

I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*

Matteo Leffi

SOMMARIO: 1. Introduzione: l'importanza dei trasferimenti di dati. –
2. Trasferimenti di dati personali verso paesi terzi o organizzazioni
internazionali nel Regolamento (UE) 679/2016.

1. Introduzione: l'importanza dei trasferimenti di dati

Nella società contemporanea, significativamente ribattezzata "società dell'informazione", l'importanza rivestita dai flussi di informazioni, e quindi di dati, è primaria.

Questi ultimi, sino a non molti anni fa mero strumento funzionale ai traffici commerciali, sono oggi diventati essi stessi merci, beni economici con un proprio valore intrinseco: nell'era del *web*, dell'*internet of things*, dei *social network* e dei *big data* essi possono venire raccolti in grande quantità, digitalizzati, aggregati, combinati, studiati e, soprattutto, venduti e sfruttati economicamente o per altre finalità.

In questo quadro, gli scambi di dati tra diversi Stati e diverse aree economiche del pianeta non sono (più) soltanto un mero aspetto dei traffici commerciali: essi assurgono al contempo a beni di scambio e infrastruttura portante di rapporti giuridici ed economici via via più interdipendenti e interconnessi. Un'infrastruttura, è il caso di rimarcarlo, intrinsecamente internazionale, fluida e delocalizzata.

L'estrema importanza dei flussi di dati scambiati nel mondo (*in primis*, per rilevanza quantitativa e qualitativa, quelli tra Unione europea e Stati Uniti d'America), inoltre, rende questi complessi scambi tutt'altro che neutrali: essi svolgono nella società della "rivoluzione digitale" un ruolo sempre più incisivo quanto agli equilibri geopolitici, economici, culturali.

Non solo: poiché molto spesso questi dati, singolarmente o per effetto delle loro aggregazioni e combinazioni da parte di imprese private o poteri pubblici, contengono informazioni personali e si prestano dunque a dire molto su carattere, abitudini, opinioni, attività

ed esperienze dei soggetti cui appartengono, è di estrema importanza considerare le ripercussioni che questi fenomeni producono sui diritti fondamentali della persona, e, in ultima istanza, su ognuno di noi.

Sulla scorta di quanto sopra, è evidente come il tema del trasferimento dei dati personali dall'Unione europea verso stati terzi extra-europei sia un tema particolarmente rilevante nell'attuale contesto economico, giuridico e politico.

Ciò è particolarmente vero se si tiene conto che, come autorevolmente rilevato, «l'esportazione extraeuropea di dati personali finisce per comportare, nella maggior parte delle occasioni, la transizione di informazioni da un'area giuridica ad elevato grado di protezione per il diritto alla riservatezza verso ordinamenti ove il *right to privacy* non è circondato dalle medesime garanzie»¹.

A riprova dell'importanza che già nel 1995 aveva - e si intuiva avrebbe ancora acquisito in futuro - questo tema, la Direttiva 95/46/CE, per più di vent'anni comune cornice di riferimento della *data protection* europea, dedica il proprio intero Capo IV al problema.

Alla luce del fatto che il grado di tutela dei dati personali raggiunto dalla normativa europea unitaria non ha eguali negli altri Paesi industrializzati, non è difficoltoso intuire la *ratio* che sottende le disposizioni della Direttiva 95/46/CE dedicate al trasferimento di dati personali dal territorio dell'Unione verso Stati terzi.

In brevis, permettere siffatti trasferimenti, senza che questi siano sottoposti a condizioni o limitazioni di sorta, equivarrebbe a rendere possibili e ad avallare pratiche di *shopping* regolatorio da parte di soggetti interessati ad aggirare la più stretta cornice normativa europea, a favore di sistemi più congeniali al titolare del trattamento poiché caratterizzati da forme di tutela più blande o comunque meno costose.

Si tratta, per usare le parole della Commissione europea, di un problema afferente «la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati» in uno stato terzo².

¹ S. SICA, V. D'ANTONIO, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 4/5, 2015, p. 801.

² Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite (COM/2013/847 *final*) del 27 novembre 2013, punto 25.

2. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali nel Regolamento (UE) 679/2016.

A decorrere dal 25 maggio 2018 la disciplina in materia di dati personali dettata dalla Direttiva 95/46/CE cesserà di avere vigore, in favore delle disposizioni del nuovo GDPR – *General Data Protection Regulation*³.

Tra i profili coinvolti dall'aggiornamento della normativa europea sulla *data protection*, ve ne sono senza dubbio molteplici di interesse in una dimensione internazionale, poiché coinvolgono la disciplina del trasferimento di dati verso Paesi terzi e con essa, in un certo senso, la “proiezione esterna” del diritto dell’Unione europea in materia di protezione dei dati personali.

L'attenzione che la nuova disciplina dedica a questi temi è massima, e le motivazioni di questo interesse, che ribadiscono quanto già sviluppato nell'introduzione di questo contributo, emergono già dal sesto Considerando al nuovo Regolamento, che vale la pena riportare qui per esteso: «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali»⁴.

Come osservato in dottrina, alla base della centralità di questi profili non vi sarebbe (più) soltanto e soprattutto lo sviluppo della società digitale con i suoi portati economici, tecnologici e culturali; infatti, in special modo a seguito della decisione *Schrems* che ha

³ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati, pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016).

