FABIO BALDUCCI ROMANO

I trasferimenti di dati personali

SOMMARIO: 1. Cenni introduttivi. – 2. Nozione di trasferimento. – 3. Trasferimento sulla base di una decisione di adeguatezza. – 4. Trasferimento soggetto a garanzie adeguate. – 5. Norme vincolanti d'impresa. – 6. Trasferimento o comunicazione disposti da sentenze o provvedimenti amministrativi di Paesi terzi. – 7. Deroghe in specifiche situazioni. – 8. L'adeguamento del Codice della *privacy*.

1. Cenni introduttivi

L'enorme sviluppo della rete internet e dei servizi della società dell'informazione ha notevolmente incrementato e facilitato la circolazione globale di dati personali.

Secondo recenti statistiche, l'83% della popolazione dell'Europa occidentale accede alla rete, mentre il 48% utilizza i *social network*[1]. A livello nazionale, il 56,1% degli utenti di internet ha utilizzato un *social network* e quasi un terzo ha pubblicato sul web contenuti di propria creazione[2].

I dati personali degli utenti dei servizi della società dell'informazione sono frequentemente trasferiti in paesi extraeuropei, perché i maggiori fornitori di questi servizi sono stabiliti negli Stati Uniti: grazie alla velocità della rete, i dati raccolti in qualsiasi parte del mondo possono essere conservati in *data center* spesso collocati, per comprensibili scelte di natura imprenditoriale, presso gli stabilimenti dei prestatori dei servizi.

Sotto il profilo giuridico, tuttavia, il trasferimento pone evidenti problemi di tutela dei diritti delle persone, poiché i dati esportati ~~trasferiti~~ sfuggono alla giurisdizione dell'Unione e degli Stati membri.

Una volta che i dati sono trasferiti, l'Unione non può controllarne il trattamento: tali dati potrebbero essere utilizzati per finalità difformi rispetto a quelle prestabilite, comunicati a terzi ovvero ritrasferiti verso altri Paesi. Il

---

[1] *Fonte*: We Are Social: *https://www.slideshare.net/wearesocialsg/digital-in-2016.*.

[2] *Fonte*: ISTAT: *https://www.istat.it/it/archivio/176914* (dati relativi al 2015).

singolo soggetto interessato è spesso del tutto inconsapevole del modo in cui i propri dati potranno essere utilizzati dopo il trasferimento. Anche laddove la persona interessata fosse sufficientemente informata, la modificabilità delle norme che riguardano il trattamento di tali dati in un Paese terzo (si pensi alle norme connesse ad esigenze di sicurezza pubblica) e la possibilità che i dati vengano ulteriormente trasferiti verso altri paesi extraeuropei rende completamente imprevedibile la disciplina del trattamento [3].

Il legislatore europeo parte quindi dall'assunto dell'inefficacia degli strumenti di tutela successivi al trasferimento, perché estranei alla propria giurisdizione, e stabilisce una serie di garanzie preventive rispetto al trasferimento.

Le garanzie *ex ante* servono ad assicurare che, di norma, il Paese di destinazione dei dati fornisca agli individui un livello di protezione non solo adeguato, ma sostanzialmente equivalente a quello previsto dal diritto europeo [4].

---

[3] Per un inquadramento del problema giuridico del trasferimento dei dati, v.: A. Mantelero, *From Safe Harbour to Privacy Shield. The "Medieval" Sovereignty on personal data*, in *Contr. e impr./Europa*, 2016, 338 ss.; P. Piroddi, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo Regolamento generale sulla protezione dei dati*, *Dir. inf. e inform.*, 2015, 827 ss.; G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. inf. e inform.*, 2015, 697 ss.; G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al safe harbor agreement?*, in *Dir. inf. e inform.*, 2015, 865 ss.; E.A. Rossi, *Nuovi aspetti ai vecchi problemi in tema di strumenti internazionali sul trasferimento di dati personali*, in *Dir. comunit. e scambi internaz.*, 2016, 75 ss.; F. Rossi Dal Pozzo, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Riv. dir. int.*, 2016, 690 ss.; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Giappichelli, Torino, 2016, p. 89 ss.; M.C. Meneghetti, *Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 423 ss.

