà contenere anche le informazioni sui trattamenti dei dati personali sui trattamenti svolti dall'Agenzia nazionale e dagli organismi UE preposti al monitoraggio del programma, reperibili ai link prima richiamati.

In taluni casi, sarebbe opportuno evidenziare agli interessati anche i potenziali rischi derivanti dalle attività di trattamento che loro potrebbero porre in essere autonomamente, una volta giunti alla destinazione richiesta.

7. — *Accordi internazionali di cooperazione universitari.*

Le Università stipulano accordi di mobilità internazionale con diversi partner extra UE, tra cui università pubbliche e private, enti di ricerca, industrie e ospedali, al fine di favorire il maturarsi di quelle esperienze che sono essenziali in un mercato sempre più globale, agevolando il confronto di studenti, docenti e personale universitario con culture e contesti diversi, attraverso esperienze di studio e di lavoro all'estero, finalità ritenute di interesse pubblico rilevante, riconosciute tali anche dall'Unione Europea attraverso le azioni chiave di vari programmi.

Le stipule degli accordi sono disciplinati da linee guida o regolamenti universitari, redatti secondo le previsioni normative e statutarie del singolo Ateneo. Gli accordi possono essere strutturati in due livelli, con un accordo quadro di primo livello tra l'università e l'ente partner, anche di natura pluriennale, che comprende i vari obiettivi raggiungibili attraverso successivi protocolli attuativi o accordi specifici di collaborazione, di secondo livello, anch'essi soggetti ad ulteriore approvazione da parte degli organi universitari.

Come per l'Erasmus, nell'ambito degli accordi internazionali l'oggetto del trasferimento sono le persone più che i dati. I dati personali sono quasi sempre i pochi necessari perché chi partecipa all'accordo possa essere riconosciuto e accolto all'arrivo dall'ente partner, essere avviato all'attività oggetto dell'accordo ed ottenere il rimborso spese, se previsto. In diverse occasioni i protocolli attuativi o gli accordi internazionali con istituzioni extra UE sono proposti dagli stessi docenti che intendono aderirvi, qualora approvati dagli organi di ateneo, al fine di perseguire attività didattiche, di ricerca o divulgative con colleghi già conosciuti in altri contesti e che svolgono la loro attività presso il partner proposto. Ciò non toglie che vi sia comunque un trasferimento di dati personali verso paesi esteri e corra l'obbligo di rispettare il GDPR, secondo le modalità finora esaminate.

In presenza di un accordo quadro sottoscritto con l'Ente partner, privato o pubblico che sia, è difficile inquadrare come non ripetitivo o occasionale il trasferimento. Se da un lato in nessuna documentazione consultata c'è una

definizione di "occasionale", è però evidenziato che per i trasferimenti "a regime", come appaiono quelli previsti da un accordo, e in assenza di una decisione di adeguatezza applicabile, andrebbe individuata una garanzia di cui all'art. 46 e non una deroga. Solitamente lo stesso soggetto potrà parteciparvi circa una volta l'anno per lo stesso, e potrà riproporsi secondo la durata dell'accordo quadro; la numerosità degli accordi stipulati da uno stesso ateneo spesso supera il centinaio, in atenei di grandi dimensioni anche varie centinaia, con partner di tutto il mondo.

In assenza di una decisione di adeguatezza la regola richiederebbe il ricorso alle SCC, anche integrate sulla base delle raccomandazioni 01/2020 EDPB, o il ricorso alle garanzie di cui agli artt. 46, § 2, lett. *a)* e 46, § 3, lett. *b)*, quest'ultima utilizzabile nel caso di accordi tra autorità o organismi pubblici, previa approvazione del garante.

L'attività di trattamento è senz'altro necessaria per conseguire un importante interesse pubblico, spesso richiesto dallo stesso interessato e talvolta richiesto dall'Università al proprio docente o ricercatore. Chiunque abbia utilizzato le SCC comprende che per alcuni enti, collocati in paesi non soggetti al GDPR, anche la sola interpretazione dei contenuti delle SCC richiede un'attenzione di non poco conto, considerati gli impegni che si vanno a sottoscrivere a fronte delle poche persone che l'ente dovrà accogliere e che potrebbe avere difficoltà a recepirle.

