SAPIENZA
UNIVERSITÀ DI ROMA

Facoltà di Giurisprudenza

Dipartimento di Scienze Giuridiche

Dottorato in Autonomia privata, impresa, lavoro e tutela dei diritti nella prospettiva europea ed internazionale - XXX Ciclo

Curriculum in Diritto Commerciale Comparato e Uniforme

Le clausole Binding Corporate Rules nei contratti per la circolazione transnazionale dei dati tra multinazionali alla luce del nuovo regolamento europeo 2016/679.

Relatore:

Chiar.mo Prof. Guido Alpa

Candidato:

Andrea Cosma Mortati

A.A. 2017/2018

Una volta il tempo diventa un solo punto, e il secondo dove sei uguale a te stesso è pari all'esplosione di una supernova…

Indice

Ringraziamenti

Sono molte le persone che desidero ringraziare per avermi aiutato a realizzare questo mio lavoro.

Al mio maestro, il Professor Guido Alpa, desidero rivolgere il ringraziamento più sentito. Per avermi concesso il privilegio e l'onore di essergli stato accanto in questi anni, per avermi dato la possibilità di imparare da lui, per la sua sempre pronta disponibilità, per il suo gentile esempio, per ogni parola o consiglio ricevuto, per avermi insegnato il fascino e la bellezza della ricerca nel diritto e per ogni preziosa perla lasciata lungo il mio cammino.

Ringrazio profondamente il Professor Andrea Biondi, per avermi permesso di frequentare la biblioteca del Kings College e l'Institute of Advanced Legal Studies of London: il mio lavoro non sarebbe stato di altrettanto pregio senza le occasioni di ricerca offertemi.

Uno speciale ringraziamento va al Professor Pierre De Gioia - Carabellese che mi ha introdotto alla Heriot-Watt University of Edinburgh, e che ha supervisionato il mio lavoro in questi ultimi cinque mesi, dandomi la possibilità di immergermi e respirare a trecentosessanta gradi la vita e la ricerca dell'accademia d'oltre manica, non mancando in nessuna occasione di offrirmi efficaci consigli ed un eccellente esempio di serietà e dedizione allo studio e alla ricerca.

Un immenso grazie all'Avvocato Rocco Panetta, per avermi accolto nel Suo Studio e per avermi permesso un'eccellente occasione di crescita professionale ed una proficua e critica panoramica di taglio pratico sull'argomento.

Manuela Laurent, Responsabile della Biblioteca dell'Istituto di Diritto Comparato ove ho trascorso la maggior parte di questi anni di studio e ricerca, che sempre mi ha offerto la sua consulenza e tutta la sua professionalità, soprattutto nell'utilizzo dei vari programmi di ricerca, per la buona riuscita del mio lavoro: non potrò mai ringraziarla abbastanza.

Le Dottoresse Sabina Kirschen e Clizia D'Agata ed il Dottor Riccardo Sanchini, che mi hanno accolto e fatto sentire "un giovane collega" presso il Garante della privacy, con la loro serietà e la loro passione si sono distinti per gentilezza, competenza e professionalità, offrendomi impareggiabili spunti per lo sviluppo del mio lavoro.

I Colleghi e compagni di stanza Luca Aglitti e Aurora Rasi, dottorandi di diritto internazionale, sono stati di fondamentale importanza per tutte le occasioni di scambio e arricchimento: è infatti, incalcolabile il valore di un brillante confronto di idee tra chi guarda il mondo del diritto da prospettive diverse.

Ringrazio ancora quanti mi hanno accompagnato lungo questo mio percorso e quanti non hanno mai smesso di credere in me.

Introduzione

Il diritto alla protezione dei dati personali[1] è considerato un diritto fondamentale sia dalle fonti nazionali che da quelle sovranazionali. Nel corso dell'ultimo ventennio tuttavia, la sua tutela rischiava di subire una contrattura a causa dell'imponente sviluppo che ha avuto la dematerializzazione e la digitalizzazione dei dati personali. Tale fenomeno ha fatto sì che i dati personali subissero dei costanti e veloci trasferimenti da un server ad un altro il più delle volte posizionati in paesi differenti e quindi soggetti a differenti normative sul trattamento dei dati personali. Fortunatamente, il Legislatore comunitario non si è fatto trovare impreparato dinanzi a questa sfida che, oltre a coinvolgere gli appartenenti all'Unione Europea, si estende su un piano mondiale.