[4] In tal senso, Corte giust., sent. 6 ottobre 2015, causa C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, EU:C:2015:650, p.ti 73-74. Tra le note di commento alla sent. *Schrems*, si segnalano: L. Azoulai-~~S.~~M. Van Der Sluis, *Institutionalizing personal data protection in times of global institutional distrust: Schrems*, in *Common Market Law Review*, 2016, 1343 ss.; R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost.*, 2016, 289 ss.; B. Carotti, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa*, in *Giorn. dir. amm.*, 2016, 333 ss.; G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inf. e inform.*, 2015, 779 ss.; A. Giattini, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso Schrems e l'invalidità del sistema di "approdo sicuro"*, in *Dir. umani e dir. internaz.*, 2016, 247 ss.; A Mantelero, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per i cittadini ed imprese?*, in *Contr. e impr./Europa*, 2015, 719 ss.; M. Nino, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Dir. Un. eur.*, 2016, 755 ss.; V. Salvatore, *La Corte di giustizia restituisce (temporaneamen-*

Per questo motivo, come si vedrà, nel ricercare un difficile equilibrio tra circolazione dei dati e protezione dei diritti delle persone, l'ordinamento europeo ha progressivamente spostato l'ago della bilancia verso i diritti degli individui. Tale orientamento non solo appare condivisibile sotto il profilo giuridico, ma sembra anche l'unica via ragionevole, per l'evidente motivo che la circolazione dei dati è talmente vasta e crescente che non ha alcun bisogno di incentivi giuridici.

È presto per affermare se il Regolamento 2016/679 (in seguito «il Regolamento») abbia incrementato e reso più effettive le garanzie a favore degli individui cui si riferiscono i dati. Esso comunque, nel sostituire la direttiva 95/46 (in seguito «la direttiva»), ha cercato di recepire gli insegnamenti provenienti dalla Corte di giustizia che, soprattutto con la sentenza *Schrems*, ha determinato una sostanziale evoluzione del quadro normativo.

Il tema del trasferimento dei dati è di vitale importanza per la protezione dei diritti degli individui, tanto che il Regolamento vi dedica, oltre ai *considerando* da 101 a 116, ben sette articoli, da 44 a 50[5], in luogo dei soli due della direttiva[6].

2. Nozione di trasferimento

Al pari della direttiva, il Regolamento non contiene una precisa definizione di trasferimento di dati personali, né tra le disposizioni generali, né all'interno degli articoli dedicati a tale fattispecie.

È tuttavia agevole rinvenire una definizione nella giurisprudenza della Corte, secondo cui esso costituisce un'operazione di trattamento[7], consisten-

---

te) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti, in *Studi integraz. eur.*, 2015, 623 ss.; G. SCARCHILLO, *Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*, in *Dir. comm. internaz.*, 2016, 901 ss.; V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Dir. inf. e inform.*, 2015, 683 ss.

[5] V. 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 e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), in *G.U.* 4 maggio 2016, L 119, 60-65.

[6] V. direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *G.U.* 23 novembre 1995, L 281, 45-46.

[7] Corte giust., sent. 30 maggio 2006, cause riunite C-317 e 318/04, *Parlamento c. Consiglio e Commissione*, EU:C:2006:346, p.to 56. Sul tema, v.: E. PEDILARCO, *Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei*, in *Dir. pubbl. comp. eur.*, 2006, 1225 ss.; M. SPATTI, *Il trasfe-*

te nel far trasferire dati personali da uno Stato membro verso un Paese terzo [8]. Il Regolamento aggiunge che tale fattispecie ricorre anche nel caso in cui i dati siano destinati ad un'altra organizzazione internazionale [9]. Si dovrebbe tuttavia precisare che non costituisce trasferimento l'invio di dati verso gli Stati aderenti al SEE (o verso tale organizzazione internazionale); infatti, in continuità con quanto già previsto per la direttiva, il Regolamento si applica integralmente nello Spazio Economico Europeo.