⁴ Regolamento (UE) 2016/679, Considerando numero 6.

invalidato gli accordi di *Safe Harbor* con gli Stati Uniti d'America⁵ «tutta questa materia è al centro di confronti serrati, che continueranno certamente anche con maggior forza dopo l'entrata in vigore del nuovo regolamento»⁶.

Sulla scorta di queste premesse, non stupisce quindi il sensibile incremento nel numero di disposizioni che il nuovo Regolamento, se confrontato con la normativa attualmente in vigore, dedica a queste tematiche.

Già in base a considerazioni preliminari, infatti, può notarsi *ictu oculi* come dalle due disposizioni che formavano il vecchio capo IV della Direttiva 95/46/CE (l'articolo 25 rubricato «Principi» e l'articolo 26 contenente le ipotesi di deroga a tali principi) si sia passati a ben sei disposizioni (artt. 44-50), alcune delle quali particolarmente copiose, nel nuovo capo V del Regolamento 2016/679.

Procedendo ora all'analisi individuale delle singole disposizioni, sarà possibile mettere in luce i principali caratteri di originalità e discontinuità della nuova normativa europea in materia di flussi di dati verso paesi terzi, in un impianto che comunque rimane largamente fedele, in particolar modo nei principi, a quello previsto dalla Direttiva 95/46/CE.

Per vero, la prima sorpresa arriva già dalla lettura della rubrica del capo V, la quale reca «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali».

Il dettato della Direttiva 95/46/CE faceva infatti menzione esclusiva dei «Trasferimenti di dati verso paesi terzi», riferimento che è stato dunque esteso nella nuova formulazione, finendo in questo modo per riferire l'applicabilità delle norme del Regolamento (non soltanto ai paesi terzi ma) all'endiadi «paesi terzi o organizzazioni internazionali»⁷.

⁵ Per un'analisi della decisione in parola e, più in generale, una panoramica sull'attivismo della Corte di giustizia dell'Unione europea in materia di protezione dei dati personali si rimanda a M. BASSINI, O. POLLICINO, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 4/5 2015, p. 741 e ss.

⁶ F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 109, nota 29.

⁷ Si è rilevato in dottrina come l'impianto del Capo V del nuovo Regolamento costituisca in ultima analisi una razionalizzazione ed ampliamento della (pre)vigente disciplina; quanto all'ampliamento dei soggetti passibili di una valutazione di adeguatezza da parte della Commissione europea, è stato invece evidenziato che tale novità richiederà di essere ulteriormente specificata in via interpretativa. Cfr. D. BORELLI, *La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali*

La disposizione d'apertura del capo V è l'articolo 44, che detta il «Principio generale» per i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (e per gli eventuali trasferimenti ulteriori da questi verso altri paesi terzi o organizzazioni internazionali): ovverosia il rispetto, da parte del titolare e del responsabile del trattamento, delle condizioni previste dal capo V, fatte salve le altre disposizioni del Regolamento.

Con riferimento a questo profilo pare dunque confermato l'impianto, già della Direttiva 95/46/CE, imperniato su un generale divieto di trasferimento estero dei dati personali al di fuori dei casi di «tutela adeguata» dei dati prestata nel paese terzo di trasferimento, ovvero delle altre deroghe previste tassativamente dalla normativa europea⁸.

In aggiunta a ciò, l'ultima frase dell'articolo 44 contiene quella che pare una petizione di principio, ma che probabilmente rivestirà la massima importanza e autorità in sede ermeneutica, prevedendo che: «tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato»⁹.

tra nuovo Regolamento europeo e (pre)vigente Direttiva, del 10 dicembre 2016, liberamente consultabile al seguente link: www.dimt.it/index.php/it/notizie/15688-la-valutazione-di-adequatezza-nei-trasferimenti-transfrontalieri-di-dati-personali-tra-nuovo-regolamento-europeo-e-pre-vigente-direttiva.

⁸ In questo senso P. PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *Il diritto dell'Informazione e dell'Informatica*, 2015, n. 4/5, p. 851.

⁹ Cfr. Regolamento (UE) 2016/679, articolo 44. Una tale indicazione d'intenti, come visto, non è peraltro nuova giacché riprende la preoccupazione, già manifestata nella Direttiva 95/46, che pratiche di *forum shopping* possano vanificare la *ratio* di tutela della legislazione europea in materia di dati personali. Peraltro, tale concetto è ribadito anche dal Considerando *numero* 101 al Regolamento in esame, che così recita: «È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso (...) In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento». Ciò che pare invece meno consueto - e perciò di maggior interesse - è la scelta del legislatore europeo di estrinsecare tale principio nel corpo di una norma. Secondo F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 161, «sarebbe forse ingeneroso limitarsi a sostenere che la prevalente continuità fra Regolamento e Direttiva sia legata solo alla spinta, certamente fortissima all'epoca della 95/46, ad alzare barriere difensive nei confronti degli operatori residenti in altri Stati». A parer dell'Autore

L'articolo 45, che consta di ben nove paragrafi, è dedicato al «Trasferimento sulla base di una decisione di adeguatezza» e si pone in linea di continuità con le previsioni della Direttiva del '95 quanto al trasferimento dei dati personali verso quei paesi terzi/organizzazioni internazionali (ovvero soltanto verso alcuni territori o uno o più settori specifici all'interno del Paese terzo)¹⁰ che garantiscano un livello di protezione «adeguato».