Nel corso di questa trattazione, si porrà l'accento su una particolare tipologia di trasferimento dei dati personali, ossia il traffico dei dati che intercorre tra le società di una medesima multinazionale, dislocate in paesi diversi, che abbiano ad oggetto i dati dei loro dipendenti e dei loro clienti.

Il problema principale che ha investito questa tipologia di trasferimenti, era rappresentato dalle differenti legislazioni con cui le multinazionali dovevano confrontarsi al momento del trasferimento dei dati, qualora protagonista del trasferimento medesimo fosse stata una multinazionale che doveva far elaborare i suoi dati ad una sua società dislocata fuori dai confini europei. Ci si trovava di fronte dunque ad una sorta di *patchwork legislativo* che limitava fortemente il dialogo tra il titolare e il responsabile del trattamento.

Sul punto infatti, le disposizioni comunitarie contenute nel Direttiva 95/46 stabilivano che un trasferimento di questo tipo poteva trovare applicazione, solo allorché lo stato di destinazione presentasse delle garanzie di tutela per il diritto alla protezione dei dati personali che rispettassero gli standard presenti all'interno della Comunità Europea. Qualora così non fosse, continuava la Direttiva, il trasferimento dei dati personali poteva avere luogo solo qualora i soggetti che ponevano in essere il trasferimento e il trattamento dei dati fornissero delle adeguate garanzie per la tutela del diritto alla protezione dei dati personali.

[1] www.garanteprivacy.it: sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Si necessitava dunque di uno strumento atto a risolvere due ordini di problemi: assicurare le adeguate garanzie di tutela e oltrepassare l'ostacolo del *patchwork legislativo.*

Tale strumento è rappresentato dalle *Binding Corporates Rules – BCR* (Norme Vincolanti d'Impresa).

Si tratta di uno strumento rappresentato da clausole contrattuali (*rules*) che, fissando i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*), garantiscono adeguate tutele e permettono di regolare i rapporti tra le diverse parti contrattuali alla luce di un'unica disciplina legislativa.
Ovviamente, come si è sostenuto in apertura di trattazione, l'evoluzione digitale ha fatto sì che anche le BCR subissero un'evoluzione per assolvere con efficienza al loro compito di tutela del diritto alla protezione dei dati personali.

Tuttavia, più che di evoluzione dello strumento in sé, è più corretto parlare di evoluzione nell'utilizzo che tale strumento ha subito. Le BCR, infatti, seppur disciplinate in maniera superficiale nella Direttiva 95/46, hanno assunto un ruolo centrale nella elaborazione dei pareri e nell'interpretazione delle disposizioni che riguardano il diritto alla tutela dei dati personali da parte del Gruppo di lavoro articolo *ex* art. 29 (Working Party article 29 di seguito anche "WP 29", "Gruppo di lavoro" o "Gruppo").

Per il WP 29[2], le BCR, sono state considerate lo strumento che più efficacemente di ogni altro riesce a fornire una tutela completa ed efficace dei dati personali dei soggetti interessati al trattamento.
L'attenzione per le BCR mostrata dal Gruppo di lavoro e la contestuale importanza da esse assunta nel panorama europeo, hanno indotto il Legislatore europeo a darne una più compiuta disciplina nel Regolamento europeo n. 679 del 27 aprile 2016 (di seguito "Regolamento" o "GDPR").

Tale Regolamento è l'espressione della predetta sensibilità che l'Unione Europea dimostra circa la tutela di un diritto fondamentale quale il diritto alla protezione dei dati

[2] **A. Pisapia**, "*La tutela per il trattamento e la protezione dei dati personali*", Giappichelli Editore, 2018, p. 19: "Considerando che la conoscenza e l'utilizzo dei dati personali potesse costituire la base per un trattamento discriminatori, o comunque il trattamento potesse ledere diritti fondamentali dell'individuo, l'art. 29 della Direttiva 95/46 aveva previsto l'istituzione di un Gruppo di lavoro, con carattere consultivo e indipendente, per la protezione dei dati personali".

personali. Particolare attenzione è inoltre rivolta, a quei casi in cui il trasferimento dei dati interessi paesi terzi[3] (extra-europei).