In sostanza, il trasferimento è una comunicazione di dati proveniente direttamente dall'interessato ovvero da altro soggetto che stia trattando i dati, quale titolare o responsabile, e diretta ad una persona fisica o ad un ente, pubblico o privato, stabilito al di fuori dell'ambito di applicazione territoriale del Regolamento [10], che conservi i dati stessi o effettui altre operazioni di trattamento ovvero li ritrasferisca verso un altro Paese terzo.

Il problema della definizione, tuttavia, risulta molto complesso per ragioni, al tempo stesso, tecniche e giuridiche. Sotto il profilo tecnico, non è sempre agevole distinguere le operazioni che comportano il trasferimento dei dati fuori dai confini dell'Unione, anche per la natura globale ed immateriale della rete. Sotto il profilo giuridico, l'eccessiva espansione della fattispecie finirebbe per ricomprendere tutti i casi in cui vengano caricati *online* i dati di una persona; per altro verso, l'ampliamento dell'ambito di applicazione territoriale delle norme europee in materia ha ridotto la casistica dei trasferimenti, assoggettando alcune fattispecie all'applicazione piena delle disposizioni del Regolamento [11].

Ciò ha indotto la Corte, a partire dall'ormai storica sentenza *Lindqvist* [12], a ritenere che non costituisca trasferimento l'inserimento, da parte di un soggetto stabilito nell'Unione, in una pagina internet, caricata presso un web hosting provider stabilito nell'Unione, di dati relativi ad altra persona, anche laddove i dati così inseriti divengano accessibili da Paesi terzi.

---

rimento dei dati relativi al passenger name record: gli accordi dell'Unione Europea con Australia e Stati Uniti d'America, in *Dir. comm. internaz.*, 2013, 697 ss.

[8] V. Corte giust., sent. *Schrems*, cit., p.to 45.

[9] V. art. 44 Regolamento.

[10] Si ricorda che, in base all'art. 3, par. 2, sono integralmente soggetti alla disciplina del Regolamento i trattamenti che, pur essendo effettuati da un titolare non stabilito nell'Unione, riguardano l'offerta di beni o la prestazione di servizi, anche se gratuiti, ad interessati che trovino nell'Unione, ovvero il monitoraggio del comportamento degli interessati, nella misura in cui detto comportamento abbia luogo nell'Unione.

[11] Sul tema dell'applicazione territoriale del Regolamento, per un approccio (sin troppo) critico, v. M. GÖMANN, *The new territorial scope of EU data protection law: deconstructing a revolutionary achievement*, in *Common Market Law Review*, 2017, 567 ss.

[12] Corte giust., sent. 6 novembre 2003, causa C-101/01, *Lindqvist*, EU:C:2003:596, p.ti 69-70.

Rispetto all'omologa norma della direttiva, l'art. 44 del Regolamento chiarisce che le disposizioni in materia di trasferimento costituiscono un «regime speciale», come già statuito dalla Corte [13], complementare al «regime generale» relativo alla protezione dei dati personali. Si tratta, in sostanza, di regole aggiuntive, che devono essere rispettate dal titolare e dal responsabile, fatta salva l'applicazione delle altre disposizioni del Regolamento.

Lo scopo, enunciato dalla norma, è evitare che il livello di protezione dei diritti delle persone sia pregiudicato per effetto del trasferimento.

3. Trasferimento sulla base di una decisione di adeguatezza

Il Regolamento consente il trasferimento di dati personali anzitutto nel caso in cui la Commissione abbia accertato che il Paese terzo garantisce un livello di protezione adeguato. In tale ipotesi non è necessaria un'autorizzazione ad hoc.

Rispetto all'omologa disposizione della direttiva, l'art. 45 del Regolamento prevede regole sostanziali e procedurali più precise per le decisioni di adeguatezza da parte della Commissione.

Sotto il profilo sostanziale, il par. 2 individua gli elementi che la Commissione deve esaminare nella valutazione dell'adeguatezza: *i*) in primo luogo, lo stato di diritto ed il livello di rispetto dei diritti fondamentali, nonché la legislazione in materia di protezione dei dati personali; *ii*) in secondo luogo, l'esistenza di un'autorità indipendente con poteri di vigilanza, controllo e decisione dei ricorsi; *iii*) infine, gli impegni internazionali assunti dal Paese terzo in materia di diritto alla protezione dei dati personali, sotto forma di adesione a convenzioni internazionali.