A differenza del vecchio articolo 26 della Direttiva 95/46/CE, che disegna una sorta di «parallelismo provvisorio di competenze» tra Commissione e Stati membri in materia di sindacato sull'adeguatezza della tutela fornita nel paese terzo (riservando comunque alla prima l'ultima parola in merito), nel nuovo articolo 45 scompare ogni riferimento agli Stati membri.

La Commissione è dunque l'organo dell'Unione che emerge quale *dominus* incontrastato in materia di trasferimenti basati su una decisione di adeguatezza: una volta che una siffatta decisione venga positivamente adottata con riferimento a un paese terzo o a un'organizzazione internazionale, il trasferimento non necessiterà di ulteriori autorizzazioni specifiche da parte degli Stati¹¹.

andrebbe infatti tenuto in debita considerazione l'impatto della avvenuta costituzionalizzazione della tutela dei dati personali nella normativa dell'Unione, e dunque la forte novità introdotta dall'articolo 8 della Carta dei diritti dell'Unione europea nel prevedere un diritto alla protezione dei dati di carattere personale. Accanto dunque alle preoccupazioni «difensive» (ma anche di armonizzazione e completamento del mercato interno) che stavano alla base della disciplina della Direttiva, le scelte normative contenute nel Regolamento sono fondate oggi su di un «diritto fondamentale, la difesa del quale è strettamente connessa anche alla tutela dei diritti e delle libertà fondamentali». Sul ruolo delle disposizioni «costituzionali» di cui agli articoli 7 e 8 della Carta di Nizza, si veda *ex multis* M. BASSINI, O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Il Diritto dell'Informazione e dell'Informatica*, n. 4/5, 2014, p. 831 e ss.

¹⁰ La previsione di una decisione di adeguatezza che può riconoscersi anche solo in riferimento a «un territorio o uno o più settori specifici all'interno del paese terzo» costituisce un profilo rilevante di novità apportato dal Regolamento. Si tratta di una aggiunta che fornisce alla Commissione uno strumento di flessibilità ulteriore con riguardo ai giudizi di adeguatezza, e il cui reale impatto è difficile da inquadrare con una valutazione prognostica non potendo che essere giudicato sulla base dell'applicazione che ne verrà, o meno, effettuata nella pratica.

¹¹ Di contrasto, va rilevato come il Regolamento riconosca grande indipendenza alle Autorità nazionali di controllo, alle quali è attribuito in particolare il potere di sospendere i flussi di dati personali verso un paese terzo. Così M. NINO, *Le prospettive*

Quanto invece agli elementi che devono essere considerati nel giudizio di adeguatezza della protezione dei dati, la formulazione concisa e generica del vecchio articolo 25, paragrafo secondo («tutte le circostanze relative ad un trasferimento di dati») lascia spazio a quella più completa e analitica contenuta alle lettere a), b) e c) dell'articolo 45, paragrafo secondo, del Regolamento¹².

Oggetto di valutazione saranno pertanto:

1. «lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento»;

2. «l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri»; e

3. «gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla

internazionali ed europee della tutela della Privacy, in *Il diritto dell'Unione europea*, n. 4, 2016, p. 781.

¹² In questo senso anche D. BORELLI, *La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali tra nuovo Regolamento europeo e (pre)vigente Direttiva*, cit., p. 5, il quale riconduce tale scelta di tecnica legislativa all'intento di ridurre «l'incertezza generata dalla vaghezza di talune norme della (pre)vigente normativa». In P. PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, cit., p. 854 e ss., si evidenzia invece il restringimento della discrezionalità della Commissione nella valutazione di adeguatezza della tutela che consegue al grado di dettaglio dei requisiti di seguito elencati.

loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali»¹³.

Come è possibile rilevare da una comparazione con quanto già scritto in merito ai criteri in materia di adeguatezza sotto la vigenza della Direttiva 95/46, la norma appena riportata pare aver recepito ed esplicitato tendenze già sviluppate in sede ermeneutica: si pensi ad esempio al riferimento alla «esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo» o anche agli impegni internazionali e «altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti»¹⁴.

La valutazione positiva del livello di adeguatezza da parte della Commissione può dunque avvenire, ex articolo 45, paragrafo terzo, del Regolamento «mediante atti di esecuzione»¹⁵: in questo caso tale atto¹⁶ prevede un meccanismo di riesame periodico, da effettuarsi almeno ogni quattro anni, che avrà ad oggetto l'adeguatezza della protezione dei dati

¹³ Cfr. Regolamento (UE) 2016/679, articolo 44. L'elencazione della lettera a) dell'articolo 44 del Regolamento è quella che maggiormente innova rispetto all'articolo 25 della Direttiva 95/46/CE, giacché contiene «una serie impressionante e molto precisa di requisiti che il soggetto terzo deve avere, sia con riferimento alla sua legislazione che, si potrebbe dire, alla sua stessa visione politica e ideologica di Stato di diritto e di democrazia». Vedi. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 162.

¹⁴ Peraltro, il Regolamento pare recepire gli orientamenti della Corte di Giustizia (e in particolare la giurisprudenza *Schrems*) anche in riferimento al concetto stesso di adeguatezza, laddove chiarisce che «il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione». Cfr. Regolamento UE 2016/679, Considerando 104.