Il titolare dovrà quindi effettuare, caso per caso, un bilanciamento per comprendere se ricorrere alla deroga di cui all'art. 49, § 1, lett. *d)*, qualora né le clausole contrattuali né le disposizioni da inserire in accordi amministrativi tra organismi pubblici, previa approvazione dell'autorità garante, possano essere inclusi nell'accordo o nei protocolli attuativi.

È vero che chiunque ha il diritto di una protezione dei suoi dati personali "attaccata" ai dati durante il trasferimento; è altrettanto vero che il diritto alla conoscenza, alla libertà di pensiero, di espressione e di informazione, la libertà delle arti e della ricerca scientifica e, non ultime, la libertà personale e la libertà accademica, nel rispetto del principio di proporzionalità, come in altri casi affermato (art. 52 CDFUE), possono apportare limitazioni al diritto alla protezione dei dati se necessarie e rispondenti effettivamente a finalità

di interesse generale, riconosciute dall'Unione, o all'esigenza di proteggere i diritti e le libertà dei candidati, nel pieno rispetto del diritto all'autodeterminazione informata dell'interessato. Pertanto il ricorso alla deroga per importanti motivi di interesse pubblico sarà applicabile quando incontra la volontà dell'interessato a partecipare liberamente all'accordo di mobilità, il titolare abbia avuto cura di informarlo adeguatamente sui rischi dell'attività di trattamento e ciò sia dimostrabile, specie nell'ambito di un accordo che consenta la mobilità di un limitato numero di interessati, di cui si trattano i soli dati comuni necessari all'instaurazione del rapporto con il partner di destinazione.

Nel caso di ricorso alla deroga 49, § 1, lett. *d)*, l'informativa dovrà riportare le considerazioni del titolare in merito al bilanciamento effettuato tra i diritti e la valutazione di rischio ricordando che il titolare si assume, come di regola, ogni responsabilità sulle scelte da lui operate.

8. — *Direttiva vs regolamento e l'*effetto Bruxelles.

Il Considerando 2 della direttiva 95/46/CE poneva già in evidenza che «i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui».

Come riportato al Considerando 6 GDPR, la rapidità dell'evoluzione tecnologica e la globalizzazione hanno iniziato da tempo a trasformare l'economia, le relazioni sociali e le modalità di erogazione di servizi da parte di imprese e pubbliche amministrazioni, comportando nuove sfide per la protezione dei dati personali. La portata delle informazioni e della loro condivisione in rete sta aumentando con ritmo esponenziale, creando enormi quantità di dati (c.dd. *big data*[49]) che necessitano di un livello elevato di

[49] Con la locuzione *big data* si indica un *asset* di informazioni che richiede specifiche

protezione, affinché non venga minato il clima di fiducia necessario alla loro libera circolazione e al loro utilizzo per lo sviluppo dell'economia digitale, nel rispetto dei diritti e delle libertà individuali.

Questo perché i metodi della *big data analytics* e le specifiche tecnologie di *machine learning*, utilizzate per la trasformazione dei *big data* in valore, sono fonte di nuove opportunità di mercato, consentono di migliorare i processi decisionali anche in materia ambientale o offrire servizi innovativi, ma generano anche fenomeni ad elevato impatto sociale (si pensi al fenomeno c.d. "*confirmation bias*"[50] o al famoso caso *Cambridge Analytica*).

Nel 2015 si era espresso nel merito il Gruppo WP29, con una forte preoccupazione, affermando che «una parte importante delle operazioni sui *big data* si basa sull'ampio trattamento dei dati personali delle persone nell'UE e solleva importanti questioni sociali, legali ed etiche, tra cui le preoccupazioni relative alla privacy e ai diritti di protezione dei dati di queste persone»[51] . I benefici derivanti dall'analisi dei *big data* si sarebbero quindi potuti realmente ottenere solo a condizione che le aspettative di privacy degli utenti venissero soddisfatte e i loro diritti alla protezione dei dati rispettati.

Le preoccupazioni sulle implicazioni sociali di un utilizzo dei dati sorretto solo da interessi commerciali e privo di meccanismi di vigilanza, sono state più volte documentate in UE, anche nella «Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei *big data* per i diritti fonda-

---

tecnologie e metodi analitici per la trasformazione in Valore, in termini sia di conoscenza che di mercato economico. È caratterizzato da Volume, Varietà (molte diverse tipologie, per contenuto e formato) e Velocità con cui devono essere trattate per estrarne il valore.