Il tenore letterale della norma, comunque, lascia intendere che si tratti di un elenco non tassativo, per cui la Commissione potrebbe ritenere di attribuire rilevanza anche ad elementi diversi. La disposizione non brilla per precisione, non essendo chiaro se i tre requisiti sopra ricordati debbano essere necessariamente concomitanti, ovvero se si tratti di elementi che, anche singolarmente, possano giustificare l'adozione di una decisione di adeguatezza.

Secondo l'approccio sostanzialistico, applicato dalla Corte all'art. 25 della direttiva, il «livello di protezione adeguato» andrebbe inteso quale effettiva garanzia di un livello di protezione dei diritti fondamentali *equivalente* a quello garantito nell'Unione [14]. La nozione di «equivalenza» è frutto di un'interpretazione giurisprudenziale evolutiva del canone di adeguatezza,

---

[13] V. Corte giust., sent. *Lindqvist*, cit., p.to 63.

[14] V. Corte giust., sent. *Schrems*, cit., p.ti 73-74.

previsto dalla norma. Tuttavia, il legislatore dell'Unione non ha ritenuto di modificare la terminologia, per cui il Regolamento non ha integrato nel testo il concetto di equivalenza.

Inoltre, a differenza di quanto prevedeva l'art. 25 della direttiva, l'art. 45 del Regolamento non contempla, tra gli elementi che la Commissione deve valutare ai fini della decisione di adeguatezza, né la natura dei dati né le finalità del trattamento, e non prevede nemmeno che la decisione sia presa con riferimento a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati.

In altri termini, la Commissione, e soprattutto la Corte di giustizia, dovranno chiarire se vi sia una sostanziale continuità con la direttiva, ovvero se l'oggetto delle decisioni di adeguatezza sia stato mutato per effetto del Regolamento. L'art. 45, infatti, sembra riferire tali decisioni solo alla struttura e alla natura democratica dell'ordinamento giuridico dello stato terzo (o della parte dello Stato terzo ovvero dell'organizzazione internazionale) destinatario del trasferimento.

Sembra comunque che la nuova disposizione, nonostante la diversa formulazione, debba leggersi in continuità con la precedente, poiché la Corte ha chiaramente affermato che la Commissione, per valutare le garanzie offerte da uno stato terzo, deve considerare «tutte le circostanze relative ad un trasferimento di dati personali» [15].

Risulta invece piuttosto chiaro che, per effetto dell'uniformazione normativa introdotta dal Regolamento, gli Stati membri dell'Unione hanno perso il potere di accertare che un Paese terzo assicuri o meno un livello di protezione adeguato [16]. Tale potere, infatti, è stato accentrato all'Unione ed attribuito in via esclusiva alla Commissione. Gli Stati membri potranno eventualmente adire la Corte in via diretta *ex* artt. 263 o 265 TFUE per far accertare l'illegittimità della decisione della Commissione ovvero l'inerzia di quest'ultima [17].

Sotto il profilo procedurale, l'art. 45 regola l'esercizio del potere di decisione della Commissione. Il par. 3 prevede che, laddove la Commissione abbia ravvisato la sussistenza di garanzie adeguate per il trasferimento dei dati in un Paese terzo o in uno o più settori specifici all'interno di un Paese terzo, o in un'organizzazione internazionale, essa può adottare una decisione, secondo la procedura di cui all'art. 93, par. 2 del Regolamento [18]. L'atto deve indica-

---

[15] V. Corte giust., sent. *Schrems*, cit., p.to 75. Si precisa tuttavia che tale statuizione si riferisce all'art. 25, par. 2 della direttiva 95/46/CE, al tempo vigente.

[16] V. Corte giust., sent. *Schrems*, cit., p.to 50.

[17] Cfr. Corte giust., sent. *Schrems*, cit., p.to 51.

[18] Tale disposizione rinvia alla procedura d'esame di cui all'art. 5 del Regolamento UE n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri

re l'ambito geografico di applicazione e l'autorità di controllo competente del Paese terzo, nonché il termine – non più lungo quattro anni – entro il quale la decisione di adeguatezza sarà soggetta a riesame periodico.