¹⁵ A norma del paragrafo 5 dell'articolo 45 viene inoltre riconosciuto alla Commissione il potere di adottare atti di esecuzioni che siano immediatamente applicabili, al ricorrere di «imperativi motivi di urgenza debitamente giustificati». Siffatti atti di esecuzione dovranno adottarsi secondo la procedura d'esame prevista dall'articolo 93, paragrafo terzo del Regolamento, il quale rimanda a propria volta all'applicazione l'articolo 5 del Regolamento (UE) n. 182/2011 in combinato con il suo articolo 8. In questa categoria rientrerebbero ad esempio atti quali gli accordi di *Safe Harbor* o il *Privacy Shield*. Così D. BORELLI, *La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali tra nuovo Regolamento europeo e (pre)vigente Direttiva*, cit., p. 5.

¹⁶ A norma della disposizione in parola, tale atto di esecuzione andrà adottato secondo la procedura d'esame prevista dall'articolo 93, paragrafo secondo del Regolamento, il quale rimanda a propria volta all'applicazione dell'articolo 5 del Regolamento (UE) n. 182/2011.

personali in riferimento agli «sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale»¹⁷.

Tali rilievi si accompagnano ad una più generale e costante attività di controllo da parte della Commissione su tali «sviluppi pertinenti» in grado di incidere sul funzionamento delle decisioni (articolo 45, paragrafo quarto)¹⁸.

Esito di queste pratiche di “monitoraggio” potrebbe essere un riscontro negativo con riferimento al permanere dello standard di adeguatezza di protezione dei dati richiesto dalla normativa dell'Unione: a quel punto la Commissione europea potrà esercitare una serie di poteri.

Da un lato, essa può revocare, modificare o sospendere (nella misura che si riveli necessaria) la decisione precedentemente adottata, per il tramite di atti di esecuzione con efficacia *ex tunc* (articolo 45, paragrafo quinto)¹⁹; dall'altro lato, all'esercizio di tali poteri fa da contraltare l'obbligo per la Commissione di avviare consultazioni per porre rimedio alla situazione così venutasi a creare (articolo 45, paragrafo sesto)²⁰.

La lista dei paesi terzi e delle organizzazioni internazionali nei confronti delle quali è stata adottata una decisione di adeguatezza (o una decisione di tal guisa è stata revocata, sospesa o modificata) viene pubblicata ad opera della Commissione europea sul suo sito web e nella

¹⁷ Sul punto anche M. NINO, *Le prospettive internazionali ed europee della tutela della Privacy*, cit., p. 781.

¹⁸ Il paragrafo citato fa peraltro espresso riferimento non soltanto alle decisioni di adeguatezza adottate ex art. 45, paragrafo 3 del Regolamento, ma anche a quelle adottate ex art. 25, paragrafo 6 della Direttiva 95/46/CE.

¹⁹ Tali atti andranno adottati di norma seguendo la già citata procedura d'esame prevista dall'articolo 93, paragrafo secondo del Regolamento ovvero, in caso di estrema urgenza, quella prevista dal paragrafo terzo del medesimo articolo. Al paragrafo settimo si chiarisce invece come una siffatta previsione lasci impregiudicati i trasferimenti che trovano la loro base giuridica nei successivi articoli da 46 a 49.

²⁰ È evidente l'intento sotteso alla previsione di questi meccanismi di monitoraggio e riesame periodico, nonché dei poteri di revoca, modifica o sospensione delle decisioni di adeguatezza individuati in capo alla Commissione. Si è voluto evitare per il futuro, infatti, ciò che è successo nel caso *Schrems*, con la Corte di giustizia "costretta" ad invalidare un accordo risalente a ben 15 anni prima, e mai revisionato, che non rispondeva più adeguatamente alle evoluzioni intervenute nel tempo quanto alle esigenze di adeguatezza della tutela. Di questo parere anche D. BORELLI, *La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali tra nuovo Regolamento europeo e (pre)vigente Direttiva*, cit., p. 5. Peraltro, la genericità dell'obbligo di avviare nuove trattative e la mancanza di termini temporali previsti a questo fine, finisce per risolversi in un ampio sindacato discrezionale in capo alla Commissione europea.

Gazzetta ufficiale dell'Unione europea, a norma del disposto dell'articolo 45, paragrafo ottavo.

Il successivo paragrafo nono, infine, contiene una clausola di raccordo che fa salva l'efficacia delle decisioni adottate dalla Commissione sotto la vigenza dell'articolo 25, paragrafo 6 della vecchia Direttiva 95/46/CE e che non siano state successivamente modificate, sostituite ovvero abrogate da una decisione adottata ai sensi del Regolamento 2016/679²¹.

Il nuovo articolo 46, rubricato «Trasferimento soggetto a garanzie adeguate», disciplina invece quella che altrove è stata individuata come la seconda di tre «situazioni tipo» in base alle quali è possibile trasferire i dati personali verso Paesi terzi o verso organizzazioni internazionali²².

Si tratta quindi di una ipotesi alternativa a una decisione di adeguatezza, valida in ogni caso «a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi»²³.

In particolare, sotto la generica dicitura di «garanzie adeguate» sono ricondotte numerose e differenti fattispecie, che potrebbero categorizzarsi in questo modo: da un lato quelle salvaguardie che non necessitano di una specifica autorizzazione da parte di un'Autorità di controllo (elencate al paragrafo secondo, lettere da a) sino ad f), dell'articolo 46); dall'altra quelle che invece la richiedono (elencate invece al paragrafo terzo, lettere a) e b) del medesimo articolo)²⁴.