[50] Indica un fenomeno cognitivo umano per il quale le persone tendono a muoversi entro un ambito delimitato dalle loro convinzioni acquisite, tendendo a confermare solo le opinioni già maturate (cfr. *wikipedia.org*). Questo fenomeno viene osservato, ad esempio, in conseguenza dell'offerta, da parte dei motori di ricerca, di proposte quanto più possibile vicine agli interessi del "navigatore", che si attagliano meglio alla sua opinione, così riducendo sempre più le occasioni di un confronto critico per maturare un'opinione maggiormente consapevole, eventualmente diversa e frutto di molteplici punti di osservazione.

[51] Gruppo WP29, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, in *ec.europa.eu/justice*.

mentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto» e sono concrete, così com'è necessaria e concreta l'esigenza di un'etica del digitale e di una normativa sui trattamenti dei dati personali che, a livello mondiale, sia compatibile con il diritto primario e secondario dell'UE, su cui l'Ue sta lavorando.

Tale requisito non è semplice da realizzare in quanto, allargando lo sguardo oltre i confini europei, si osserva che l'ordinamento internazionale non è ancora riuscito a darsi una regolamentazione sugli standard applicabili in materia di protezione dei dati personali. Lo spazio digitale, divenuto scenario di scambi commerciali e via di comunicazione, è privo di una disciplina precisa e di regole generali per il trasferimento di dati. La sovranità dello "stato digitale" sembra appannaggio dei big player di servizi e infrastrutture digitali, in base all'entità del loro potere economico.

Ecco quindi che l'Unione europea, che guarda con particolare attenzione al mercato unico digitale e agli scenari di rischio accennati, con il passaggio dalla direttiva al GDPR sta cercando di sfruttare il suo potere politico ed economico per conseguire, nell'ambito della protezione dei dati personali, quell'*effetto Bruxelles* già raggiunto nell'estendere l'applicabilità delle proprie norme fuori dai confini europei, in ambiti quali la politica competitiva, la sicurezza e la salute dei consumatori, la tutela dell'ambiente.

Per poter esercitare tale influenza, il GDPR da un lato amplia l'ambito di applicazione territoriale attraverso l'art. 3, soprattutto ai §§ 1 e 2, dall'altro rafforza al Capo V il dettato normativo sui trasferimenti extra UE, perché il trasferimento abbia luogo soltanto qualora sia assicurata ai dati personali una continuità del livello di protezione, rispetto quella garantita in Unione europea, "incollata" ai dati (*sticky regulation*).

La protezione che il GDPR vuole assicurare deve tener conto anche di qualsiasi ulteriore successivo trasferimento, dal paese estero verso altre destinazioni, considerando che i trasferimenti verso paesi esteri non sono consentiti, in linea di principio, a meno che non intervengano specifiche garanzie che il GDPR come abbiamo visto elenca, lasciando alle deroghe un ruolo marginale e solo per specifiche situazioni.

In linea con tale intento, sia le interpretazioni del GDPR formulate da

parte dei Garanti nazionali dell' EDPB sia soprattutto le decisioni della Corte di Giustizia dell'Unione Europea, espresse con le sentenze intervenute già durante l'iter di approvazione del regolamento, che è entrato in vigore nel 2016 (si pensi alla citata sentenza *Schrems I*), chiariscono che il passaggio dalla direttiva al regolamento vuole sì garantire la tutela uniforme del diritto alla protezione dei dati personali in tutto il territorio dell'Unione ma, nei limiti del possibile, vuole assicurare all'interessato la stessa tutela ai suoi diritti, anche a seguito dei trasferimenti e trattamenti dei suoi dati personali nei paesi extra UE. I confini di applicazione delle norme UE, in un mondo digitale non delimitabile, si estendono così a tutti gli operatori che vogliono interagire con l'Europa e i suoi cittadini, in considerazione delle ricadute che tali trattamenti possono avere su quei diritti e quelle libertà tutelate nella CDFUE.

A tre anni dall'entrata in vigore del GDPR, la sentenza dell'Alta Corte irlandese, dando seguito alla sentenza *Schrems II* della CGUE di dieci mesi prima, ha rimosso gli ostacoli affinché il loro Garante nazionale possa proseguire e concludere il procedimento che vieterà a Facebook il trasferimento dei dati negli USA. Appare sempre più chiaro che lo scopo della disciplina europea – di garantire che i cittadini europei possano tornare ad esercitare la piena autorità sui propri dati in un mercato, quale quello digitale, globale e non frazionabile a livello continentale – è per l'UE difficilmente negoziabile, in quanto i diritti vanno sì bilanciati ma alcuni restano inalienabili. Occorrerà vedere nel prossimo futuro in che misura ci riuscirà.