Il par. 4 dello stesso art. 45, invece, istituisce una forma di controllo permanente delle condizioni accertate con le decisioni di adeguatezza.

All'esito del riesame periodico o del controllo permanente, la Commissione può adottare un provvedimento con cui revoca, modifica o sospende la decisione di adeguatezza. Tali atti sono, di regola, adottati con la medesima procedura prevista per le decisioni di adeguatezza [19]. In base al par. 6, eventuali consultazioni con il Paese terzo sono avviate soltanto dopo l'adozione della decisione di revoca, modifica o sospensione.

L'eventuale sopravvenienza di una decisione di revoca, modifica o sospensione non impedisce il trasferimento dei dati basato su un diverso fondamento [20].

Per assicurare l'informazione dei cittadini, la Commissione pubblica in *Gazzetta Ufficiale* e sul proprio sito internet istituzionale l'elenco dei paesi terzi destinatari sia delle decisioni di adeguatezza sia di quelle di revoca, modifica o sospensione.

Infine, la norma prevede che le decisioni già adottate dalla Commissione sulla base della direttiva rimangano in vigore sino all'emanazione di nuovi provvedimenti.

4. Trasferimento soggetto a garanzie adeguate

L'art. 46 del Regolamento si applica qualora manchi una decisione di adeguatezza, ovvero qualora sia stato adottato un provvedimento di revoca, modifica o sospensione di tale decisione, per cui il trasferimento non può essere effettuato o non può proseguire sulla base dell'art. 45.

In casi simili, la direttiva prevedeva la possibilità che il responsabile fornisse «garanzie sufficienti» per la protezione della vita privata e dei dati personali, anche sulla base di «clausole contrattuali appropriate». Competeva agli Stati membri la valutazione delle suddette garanzie e l'autorizzazione al trasferimento dei dati. La Commissione, invece, disponeva del potere di adottare clausole contrattuali standard, mediante decisioni obbligatorie per gli Stati medesimi.

---

dell'esercizio delle competenze di esecuzione attribuite alla Commissione, in *G.U.* 28 febbraio 2011, L 55, 15-16.

[19] In caso di urgenza si applica invece la procedura di cui all'art. 8, relativo agli atti di esecuzione immediatamente applicabili del Regolamento UE n. 182/2011, cit.

[20] Cfr. art. 46, par. 1 del Regolamento.

Il Regolamento ha ridenominato le garanzie, ora definite «adeguate» e non più «sufficienti», prevedendo, in linea generale, che esse debbano sempre comprendere diritti azionabili e mezzi di ricorso effettivi.

Le *garanzie adeguate* possono essere fornite da due diversi tipi di strumenti. Il primo tipo si applica a categorie di trattamenti di dati ed è costituito da: *i*) strumenti giuridicamente vincolanti ed esecutivi tra autorità pubbliche o organismi pubblici; *ii*) norme vincolanti d'impresa, di cui si dirà in seguito; *iii*) clausole standard di protezione adottate dalla Commissione; iv) clausole standard di protezione adottate da un'autorità nazionale ed approvate dalla Commissione; *v*) codici di condotta; *vi*) sistemi di certificazione.

Il secondo tipo di strumenti di garanzia adeguata, soggetti ad autorizzazione da parte dell'autorità nazionale competente, riguarda singoli trattamenti ed è costituito da: *i*) clausole contrattuali tra il titolare (o responsabile) del trattamento e l'omologo soggetto del Paese terzo in cui devono essere trasferiti i dati; *ii*) clausole da inserire in accordi tra autorità pubbliche od organismi pubblici.

Rispetto all'iniziale proposta, l'articolo è stato notevolmente modificato, e non tutti gli emendamenti meritano un giudizio favorevole.