²¹ Questo rilievo, come si vedrà, vale peraltro a salvaguardare l'efficacia del nuovo accordo di *Privacy Shield* tra UE e Stati Uniti nel delicato passaggio dalla vigenza della Direttiva 95/46 alla nuova normativa dettata dal Regolamento. Tale volontà emerge inoltre anche dal Considerando 102 al Regolamento, laddove si legge che «Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati».

²² Si veda in proposito C. COMINOTTO, A. MINICHELLO, F. CURTARELLI, *Il trasferimento dei dati personali in Paesi extra UE*, Diritto 24 – Il Sole 24 Ore, 3 ottobre 2016, liberamente consultabile al link: <http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2016-10-03/il-trasferimento-dati-personali-paesi-extra-ue-180336.php>.

²³ Cfr. Regolamento (UE) 2016/679, articolo 46, paragrafo 1.

²⁴ F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 110, nota 29. Peraltro, l'elencazione contenuta all'articolo 46 dovrebbe considerarsi esemplificativa e non tassativa. Vedi P. PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, cit., p. 852.

Segnatamente, al primo novero di «garanzie adeguate» vanno ascritte le *binding corporate rules* (o “BCR”)²⁵, le *standard data protection clauses* (o “SDPC”)²⁶, i codici di condotta²⁷ e i meccanismi di certificazione²⁸ (questi ultimi due vanno approvati unitamente all’impegno vincolante dell’importatore ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati), nonché gli strumenti giuridicamente vincolanti e aventi «efficacia esecutiva tra autorità pubbliche o organismi pubblici»²⁹.

Più nello specifico, i codici di condotta sono volti a contribuire all’applicazione del Regolamento e possono essere elaborati da associazioni e organismi rappresentanti di categorie di titolari o responsabili del trattamento³⁰. I meccanismi di certificazione della

²⁵ Nel testo italiano «norme vincolanti d’impresa», le quali godono tra l’altro di espressa e autonoma formulazione all’articolo seguente, come vedremo nel seguito. Per *binding corporate rules* o BCR si intendono quelle «norme vincolanti d’impresa» che si traducono in regolamenti interni, *policies* aziendali, codici di condotta, attività di *audit* o altre previsioni attraverso le quali una società si obbliga, nell’effettuare il trasferimento verso le società infragruppo, al rispetto di un certo standard nel trattamento dei dati personali.

²⁶ Nel testo italiano «clausole tipo di protezione dei dati», le quali possono essere adottate dalla Commissione secondo la procedura d’esame di cui all’articolo 93, paragrafo 2, del Regolamento, ovvero possono essere adottate da un’Autorità di controllo e poi approvate dalla Commissione sulla base della medesima procedura. Per clausole tipo di protezione dei dati («clausole contrattuali standard» nella Direttiva del 95) si intendono quelle clausole le quali, incorporate nel testo di un contratto avente ad oggetto l’esportazione di dati personali, impegnano l’importatore (stabilito al di fuori dell’Unione europea) al rispetto di precise garanzie *relative* al loro trattamento, e, in ultima analisi, garantiscono un livello «adeguato» di tutela dei dati limitatamente a una determinata finalità di trattamento.

²⁷ Approvati a norma dell’articolo 40 del Regolamento.

²⁸ Approvati a norma dell’articolo 42 del *Regolamento*. Questi costituiscono «una sorta di marchio di conformità, (...) concesso dall’autorità nazionale di controllo a conclusione di una procedura amministrativa volta a certificare che il trasferimento dei dati è effettuato in conformità con le norme del regolamento, allo scopo di segnalare al pubblico l’adozione volontaria, da parte del responsabile o dell’incaricato del trattamento, di una serie di misure, procedure e controlli a garanzia della legittimità del trattamento». Cfr. P. PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, cit., p. 853.

²⁹ Cfr. Regolamento (UE) 2016/679, articolo 46, paragrafo 2. Vedi anche F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 110, nota 29.

³⁰ Cfr. Regolamento (UE) 2016/679, articolo 40. I codici di condotta possono essere elaborati allo scopo di precisare l’applicazione del Regolamento in oggetto, per esempio, in riferimento ai seguenti aspetti: «a) il trattamento corretto e trasparente dei dati; b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti

protezione dei dati, nonché i sigilli e marchi di protezione dei dati, similmente ai codici di condotta possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al Regolamento, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. Tali soggetti assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare adeguate garanzie ai diritti degli interessati.

Quanto alle «garanzie adeguate» che necessitano dell'autorizzazione dell'Autorità di controllo competente, si fa riferimento a due ipotesi: le clausole contrattuali (diverse da BCR e SDPC) tra titolare e responsabile del trattamento, ovvero tra responsabile del trattamento e destinatario dei dati personali nel Paese terzo/organizzazione internazionale; e le disposizioni che prevedono diritti azionabili ed effettivi per gli interessati che vanno inserite in accordi amministrativi tra autorità od organismi pubblici³¹.