Nel corso di questa trattazione ci si muoverà attraverso queste due distinte discipline per comprendere come le BCR rappresentino lo strumento che garantisce efficacemente questa tutela. Si analizzeranno i requisiti che le predette clausole devono presentare per far sì che la tutela sia effettivamente garantita.

Infine, saranno oggetto di trattazione gli oneri contrattuali delle parti che sottoscrivono tali clausole, e le responsabilità che derivano in caso di un loro mancato rispetto.

[3] Cfr. WP document 12 e WP document 254;www.zerounoweb.it: "Recentemente l'Article 29 Data Protection Working Party (WP29), nel documento "WP254", ha fornito indicazioni sulla cosiddetta "decisione di adeguatezza" stabilendo principi generali con l'ottica di guidare i paesi terzi a valutare la propria aderenza ai principi stabiliti dal GDPR: l'adeguatezza può essere raggiunta attraverso una combinazione di diritti per gli interessati e obblighi nei confronti di coloro che trattano i dati o che ne esercitano controllo".

CAPITOLO I: Il diritto alla protezione dei dati personali

§ 1. Le fonti: uno sguardo d'insieme

Nell'odierno periodo storico, la dematerializzazione e la digitalizzazione delle informazioni ha assunto un'importanza sempre maggiore.

In questo contesto, il ruolo di preminenza rappresentato dai dati personali si esplica, fra gli altri, nella loro libera circolazione. Data la loro importanza (e la loro possibile connotazione "di dati particolari" o c.d. "*dati sensibili*"[4])[5] è doveroso assicurare ai medesimi un alto grado di protezione per il loro utilizzo e conseguentemente per la loro circolazione[6]. Sebbene l'importanza di assicurare un ampio livello di protezione si sia accentuata nell'ultimo ventennio a seguito dell'avvento delle nuove tecnologie, i Legislatori nazionali ed il Legislatore europeo già dalla seconda metà del secolo scorso hanno sentito l'esigenza di intervenire con delle normative volte a proteggere le informazioni sensibili dei singoli individui.

[4] www.garanteprivacy.it: "[…] dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici e i dati biometrici; […] Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.";
Cfr. WP Document 131: Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE) 15 febbraio 2007 - WP 131.

[5] Fra i più importanti provvedimenti del Garante della Privacy circa il trattamento dei dati "sensibili" vedi:
- **Autorizzazione generale n. 1/2016** al trattamento dei dati sensibili nei rapporti di lavoro
15 dicembre 2016; Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale 15 dicembre 2016; Autorizzazione generale n. 3/2016 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;15 dicembre 2016 Autorizzazione generale n. 4/2016 al trattamento dei dati sensibili da parte dei liberi professionisti 15 dicembre 2016;
- **Autorizzazione generale n. 5/2016** al trattamento dei dati sensibili da parte di diverse categorie di titolari 15 dicembre 2016; Autorizzazione generale n. 6/2016 al trattamento dei dati sensibili da parte degli investigatori privati 15 dicembre 2016; Autorizzazione generale n. 7/2016 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici;15 dicembre 2016;
- **Autorizzazione generale n. 8/2016** al trattamento dei dati genetici 15 dicembre 2016; Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica 15 dicembre 2016.

[6] Per una dettagliata disamina dei provvedimenti di autorizzazione del Garante della Privacy al trasferimento dei dati personali presso Paesi Terzi da parte di "Gruppi Societari" è possibile consultare la pagina web www.garanteprivacy.it.

Aprendo il discorso proprio con le fonti del diritto sulla protezione dei dati personali, possiamo rilevare che tale diritto alla protezione della sfera privata[7] di un individuo dalle ingerenze altrui, soprattutto da parte dello stato, è stato per la prima volta sancito nel 1948 nella Dichiarazione Universale dei Diritti dell'Uomo[8] al cui art. 12 si dispone: *"Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni"*.