In primo luogo, l'ambito di applicazione appare alquanto diverso, perché l'originaria proposta prevedeva che il trasferimento in presenza di garanzie adeguate potesse effettuarsi in assenza di decisioni (di qualsiasi tipo) da parte della Commissione [21]; l'art. 46 del Regolamento, invece, consente di ricorrere a tale fattispecie in mancanza di una decisione di adeguatezza. Il tenore letterale della disposizione sembra quindi consentire il ricorso agli strumenti di «garanzia adeguata» anche in presenza di un provvedimento di revoca, modifica o sospensione della decisione di adeguatezza. Giova, al riguardo, ricordare che una decisione di revoca, modifica o sospensione viene presa sulla base dell'inadeguatezza dell'ordinamento giuridico dello Stato terzo in cui i dati sono trasferiti. Sembra perciò difficile ipotizzare che i diritti degli interessati possano essere sufficientemente protetti in un contesto statuale in cui le libertà fondamentali non sono garantite. Appare quindi ragionevole ricorrere alle «garanzie adeguate» solo se manchi una decisione di adeguatezza relativa al Paese terzo destinatario del trasferimento.

In secondo luogo, l'elenco degli strumenti di garanzia adeguata è stato notevolmente ampliato, sino a comprendere istituti giuridici che difficilmente si prestano a garantire «diritti azionabili» e «mezzi di ricorso effettivi», come i codici di condotta e i meccanismi di certificazione.

---

[21] Cfr. Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), COM/2012/011 final, adottata il 25 gennaio 2012, art. 42.

5. Norme vincolanti d'impresa

L'art. 47 del Regolamento disciplina nel dettaglio lo strumento delle norme vincolanti d'impresa (*corporate binding rules*). Si tratta di un istituto applicabile ai rapporti tra società multinazionali appartenenti al medesimo gruppo, nel caso in cui il trasferimento dei dati avvenga tra una o più affiliate stabilite nell'Unione e una o più società del gruppo, stabilite in un Paese terzo.

Le *corporate binding rules* si riferiscono a categorie di trattamenti di dati personali, o anche a tutti i dati trattati dal gruppo societario; esse devono essere approvate da parte dell'autorità di controllo nazionale competente [22], che deve verificare la sussistenza dei requisiti minimi previsti dalla lunga lista contenuta nel par. 2 dell'art. 47.

In sintesi, occorre un'indicazione della struttura del gruppo societario, dei trattamenti e dei trasferimenti dei dati, con precisazione delle finalità dei trattamenti che verranno effettuati fuori dall'Unione ed identificazione dei paesi terzi in cui i dati saranno trattati. Devono essere altresì indicati i diritti e le garanzie dell'interessato, comprese le informazioni e le procedure di reclamo previste.

Lo strumento tende a responsabilizzare la società stabilita nell'Unione per i trattamenti dei dati trasferiti alle altre società del gruppo, che hanno sede in ~~una~~ un Paese terzo. È comunque ~~tuttavia~~ previsto che il titolare del trattamento stabilito nell'Unione possa essere esonerato anche completamente da tale responsabilità, a condizione che dimostri che l'evento dannoso non è a lui imputabile [23].

Appare tuttavia discutibile la previsione di una simile possibilità di esenzione da responsabilità, perché essa mina le fondamenta dello strumento. Tale esenzione, peraltro, sembrerebbe in netto contrasto con l'orientamento estensivo, assunto dalla giurisprudenza della Corte di giustizia nei confronti ~~delle~~ dei gruppi di imprese multinazionali ~~multifunzionali~~ a proposito della ripartizione delle funzioni tra le società controllate ~~all'interno dei gruppi societari~~, giustificato con lo scopo di garantire una tutela più ampia e completa dei diritti degli interessati [24].

---

[22] V. artt. 63 ss. del Regolamento.

[23] V. art. 47, par. 2, lett. f) del Regolamento.

[24] Da ultima, v.: Corte giust., sent. 5 giugno 2018, causa C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, par. 64, in *Foro it.*, 2018, IV, 361 ss., con nota di commento di R. ~~Pardolesi~~ PARDOLESI e S. ~~Bonavita~~ BONAVITA, 377 ss.; in senso conforme, v. Corte giust., sent. 13 maggio 2014, causa C-131/12, *Google Spain e Google*, EU:C:2014:317, par. 55-56; sul tema, v. G. CAGGIANO, *L'interpretazione del contesto delle attività di stabilimento dei responsabili del trattamento dei dati personali*, in *Dir. inf. e inform.*, 2014, 4-5, 605 ss.