Anche l'articolo 46 si chiude con una clausola residuale, che fa salve questa volta le autorizzazioni rilasciate sotto la vigenza della Direttiva 95/46/CE ai sensi dell'articolo 26, paragrafo secondo, e le decisioni adottate in base all'articolo 26, paragrafo quarto (*model*

specifici; c) la raccolta dei dati personali; d) la pseudonimizzazione dei dati personali; e) l'informazione fornita al pubblico e agli interessati; f) l'esercizio dei diritti degli interessati; g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore; h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32; i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato; j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79».

³¹ Secondo il dettato dell'articolo 46, paragrafo 4 del Regolamento, in queste ipotesi l'Autorità di controllo applica il meccanismo di coerenza ex art. 63, il quale recita: «Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione». Tale meccanismo (previsto alla sezione 3 del capo VI del Regolamento) si basa sull'interessamento di un neo istituito comitato europeo per la protezione dei dati (*European Data Protection Board*) organismo dell'Unione dotato di autonomia giuridica e composto dal garante europeo della protezione dei dati e dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro, o dai rispettivi rappresentanti.

contractual clauses), purché non modificate, sostituite o abrogate conformemente alle norme del presente Regolamento.

Il successivo articolo 47, interamente dedicato alle norme vincolanti d'impresa (*binding corporate rules*), testimonia dell'importanza e del ruolo cui questo strumento è assurto nel sistema europeo di trasferimento estero dei dati personali.

I rilievi tratti dalla prassi e dall'uso che di tali clausole è stato fatto sotto la vigenza della Direttiva 95/46/CE hanno fornito lo spunto per formalizzare questo meccanismo, che nella disciplina del Regolamento è stato cristallizzato con la previsione di vincoli e regole specifici, anche di tipo procedurale³².

A tale proposito, si prevede che l'Autorità di controllo competente debba approvare le BCR in conformità al meccanismo di coerenza ex art. 63 del Regolamento (e dunque con parere del nuovo Comitato europeo per la protezione dei dati) purché ricorrano determinate condizioni, e in particolare:

1. che dette clausole siano giuridicamente vincolanti e siano applicabili a tutti i membri interessati del gruppo imprenditoriale, dipendenti inclusi;
2. che dette clausole conferiscano espressamente agli interessati dal trattamento dei diritti azionabili con riferimento allo stesso;
3. che dette clausole soddisfino i requisiti previsti al seguente paragrafo dell'articolo 47³³.

Il paragrafo secondo dell'articolo in parola, dalla lettera a) alla lettera n), elenca infatti un lungo novero di informazioni che le *binding corporate rules* devono necessariamente specificare.

Si tratta, in sostanza, dei requisiti minimi di contenuto previsti per le BCR già enucleati nel passato dal Gruppo Articolo 29, e oggi recepiti normativamente nel contenuto del Regolamento.

Tra di essi troviamo indicazioni in merito alla struttura e alle coordinate di contatto del gruppo imprenditoriale e dei suoi membri; la specificazione dei trasferimenti (e in particolare delle categorie di dati, il tipo di trattamento e le sue finalità, i paesi terzi interessati); la precisazione della natura giuridicamente vincolante, esternamente ed internamente, delle BCR; specificazioni in merito all'applicazione dei

³² F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 110, nota 29.

³³ Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2.

principi generali di protezione dei dati³⁴ e dei diritti dell'interessato in relazione al trattamento, compresi i mezzi per esercitarli³⁵; nonché l'assunzione di responsabilità in capo al titolare o al responsabile del trattamento in caso di violazione delle BCR da parte di un membro interessato del gruppo societario stabilito fuori dall'Unione³⁶.

Ancora, ai sensi della nuova normativa europea le BCR specificano anche le modalità in base alle quali le informazioni sulle stesse vengono fornite all'interessato; le procedure di reclamo, i compiti del responsabile della protezione dei dati designato³⁷; i meccanismi adottati all'interno del gruppo di imprese per garantire la verifica della conformità alle BCR³⁸, quelli per riferire e registrare le modifiche delle norme e infine

³⁴ E specialmente in relazione «alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa». Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera d).

³⁵ Compresi «il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa». Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera e).

³⁶ Salvo l'esonero totale o parziale da siffatta responsabilità qualora il titolare o responsabile del trattamento stabilito nel territorio di uno Stato membro dimostri la non imputabilità dell'evento dannoso al membro interessato non stabilito nel territorio dell'Unione. Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera f).

³⁷ «o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami». Il riferimento al responsabile della protezione dei dati personali designato rimanda all'articolo 35 del Regolamento che regola la valutazione d'impatto sul trattamento dei dati. Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera h).

³⁸ Così come i meccanismi di cooperazione con l'Autorità di controllo per garantire la conformità da parte di ogni membro del gruppo e in particolare la messa a disposizione dell'Autorità dei risultati delle verifiche menzionate (cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera l)) ; nonché quelli per segnalare all'Autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo in un Paese terzo e che potrebbe avere effetti negativi sostanziali sulle garanzie riconosciute dalle BCR (Cfr. Regolamento (UE) 2016/679, articolo 47, paragrafo 2, lettera m)).

la formazione «appropriata» in materia di protezione dei dati posseduta dal personale che accede su base regolare agli stessi.

La circostanza che le *binding corporate rules* debbano soddisfare tutte le *condiciones sine quibus non* di cui si è dato conto, peraltro, non esclude che le compagnie possano richiedere l'approvazione di clausole disegnate sul modello di *data protection* più in linea con le esigenze della propria struttura societaria e dell'attività da essa svolta.