Con l'istituzione del Consiglio d'Europa[9] poi, al fine di promuovere i diritti dell'uomo e lo sviluppo sociale, nel 1950 è stata adottata la Convenzione europea dei Diritti dell'Uomo (CEDU), entrata poi in vigore nel 1953. Nello studio introduttivo che si sta conducendo, una particolare attenzione merita l'art. 8[10] della citata Carta, il quale al primo comma sancisce un principio similare a quanto previsto dall'art. 12 della Dichiarazione Universale dei Diritti dell'Uomo, poiché sottolinea il diritto di ciascun individuo al rispetto della sua riservatezza nei medesimi termini dell'art. 12, cioè nella sua vita privata, familiare, nel suo domicilio e della sua corrispondenza. Tuttavia, al secondo comma[11], l'art. 8 CEDU disegna un confine oltre il quale è possibile che il diritto in questione, subisca una contrattura a fronte di ingerenze da parte della pubblica autorità solo ed esclusivamente nei casi in cui si realizzino due presupposti, cioè che la limitazione del diritto alla riservatezza dei dati personali sia prevista dalla legge, da un

[7] Si tratta di un diritto particolarmente complesso, difficile ed esigente per una molteplicità di ragioni. Innanzitutto perché, coinvolgendo onore e reputazione, tocca la sfera più intima e sensibile della dignità umana, interpella cioè il valore dei valori dell'intera costruzione giuridica dei diritti umani. Allo stesso tempo, la sua protezione e la stessa interpretazione dei suoi contenuti deve confrontarsi con l'evoluzione di una tecnologia sempre più pervasiva e invasiva e con le esigenze, sempre più impellenti, della sicurezza sociale e collettiva, interna e internazionale.

[8] A Parigi, il 10 dicembre 1948, l'Assemblea Generale delle Nazioni Unite approvò e proclamò la Dichiarazione Universale dei Diritti Umani. Il testo ufficiale della Dichiarazione è disponibile nelle lingue ufficiali delle Nazioni Unite, cioè cinese, francese, inglese, russo e spagnolo.

[9] Il Consiglio d'Europa (CdE) fu fondato il 5 maggio 1949 con il Trattato di Londra. Esso è un'organizzazione internazionale il cui scopo è promuovere la democrazia, i diritti umani, l'identità culturale europea e la ricerca di soluzioni ai problemi sociali in Europa. E' composta da 47 stati membri di cui 28 appartenenti all'Unione Europea.

[10] Articolo 8, comma primo, Carta EDU: <<Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza>>.

[11] Articolo 8, comma secondo, Carta EDU: <<Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui>>.

lato, e che sia il precipitato di un'attività necessaria al fine di garantire la sicurezza nazionale, il benessere economico del paese, la difesa dell'ordine, la prevenzione dei reati; ovvero la protezione della salute, della morale e la tutela dei diritti e delle libertà altrui, dall'altro.

Come si è anticipato, l'emergere delle nuove tecnologie ha determinato un crescente bisogno di norme sempre più dettagliate al fine di garantire un'adeguata tutela dei dati personali degli individui. Così, a partire dagli anni Settanta, il Comitato dei Ministri del Consiglio d'Europa ha adottato diverse soluzioni in materia di protezione dei dati personali proprio sull'impulso fornito dall'art. 8 CEDU. Essendo il diritto alla *privacy* annoverabile tra i diritti fondamentali dell'individuo, è emblematico rilevare come gli interventi in materia, abbiano toccato tutti i contesti nei quali tale diritto si rintraccia. Un esempio può essere rappresentato dalla Risoluzione emanata dal Comitato di cui sopra, adottata il 20 Settembre 1974[12], nella quale si raccomanda a tutti i Governi degli Stati membri di adottare soluzioni che possano garantire la tutela del diritto alla riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico.

Tuttavia, il primo intervento che più di ogni altro sottolinea l'importanza che ha raggiunto la protezione dei dati personali è rappresentato dalla Convenzione numero 108[13] redatta dal Consiglio d'Europa e aperta alla firma nel 1981, la quale si pone come

[12] RISOLUZIONE DEL CONSIGLIO (74) sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico (Adottata dal Comitato dei Ministri il 20 settembre 1974 durante la 236ma riunione dei Delegati dei Ministri) **R(74)** del 20 settembre 1974 in Council of Eur *Commitee of Ministers, Recommendations and Resolutions*, 1973.