9. — *Conclusioni.*

Il trasferimento di dati personali verso paesi terzi è considerato un trattamento ad alto rischio per le libertà e i diritti fondamentali e pertanto può avere luogo solo nel rispetto delle condizioni di cui al Capo V prima riportate.

In virtù dell'*accountability*, il titolare assume una responsabilità interpretativa della normativa applicabile all'attività di trattamento, dei fattori di rischio

e delle condizioni di garanzia che dovrà conseguentemente porre in essere. La decisione deve prenderla sulla base di un contesto normativo non sempre facile da comprendere, in continua evoluzione e che richiede la lettura di documenti interpretativi del Board europeo, a volte anche specifici dei contesti nei quali porrà in essere l'attività di trattamento. Il suo modus operandi dovrà tener conto, caso per caso, della natura, dell'oggetto, del contesto e delle finalità del trattamento, delle migliori pratiche attuabili allo stato dell'arte rispetto ai costi di attuazione come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, in relazione alla portata dell'attività e della tipologia e quantità dei dati trattati.

L'unica via perseguibile per il titolare diviene quindi la dimostrabilità delle scelte e criteri operati, avendo compiuto ogni sforzo possibile per bilanciare rischi, diritti e libertà degli interessati.

È fondamentale quindi che innanzitutto conosca quali siano le attività di trattamento che comportano trasferimenti di dati extra UE, sia che esse riguardino i progetti di ricerca, le attività didattiche, la mobilità del personale e degli studenti, l'utilizzo di piattaforme di servizi in cloud, le richieste di dati provenienti da paesi terzi, p.e. inerenti curriculum di laureati o dipendenti dell'Ateneo, o altre attività amministrative anche frequenti in ambito universitario, come l'affidamento a terzi di servizi inerenti il personale o gli studenti, che potrebbero comportare trasferimenti di dati extra UE in virtù di sub-responsabili individuati dalle società appaltatrici del servizio.

È ovvio che le valutazioni che effettuerà nel caso dell'accordi di mobilità del singolo docente per poter perseguire un'attività di ricerca saranno ben diverse da quelle che andranno effettuate per l'affidamento di un servizio di posta elettronica di Ateneo ad un provider extra UE, che magari prevede anche l'utilizzo di uno spazio condiviso per la memorizzazione e condivisione di tutta la documentazione amministrativa o di ricerca di ateneo a iniziare dall'ipotesi, nel secondo caso, di un obbligo di DPIA e dall'esclusione certa del ricorso alle deroghe.

Tra i fattori di qualità di un aggiudicatario, valutabili in fase di gara, andrebbe considerata, nell'ordine, l'appartenenza del fornitore allo spazio economico europeo o la localizzazione in territori per i quali esista una de-

cisione di adeguatezza o, in ultima ipotesi, l'assunzione dell'impegno alla sottoscrizione di clausole contrattuali standard, integrate secondo le ulteriori misure di garanzia che il titolare dovesse ritenere necessarie, al momento della sottoscrizione del contratto, pena la risoluzione dell'affidamento.

Il censimento delle attività di trattamento dei dati personali, finalizzato alla redazione del Registro delle attività, deve porre in evidenza tutti i trasferimenti extra UE mentre la conoscenza della loro esistenza deve consentire una seria analisi dell'attività, sia rispetto l'adeguatezza, pertinenza e non eccedenza dei dati oggetto di trasferimento rispetto alle finalità dello stesso, sia con riguardo alla condizione di garanzia individuata, tra quelle previste dal GDPR, perché il trasferimento sia lecito, specie in presenza di categorie particolari di dati personali.

Occorre anche tener presente che, con il GDPR, le decisioni di adeguatezza possono essere revocate e, in condizioni particolari, anche in tempi molto brevi. Nei casi di movimenti della scena politica del paese di destinazione, già osservabili al momento di avviare un trasferimento con un ente situato in tale paese e che potrebbero inficiare i presupposti di adeguatezza su cui si fonda una decisione esistente, potrebbe costituire una valida misura di "privacy by design" inserire negli accordi l'impegno a sottoscrivere delle garanzie specifiche, già accluse all'accordo, cui poter far immediatamente ricorso al venir meno della decisione di adeguatezza.