Inoltre, l'efficacia delle norme vincolanti d'impresa dipende dalla stabilità e rigidità che tali regole dovrebbero assumere in seguito all'autorizzazione da parte dell'autorità nazionale di controllo. È infatti evidente che l'eventuale modificabilità unilaterale priverebbe gli interessati di garanzie sufficienti, rendendo peraltro non prevedibili *ex ante* le regole che dovranno sovrintendere al trattamento dei dati [25]. A tale riguardo, il testo del Regolamento non appare del tutto chiaro. Sembra, anzi, che la modificazione delle *corporate binding rules* possa essere soggetta a mera comunicazione all'autorità di controllo, senza necessità di preventiva autorizzazione [26].

Ulteriore elemento di debolezza dello strumento è costituito dalla frammentazione delle competenze autorizzative. In un contesto normativo uniformato per effetto del Regolamento, sarebbe stato preferibile accentrare all'Unione la funzione regolatoria, attribuendo alla Commissione il potere di autorizzare le *corporate binding rules*, e lasciando alle autorità nazionali i poteri di vigilanza e protezione dei diritti delle persone. Si dubita, infatti, che le singole autorità dispongano della capacità di negoziare regole destinate a grandi gruppi multinazionali, il cui potere economico è talvolta superiore a quello degli stessi Stati membri.

6. Trasferimento o comunicazione disposti da sentenze o provvedimenti amministrativi di Paesi terzi

Secondo l'art. 48, i dati personali raccolti da un titolare o responsabile stabilito nell'Unione possono essere trasferiti anche in presenza di provvedimenti dell'autorità giudiziaria o amministrativa di un Paese terzo, a condizione che tali provvedimenti possano fondarsi su un accordo internazionale vigente. La norma si applica alla materia civile ed amministrativa, poiché i trattamenti di dati effettuati per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, sono disciplinati dalla direttiva 2016/680 [27].

---

[25] Di diversa opinione, G.M. Riccio, *Model contract clauses e corporate binding rules*, cit., 878.

[26] Cfr. art. 47, par. 2, lett. k) del Regolamento.

[27] V. direttiva 2016/680/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in *G.U.U.E.* 4 maggio 2016, L 119, 89-131. Tale direttiva è stata trasposta con d.lgs. 18 maggio 2018, n. 51, in *G.U.* 24 maggio 2018, n. 119.

La fattispecie di cui all'art. 48 è caratterizzata da un provvedimento puntuale, una sentenza o una decisione di un'autorità amministrativa, e non può che riguardare specifici dati il cui trasferimento sia necessario, ad esempio, per scopi istruttori.

Si tratta di una disposizione non presente nella direttiva, la cui efficacia andrà vagliata sulla base della casistica applicativa. È infatti evidente che, in mancanza di un accordo internazionale, i provvedimenti dell'autorità giudiziaria o amministrativa di un Paese terzo non sono automaticamente riconosciuti, ma potrebbero essere riconosciuti, ad esempio, sulla base di una procedura di rogatoria internazionale rimessa al ministro della giustizia dello Stato membro in cui la sentenza estera deve essere eseguita. Il testo della nuova disposizione sembra escludere tale eventualità ogniqualvolta debbano essere trasferiti dati personali. È tuttavia agevole osservare che, a stretto rigore, la fattispecie ricorrerà praticamente in tutti i casi di prove (si pensi, ad es., a tabulati telefonici, documenti contabili o fiscali, estratti conto bancari, ecc.) la cui comunicazione venga richiesta da un'autorità giudiziaria straniera. Occorrerà perciò un chiarimento giurisprudenziale, anche al fine di precisare i rapporti tra questa disposizione e quella contenuta nell'art. 49, che consente i trasferimenti di dati sulla base di un importante motivo di interesse pubblico, ovvero per la tutela giurisdizionale dei diritti [28].

7. Deroghe in specifiche situazioni

L'art. 49 contiene un elenco di casi in cui, nonostante la mancanza delle «garanzie adeguate», il trasferimento è consentito a causa della *specifica situazione*.