[13] Cfr. Protocollo che aggiorna la Convenzione 108. "Dopo un lungo iter iniziato nel 2011 è stato portato a termine dal Comitato dei ministri del Consiglio d'Europa, il processo di modernizzazione della Convenzione 108 del 1981 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali.
L'adozione formale è avvenuta in occasione della Ministeriale di Elsinore il 18 maggio scorso. Il Protocollo che ha emendato, aggiorna la Convenzione 108, è aperto alla firma dal 25 giugno 2018, in occasione della sessione dell'Assemblea Parlamentare del Consiglio d'Europa.
La modernizzazione della Convenzione 108, che è tuttora l'unico strumento sulla protezione dei dati vincolante a livello internazionale, risponde alle molte sfide intervenute negli anni per l'avvento delle nuove tecnologie, assicurando la tenuta dei principi della Convenzione e rafforzandone i meccanismi per la sua effettiva implementazione.
Il Protocollo garantisce standard elevati in una cornice normativa flessibile che facilita la loro adozione da parte di un ampio numero di Paesi, inclusi quelli che non fanno parte del Consiglio d'Europa. Costituisce, inoltre, un ponte tra i diversi approcci regionali, incluso il Regolamento (UE) 2016/679 (pienamente applicabile dal 25 maggio 2018) che colloca l'adesione da parte di Paesi terzi alla Convenzione 108 tra i criteri da considerare nella valutazione di adeguatezza di tali Paesi nel contesto dei trasferimenti dei dati. Il Protocollo contiene diverse novità rispetto all'originario. In particolare: il rafforzamento degli obblighi di trasparenza a carico dei titolari del trattamento; l'ampliamento dei diritti degli interessati, che ora racchiudono anche il diritto a non essere soggetto a decisioni puramente automatizzate e a conoscere la logica del trattamento; maggiori garanzie per la sicurezza dei dati, incluso l'obbligo di notificare i *data breach*, e di assicurare un approccio di *privacy by design*. Il Protocollo rafforza inoltre i compiti delle

l'unico strumento internazionale giuridicamente rilevante in materia di protezione dei dati personali rispetto al trattamento automatizzato degli stessi, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa[14].

Tale Convenzione, ratificata in Italia con L. n. 98 del 1989, oltre allo scopo di protezione degli individui dall'uso abusivo del trattamento automatizzato disciplina ovviamente anche il flusso transfrontaliero dei dati.

Oltre alle garanzie previste per il trattamento automatizzato dei dati di carattere personale, essa bandisce il trattamento dei dati "delicati"[15] sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale, le condanne penali, in assenza di garanzie previste dal diritto interno. Inoltre, la Convenzione garantisce anche alle persone di conoscere le informazioni catalogate su di loro e ad esigere, se del caso, delle rettifiche[16].

Infine, il dato caratteristico di questa Convenzione, che di fatto apre alla necessità di utilizzo delle BCR, attiene al fatto che questa impone delle limitazioni ai flussi transfrontalieri dei dati personali verso i paesi ove non esiste alcuna adeguata protezione equivalente.

Riservandoci di analizzare successivamente le caratteristiche della citata Convenzione[17], possiamo rilevare una volta di più, come per l'importanza della materia oggetto di trattazione questa sia aperta all'adesione anche di stati non membri del Consiglio d'Europa, compresi dunque paesi extraeuropei.

Si noti quindi che la portata della Convenzione n. 108 come standard universale e il suo carattere aperto potrebbero costituire un presupposto per promuovere la protezione dei dati a livello mondiale[18].

Autorità di protezione dati e del Comitato della Convenzione, chiamato a svolgere un ruolo nella valutazione dell'effettivo rispetto dei principi della Convenzione che deve essere assicurato dai Paesi che ne faranno parte" in *www.gpdp.it*.

[14] Si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che pubblico, e quindi anche ai trattamenti effettuati da polizia e autorità giudiziaria. La normativa mira a proteggere gli individui da abusi e regolamentare i flussi transnazionali dei dati, e trae diretta inspirazione dall'articolo 8 della Convenzione europea dei diritti dell'uomo. L'articolo 1 recita: *<<Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano (protezione dei dati)>>.* Cfr.https://protezionedatipersonali.it/convenzione-108-consiglio-europa.

[15] Sul punto si veda meglio Nota 4.

[16] www.coe.int

[17] V. *par. 2*.

[18] Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, Belgium 2014.