Considerate le numerosissime e diversificate attività con cui l'Università tratta i dati personali, costituirebbe un'importante elemento di *accountability* l'adozione di codici di condotta previsti e auspicati all'art. 40 GDPR o anche di linee guida su come gestire i trasferimenti, con particolare riguardo alle attività didattiche e di ricerca, che sono per loro natura libere e diversificate tra loro e che pongono pertanto in essere scenari di rischio maggiori rispetto le attività amministrative, solitamente rigidamente normate.

Le informative per l'interessato devono ovviamente contenere il criterio individuato per il trasferimento dei dati personali extra UE, se previsto, indicando quale sia il paese di destinazione e quali le garanzie approntate per la tutela dei suoi diritti.

All'interno del gruppo dei DPO universitari del Codau, è stata propo-

sta una check list dei requisiti che il trasferimento di dati personali deve soddisfare per poter essere attuato, sulla base delle sue caratteristiche e del contesto dell'attività, derivandola da una puntuale applicazione delle Raccomandazioni 01/2020 dell'EDPB. Come avvenuto per lo schema tipo per il trattamento dei dati sensibili nel 2015, cui abbiamo già accennato, sarebbe auspicabile, oltre che opportuno, che la Conferenza dei Rettori delle Università italiane (CRUI), organismo rappresentativo quindi dei "titolari dei trattamenti universitari", proponesse l'adozione di strumenti, quali simili check list, codici di condotta o linee guida sui trasferimenti di dati, anche in relazione ai numerosissimi progetti di ricerca o accordi internazionali che sono attività di trattamento comuni a tutti gli Atenei, richiedendo su di essi il parere del garante nazionale, ai sensi dell'art. 40, § 5 e dell'art. 57, § 1.m).

Esse costituirebbero un valido supporto all'*accountability* dei titolari, nel contesto universitario, come pure l'individuazione di tecniche per la pseudonimizzazione, l'anonimizzazione o la crittografia dei dati personali da poter adottare per ridurre i rischi agli interessati derivanti dai trattamenti, specie se effettuati extra UE.

Quello dei flussi di dati extra UE è un tema delicato, reso ancor più problematico dalla diversità degli ordinamenti giuridici degli Stati extra UE e dalla presenza dei colossi del mercato digitale, collocati al di fuori dello Spazio economico europeo, che forniscono servizi e infrastrutture digitali estremamente competitivi per qualità e costi, pertanto molto richiesti da aziende, enti pubblici e privati oltre che dai singoli cittadini europei.

L'UE sta affrontando questi problemi da tempo sul piano politico, oltre che normativo, con la visione strategica di un futuro dove i dati e gli algoritmi siano effettivamente utilizzati al servizio dell'uomo e sempre nel pieno rispetto dei suoi diritti e delle sue libertà, in un mondo digitale senza confini geografici.

Il GDPR, nel recepire la necessità di disciplinare la tutela dei dati personali, tenendo conto dell'esigenza di favorirne la libera circolazione, fornisce vari strumenti di cui il titolare può avvalersi, anche congiuntamente tra loro, per assicurare un adeguato livello di tutela dei diritti delle persone in ogni fase dell'attività di trattamento dei loro dati personali, con la flessibilità ri-

chiesta dai vari contesti delle attività di trattamento, anche con riguardo ai trasferimenti extra UE, avvalendosi responsabilmente dell'*accountability*.

Se ci si sofferma però sull'interpretazione restrittiva che la CGUE fornisce sugli strumenti di tutela previsti dal GDPR, comprese le clausole contrattuali adottate dalla Commissione europea, nonché sul terzo passo delle Raccomandazioni 01/2020 dell'EDPB, si osserva che al titolare compete anche il "valutare se vi sia qualcosa nella legge o nella prassi del paese terzo che possa incidere sull'efficacia delle garanzie adeguate degli strumenti di trasferimento", valutazione che prima era appannaggio esclusivo della Commissione Europea, al fine di assumere o meno una decisione di adeguatezza.