Come rilevato autorevolmente in dottrina, il sistema che si è costruito con questa istituzionalizzazione dello strumento delle BCR si basa sulla «grande scommessa» che i trasferimenti verso Stati terzi avvengano, anche in mancanza di una decisione di adeguatezza, sulla base di una tutela adeguata dei dati personali assicurata dalle società multinazionali sulla base delle proprie clausole passate al vaglio della Commissione³⁹.

L'articolo 48 si occupa di trasferimenti o comunicazioni di dati non autorizzati dal diritto dell'Unione, e dispone più nello specifico in materia di sentenze di un'autorità giurisdizionale - ovvero di decisioni di un'autorità amministrativa - di uno Stato terzo, che disponga il trasferimento o la comunicazione di dati personali.

La norma condiziona il riconoscimento o l'acquisto di un qualsivoglia carattere esecutivo da parte di tale sentenza/decisione all'esistenza di un accordo internazionale (per esempio un accordo di mutua assistenza giudiziaria) in vigore tra lo Stato terzo richiedente e l'Unione europea o un suo Stato membro⁴⁰.

Di massima importanza è il dettato dell'articolo 49 del nuovo Regolamento, che analogamente all'articolo 26 della Direttiva 95/46/CE precisa il regime delle deroghe (accanto alle ipotesi «garanzie adeguate» poc'anzi analizzate) che eccezionalmente legittimano il trasferimento estero dei dati nelle circostanze in cui manchi il livello di tutela adeguato richiesto dal Regolamento⁴¹.

Fatto salvo per il maggior grado di dettaglio delle formulazioni proprio del Regolamento, il sistema derogatorio si rifà fedelmente alle ipotesi elencate tassativamente nella Direttiva. Se non è possibile basare

³⁹ F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 164.

⁴⁰ Vengono naturalmente fatti salvi gli altri presupposti del trasferimento previsti dal capo V.

⁴¹ Ci si riferisce alle ipotesi ordinarie di trasferimenti fondati su una decisione di adeguatezza della Commissione ex articolo 45, a quelli soggetti a garanzie adeguate ex articolo 46 e a quelli basati su norme vincolanti di impresa ex articolo 47.

il trattamento su alcuna delle tre ipotesi ordinarie, né su alcuna delle deroghe di cui al primo paragrafo dell'articolo 49, il trasferimento verso paesi extra UE potrebbe nondimeno essere, infatti, ammesso in forza del paragrafo secondo.

Ciò avviene qualora il trasferimento non sia ripetitivo, riguardi un limitato numero di interessati e sia necessario al perseguimento di interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato⁴².

In tali occasioni il titolare informa comunque l'autorità di controllo e, in aggiunta agli ordinari doveri di informativa, mette l'interessato del trasferimento a conoscenza degli interessi legittimi cogenti perseguiti.

Da ultimo, un'altra rilevante novità è contenuta dall'articolo 50 conclusivo del capo V, rubricato «Cooperazione internazionale per la protezione dei dati personali».

Esso prende le mosse da considerazioni riguardanti la natura dei dati personali e la loro importanza per l'espansione del commercio e della cooperazione internazionale, ed elenca una serie di norme accomunate da finalità di promozione in tal senso⁴³.

Il nuovo articolo 50 del Regolamento dispone dunque che la Commissione e le Autorità di controllo possono adottare, in relazioni ai Paesi terzi e alle organizzazioni internazionali, «misure appropriate»

⁴² In questo caso, il titolare del trattamento deve aver inoltre valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione aver fornito garanzie adeguate relativamente alla protezione dei dati personali. Cfr. Regolamento (UE) 2016/679, articolo 49, paragrafo 2. La casistica derogatoria cui si fa riferimento riguarda, in particolare, i casi in cui: l'interessato abbia esplicitamente acconsentito al trasferimento proposto (previa informazione circa i rischi connessi a trasferimenti di dati in assenza di una decisione di adeguatezza e di garanzie adeguate); il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento (ovvero all'esecuzione di misure precontrattuali su istanza dell'interessato dal trattamento); 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; il trasferimento sia necessario per importanti motivi di interesse pubblico; il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; 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; 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, al concorrere dei requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

⁴³ Si veda in proposito il testo dei Considerando al Regolamento nn. 102 e 116.

per sviluppare la cooperazione internazionale con riferimento ai seguenti ambiti:

1. l'applicazione efficace della legislazione in materia di protezione dei dati personali;
2. la mutua assistenza internazionale sul piano dell'*enforcement* della legislazione a tutela dei dati, segnatamente mediante scambio di informazioni, notificazioni, deferimento dei reclami e assistenza alle attività di indagine;
3. il coinvolgimento degli *stakeholders* nelle discussioni e attività volte a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;
4. la promozione dello scambio e della documentazione in materia di dati personali, in riferimento tanto alle legislazioni che alle prassi e ai conflitti di giurisdizione con Paesi terzi.

Questo attivismo europeo in materia, culminato nella “codificazione” delle citate misure adeguate al perseguimento degli obiettivi di cooperazione internazionale, si presta ad essere letto in diversi modi, anche di segno diametralmente opposto.