A livello strettamente europeo, il primo passo che segna definitivamente l'importanza e l'attenzione che le istituzioni sovranazionali rivolgono alla tutela del diritto in questione si ha nel 1995 con la Direttiva numero 46 CE[19] la quale, essendo definita "Direttiva Madre", diviene il testo di riferimento in materia di protezione dei dati personali.

Con questo intervento, la Comunità europea ha introdotto un complesso sistema di regole che devono governare i trattamenti, anche non automatizzati, dei dati personali. Pertanto, la Direttiva delinea i confini entro i quali è ammessa la raccolta e l'utilizzo dei medesimi ed inoltre, impone agli Stati membri di istituire al loro interno un organismo indipendente che sia incaricato della protezione di tali dati. In Italia questo è avvenuto con l'istituzione del Garante per la protezione dei dati personali con l.n. 675 del 1996[20] (c.d. *legge sulla Privacy*). A ciò, sempre a livello interno, ha fatto seguito l'emanazione del Codice della Privacy approvato con D.lgs. n. 196 del 2003[21], il quale ha inoltre prodotto l'abrogazione della l. n. 675 del 1996.

Ancora a livello comunitario, prima di giungere ai fondamentali TUE e TFUE, occorre segnalare un ulteriore Regolamento e due Direttive intermedie. Il primo, il Regolamento n. 45 del 2001[22], concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali, da parte degli organismi e delle istituzioni comunitarie, nonché la libera circolazione dei dati stessi. Ha fatto seguito poi la Direttiva n. 58 del 2002[23], la quale, stabilisce la necessità che gli Stati membri pongano in essere un lavoro di armonizzazione della legislazione interna relativamente al trattamento dei dati personali nel settore delle comunicazioni elettroniche.

---

[19] 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.

[20] A seguito delle successive modifiche e rettifiche, la l. n.675/96 fu oggetto di "consolidamento ad opera del d.lgs. 28 dicembre 2001, n. 467- (Pubblicato sulla Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - Suppl. Ordinario n. 3) La Legge fu abrogata ai sensi dell'articolo 183, comma 1, lettera a), del "Codice in materia dei dati personali" del 2003.

[21] Il Testo Unico riunisce la normativa vigente in materia accumulatosi dal 1996, fu ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione degli adempimenti sostituendo la precedente normativa (legge 31 dicembre 1996, n. 675).

[22]Il Regolamento n. 45 del 2001 è stato elaborato il 18 dicembre 2000 e pubblicato il successivo 12 gennaio 2001. Esso è entrato in vigore il ventesimo giorno successivo alla data di pubblicazione nella Gazzetta Ufficiale, ossia il 1° febbraio 2001.

[23] La Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) è stata pubblicata in Gazzetta Ufficiale n. L 201 del 31/07/2002.

Infine, nel 2006, sempre nel contesto delle comunicazioni elettroniche venne emanata la Direttiva numero 24[24] che oltre a modificare la precedente, ha disciplinato la conservazione dei dati, generati o trattati, nell'ambito della fornitura di tali comunicazioni.

Si noti che il dato caratteristico di quest'ultimi tre interventi, attiene al fatto che in tutti si risente la forte influenza della "Direttiva Madre" al punto di ripercorrerne i passaggi salienti e riprodurne diverse parti[25].

Ad oggi, la consacrazione del diritto alla tutela dei dati, come diritto individuale della persona è presente, come prima anticipato in due norme del Trattato di Lisbona 2009: l'art. 6 TUE (Trattato sull'Unione Europea)[26] e l'art. 16 TFUE (Trattato sul funzionamento dell'Unione Europea)[27].

Il primo stabilisce che: *"L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo […]. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. […] I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali".*

Simbolico è il riconoscimento dei medesimi diritti garantiti dalla Carta di Nizza[28] del 2000 tra i quali vi è la protezione dei dati personali di cui all'art. 8.

---

[24] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (No longer in force, Date of end of validity: 08/04/2014).

[25] Per un'analisi approfondita della "Direttiva Madre", *v. par. 3*.

[26] Il Trattato di Lisbona è stato firmato il 13 dicembre 2007 ed è entrato ufficialmente in vigore il 1° dicembre 2009.