Inoltre, per il principio di responsabilizzazione, che comporta vigilanza continua sulle attività poste in essere, il titolare deve anche rivalutare periodicamente, come previsto al passo 6 delle Raccomandazioni 01/2020, il livello di protezione assicurato ai dati trasferiti verso paesi terzi e controllare se vi siano stati o vi saranno sviluppi che possano influire su tale protezione.

Al di là dell'impossibilità che il titolare possa essere competente e in grado di porre in essere una valutazione del contesto normativo dei paesi destinatari e sub-destinatari di questo tipo, si evidenziano almeno tre situazioni insolite: a) la discrezionalità del titolare in una tale valutazione; b) una valutazione del rischio del trasferimento "piatta", non basata sul contesto dell'attività di trattamento; c) l'impossibilità di effettuare rivalutazioni periodiche nei molti casi di squilibrio di competenze tecnologiche tra le parti.

Riguardo la discrezionalità, essa rischia di minare quell'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone non solo in tutta l'Unione, ma anche solo già all'interno dello stesso Stato membro, sulla base di valutazioni soggettive e diverse tra differenti titolari (ad esempio università diverse), chiamati ciascuno ad prendere in proprio una decisione di adeguatezza, ferma restando la difficile competenza dei più in materia.

Da una lettura fedele anche delle Raccomandazioni 01/2020 dell'EDPB, questa valutazione di impatto del trasferimento va inoltre applicata in tutti i casi in cui non vi sia il ricorso ad una decisione di adeguatezza o ad una deroga, queste ultime non utilizzabili per i trasferimenti "a regime", indipen-

dentemente dal contesto dell'attività di trattamento, dalla tipologia e quantità dei dati trasferiti, ad esempio, oppure dal se si trasferiscano solo un nome e cognome o se si trasferiscano dati sanitari o biologici.

Siffatta valutazione, diversa dalla DPIA e basata sulla roadmap disegnata dalle Raccomandazioni 01/2020, se applicata ad ogni attività che comporti un trasferimento di dati extra UE ha un costo elevato, ancor più nel caso di utilizzi di servizi di fornitori extra UE per i quali andrebbero valutati anche i rischi degli eventuali successivi trasferimenti verso altri paesi terzi. Considerata la difficoltà di comprensione della normativa di paesi extra UE, data la diversa forma linguistica, e la complessità dell'analisi tecnico giuridica che occorre effettuare per verificare l'adeguatezza di tale paese, a monte dell'eventuale trasferimento dei dati, nei costi di gestione andrebbero considerati anche gli strumenti tecnici e le professionalità ritenuti più consoni ad una valutazione quanto più esatta di tale contesto giuridico. Questo può portare da un lato ad un aumento dei costi di gestione, dall'altro a rischi quali quello di optare per un servizio che si dichiari "GDPR compliance" ma che ha un livello di qualità sensibilmente inferiore, con un aumento dei rischi dell'attività di trattamento.

Va inoltre tenuto conto delle eventuali modifiche normative, successive al trasferimento, di cui l'importatore potrebbe non dare comunicazione al titolare, tali da comportare una restrizione dei diritti degli interessati e la conseguente necessaria revoca stessa degli accordi, qualora il titolare ne venisse posto a conoscenza.

Se poi già ora si assiste alla difficoltà di disciplinare le attività di trattamento con un *big player* del mercato digitale extra UE, che spesso per la responsabilità *ex* art. 28 GDPR pubblica le proprie condizioni stabilite unilateralmente che i titolari sono tenuti ad accettare in toto - tanto più sarà difficile fargli sottoscrivere delle clausole contrattuali che, oltre allo standard, vogliano imporre le ulteriori misure di garanzia che il titolare ritiene di dover adottare. Gli accordi proposti dal titolare vengono considerati sempre negoziabili, mentre le clausole contrattuali standard no.

Il progetto di decisione delle nuove clausole contrattuali, pubblicato dalla Commissione europea e che dovrà recepire esso stesso le indicazioni for-

nite con la "joint opinion" del EDPB e dell'EDPS, sarà quindi decisivo per comprendere quale sarà il contesto ritenuto adeguato, rispetto quanto sinora evidenziato, per effettuare trasferimenti extra UE, mantenendo il principio dell'uniforme e coerente applicazione normativa; l'EDPB dovrà sforzarsi di fornire altri strumenti al titolare per supportarlo in questo contesto di attività, che non siano solo una *roadmap*.

E nel frattempo? Il titolare si assume la sua responsabilità, essendo "competente e in grado di dimostrarlo".