In particolare, il divieto di trasferimento non si applica qualora l'interessato vi abbia esplicitamente acconsentito, dopo essere stato informato dei relativi rischi, ovvero quando sia necessario per l'adempimento di un contratto tra l'interessato ed il titolare del trattamento ovvero tra quest'ultimo ed un terzo, a condizione che il contratto sia a favore dell'interessato.

Ulteriori deroghe sono previste per motivi di interesse pubblico o per la tutela giurisdizionale di un diritto, ovvero per la tutela di un interesse vitale della persona cui si riferiscono in dati, qualora costui sia incapace di esprimere il proprio consenso.

È altresì prevista la possibilità di trasferire specifici dati contenuti in registri pubblici o destinati all'informazione del pubblico, purché siano rispettate le condizioni previste dalle norme nazionali od europee applicabili al registro medesimo.

---

[28] V. art. 49, par. 1, lett. d) ed e) del Regolamento.

Si tratta di una serie di deroghe, sostanzialmente identiche a quelle già previste dalla direttiva, che – in quanto tali – andranno interpretate in senso restrittivo e secondo proporzionalità.

Merita particolare attenzione il caso del trasferimento in base al consenso dell'interessato, poiché la deroga non risulta espressamente limitata a quanto necessario per il soddisfacimento di un interesse rilevante della persona a cui si riferiscono i dati.

Al riguardo, occorre osservare che, nonostante l'espressa previsione del diritto primario, in base alla quale il consenso costituisce il fondamento del trattamento dei dati [29], il trasferimento dei dati in un Paese terzo – peraltro in mancanza di garanzie adeguate – comporterà sovente l'impossibilità dell'interessato di mantenere il controllo sui propri dati, privandolo di tutti i diritti conseguenti all'avvio del trattamento (quali l'accesso, la rettifica, l'integrazione, e la cancellazione). Per tale motivo, la deroga connessa al consenso della persona interessata dovrebbe essere sottoposta ad accurate limitazioni, relative alla qualità e quantità dei dati e alla finalità del trattamento.

Il Regolamento ha comunque introdotto uno strumento che potrebbe essere utilizzato a questo scopo. Il par. 5 dell'art. 49, infatti, prevede che norme dell'Unione o degli Stati membri possano introdurre limitazioni al trasferimento di categorie di dati in mancanza di una decisione di adeguatezza. Qualora tali limitazioni vengano introdotte nel diritto nazionale, gli Stati membri dovranno notificare alla Commissione le disposizioni adottate.

Tale potere normativo, da esercitarsi mediante atti legislativi, potrebbe, in ipotesi, essere utilizzato per limitare o addirittura vietare il trasferimento di categorie di dati, come i dati sensibili [30], idonei a rivelare informazioni più delicate sulla personalità degli individui a cui si riferiscono.

8. L'adeguamento del Codice della *privacy*

Prima di concludere la trattazione dell'argomento, appare opportuno un breve sguardo al decreto di adeguamento della normativa nazionale.

Come noto, infatti, con d.lgs. 10 agosto 2018, n. 101 [31], il Governo ha attuato la delega prevista dall'art. 13 della legge 25 ottobre 2017, n. 163 [32], adottando disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento. Tale decreto ha abrogato numerose disposizioni del Codice della *privacy* e, per quanto qui interessa, ha abolito l'intero titolo VII

[29] V. art. 16 TFUE.

[30] *Rectius*, le categorie particolari di dati personali di cui all'art. 9 del Regolamento.

[31] In *G.U.* 4 settembre 2018, n. 205.

[32] In *G.U.* 6 novembre 2017, n. 259.

della parte I, rubricato «*Trasferimenti dei dati all'estero*» [33].

Sembra peraltro che tale scelta sia perfettamente coerente con la natura giuridica ed il contenuto del Regolamento, che non lascia alcun margine di discrezionalità agli Stati membri in proposito, occupando l'intera materia del trasferimento dei dati personali.

[33] Artt. da 42 a 45 del d.lgs. 30 giugno 2003, n. 196, in *G.U.*, serie gen., ~~39~~ 29 luglio 2003, suppl. ord. n. 123.