Da un lato, i sostenitori della visione dell' “imperialismo normativo” dell'UE saranno orientati a rinvenire, nel dettato dell'articolo 50, un nuovo strumento per cercare di imporre il modello europeo di protezione dei dati personali nel resto del mondo; dall'altro, la nuova previsione normativa potrebbe incarnare invece uno *Zeitgeist* europeo in materia «ancora in bilico fra resistenza ad ogni cedimento sul piano della tutela del diritto, e volontà di aprire strade nuove, che comunque non facciano della protezione dei dati un ostacolo insormontabile allo sviluppo»⁴⁴.

A parere di chi scrive, la norma potrebbe ben rappresentare la volontà dell'Unione di esercitare ancora più saldamente il proprio *soft power* in materia di protezione dei dati personali, facendo leva sull'interdipendenza economica e informativa propria della società globalizzata, in un contesto in cui «*the world most valuable's resource is no*

⁴⁴ F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 165. L'Autore, che pur riconosce l'importanza della previsione dell'articolo 50, esprime tuttavia scetticismo in riferimento all'adeguatezza della stessa all'efficace perseguimento degli scopi che si prefigge.

*longer oil, but data*⁴⁵ (e in cui l'area economica rappresentata dall'Unione europea, di questo nuovo petrolio, è ben fornita)⁴⁶.

Quanto detto non per forza al (solo) fine di promuovere e influenzare l'emanazione di normative straniere plasmate ad immagine e somiglianza di quella europea, ma, ricollegandosi alla autorevole dottrina citata, anche con l'intento di giocare un ruolo di primo piano nella elaborazione e sperimentazione di nuove soluzioni giuridiche che, nel lungo termine, si inseriranno forse sempre più nell'orizzonte dei trattati di diritto pubblico e di altri strumenti convenzionali internazionali⁴⁷.

In conclusione, se il nuovo Regolamento generale sulla protezione dei dati è – a più di venti anni di distanza – la nottola di Minerva che si leva sul far del tramonto della Direttiva del '95, allo stesso modo soltanto il tempo e l'applicazione in concreto della nuova normativa potranno disvelare le prossime tappe di questo interessante viaggio.

⁴⁵ Citazione mutuata da un articolo apparso sull'edizione online dell'*Economist* in data 6 maggio 2017, e intitolato per l'appunto: «*The world most valuable's resource is no longer oil, but data*». L'articolo, che suggerisce lo sviluppo di nuovi approcci in materia di politiche *antitrust* con riferimento ai dati personali, considerati nella loro veste di bene di scambio e risorsa economica, può essere liberamente consultato al seguente link: <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

⁴⁶ Peraltro, tali considerazioni relative alla “proiezione esterna” della *data protection* europea sono riflesse, più in generale, da altre scelte di fondo consacrate nella lettera del nuovo Regolamento in chiave evolutiva rispetto alla disciplina dettata dalla Direttiva 95/46/CE. Su tutte, come rilevato in M. CORLEY, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, in 41 *Brooklin Journal of International Law* (2016), p. 735: «Another major change is the fact that the GDPR explicitly encompasses personal data that is handled outside the EU. The GDPR asserts authority over companies who offer their services to EU citizens and play an active role in the EU market».

⁴⁷ Secondo M. NINO, *Le prospettive internazionali ed europee della tutela della Privacy*, cit., p. 785, il combinato dei principi affermati nella decisione *Schrems* e la giurisprudenza della Corte di Giustizia, insieme all'adozione del nuovo Regolamento 2016/679, sono circostanze che valgono a configurare un articolato modello di tutela della privacy in grado di assurgere a modello in sede internazionale. L'Autore rileva in particolare come, conseguentemente, «l'Unione può svolgere un ruolo chiave e di guida, valorizzando siffatto modello nell'ambito di detti fora, nella prospettiva della costruzione di un regime internazionale di tutela della vita privata e delle informazioni di natura personale (...) sia che si scelga la strada della conclusione di un trattato internazionale (...), sia che gli Stati stabiliscano un modello giuridico internazionale sulla falsariga del modello UNCITRAL». Interessanti spunti sull'argomento provengono anche da M. CORLEY, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, cit.

Matteo Leffi

*I trasferimenti di dati verso Stati terzi
nel nuovo Regolamento UE*

ABSTRACT: Lo scritto muove dal ruolo di primo piano svolto dai trasferimenti di dati nella società contemporanea, e in particolare dall'impatto dei trasferimenti di dati verso stati terzi extra-UE sulla cornice normativa dell'Unione europea in materia di protezione dei dati personali.

Si passano quindi in rassegna le disposizioni dettate dal nuovo Regolamento (UE) 679/2016 in riferimento ai trasferimenti di dati verso Paesi terzi e organizzazioni internazionali, dando conto della *ratio* sottesa a tali previsioni, delle modalità previste per il legittimo trasferimento dei dati, nonché dei principali profili di novità e discontinuità con le relative disposizioni della Direttiva 95/46/CE.

In conclusione, si accennano infine possibili spunti evolutivi, in chiave internazionale, del regime di tutela dei dati personali, anche alla luce della natura intrinsecamente globale delle infrastrutture informatiche per mezzo delle quali enormi quantità di dati sono quotidianamente trasferite.

KEYWORDS: data protection, privacy, trasferimento di dati personali verso stati terzi, GDPR, direttiva 95/46/CE

Matteo Leffi, Praticante Avvocato in Milano,
matteoeffi@gmail.com