[27] Il Trattato sul Funzionamento dell'Unione europea (TFUE), da ultimo modificato dall'articolo 2 del trattato di Lisbona del 13 dicembre 2007 e ratificato dall'Italia con legge 2 agosto 2008, n. 130, su G.U. n. 185 dell'8-8-2008 - Suppl. ordinario n. 188 è accanto al trattato sull'Unione europea (TUE), uno dei trattati fondamentali dell'Unione europea (UE).

[28] La Carta di Nizza, è stata solennemente proclamata una prima volta il 7 dicembre 2000 a Nizza e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione. La *Carta di Nizza* ha il medesimo valore giuridico dei trattati, ai sensi dell'art. 6 del Trattato sull'Unione europea, e si pone dunque come pienamente vincolante per le istituzioni europee e gli Stati membri e allo stesso livello di trattati e protocolli ad essi allegati, come vertice dell'ordinamento dell'Unione europea. Essa risponde alla necessità emersa durante il Consiglio europeo di Colonia (3 e 4 giugno 1999) di definire un gruppo di diritti e di libertà di eccezionale rilevanza e di fede che fossero garantiti a tutti i cittadini dell'Unione.

A ciò poi si aggiunge l'art. 16 del TFUE, in base al quale: *"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*

Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea".

In esso è sostanzialmente previsto che il rispetto e la protezione dei dati personali sia garantito e soggetto al controllo di Autorità indipendenti.

Concludendo il discorso introduttivo sul quadro normativo sovranazionale, che ha portato al riconoscimento e alla tutela della riservatezza dei dati personali, occorre accennare al nuovo progetto presentato dalla Commissione Europea nel gennaio del 2012. Si tratta del "pacchetto protezione dati": produzione normativa che ha lo scopo di garantire un quadro coerente ed un sistema complessivamente armonizzato in materia di protezione dati all'interno dell'UE.

Tale pacchetto si componeva di due testi, una proposta di Regolamento, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico, e destinata a sostituire la Direttiva n. 46 del 1995 e una proposta di Direttiva[29],indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali[30].

[29] La Direttiva (UE) 2016/680 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 abroga la decisione quadro 2008/977/GAI del Consiglio. È da sottolineare a riguardo che l'Italia ancora non ha attuato la testé citata Direttiva.

[30] L'iter per l'approvazione definitiva dei due nuovi strumenti normativi ha comportato l'intervento congiunto di Parlamento europeo e Consiglio UE in base alla procedura detta di "co-decisione" (ora definita dal Trattato di Lisbona "procedura legislativa").
Il 18 dicembre 2015 è stato raggiunto un accordo sul testo del Regolamento e della Direttiva. V. il comunicato del Consiglio europeo del 18 dicembre 2015.
Il 14 aprile 2016 la plenaria del Parlamento Europeo ha adottato in seconda lettura i testi di Regolamento e Direttiva come approvati dal Consiglio. V. comunicato stampa del 14 aprile 2016.

Per il discorso che stiamo affrontando, particolare attenzione merita il primo testo, rappresentato dall'odierno Regolamento n. 679 del 2016[31] diventato, di recente, il 25 maggio 2018, definitivamente applicabile in via diretta in tutti i Paesi membri dell'UE.

§ 2. Gli *"attori"* ed i *"fattori"* nel trattamento dei dati personali: precisazioni terminologiche.

Al fine di comprende in modo chiaro e completo, le vicende che ruotano attorno al trattamento dei dati personali, attraverso le norme di origine comunitaria che regolano questo processo all'interno dei confini dell'Unione, e soprattutto, al fine di valutare l'importanza che le clausole contrattuali BCR ricoprono nel contesto della tutela dei dati in questione (quando il trattamento investe stati che non assicurano un adeguato livello di protezione), occorre fornire una definizione puntuale di chi siano i soggetti che operano in questo settore e a cosa corrispondono le operazioni che questi pongono in essere.

L'importanza di questo quadro definitorio si rinviene già da una prima analisi delle principali normative (comunitarie) di settore, poiché possiamo rilevare come questo ha subito un'evoluzione dalla "Direttiva Madre" al Regolamento n. 679 del 2016, ora ampliando talune definizioni, ovvero fornendone di nuove su elementi in precedenza non considerati.

A questo scopo assolve l'art. 2 della Direttiva 95/46 e l'art. 4 del Regolamento n. 679 del 2016. Per disegnare questo quadro evolutivo, partiremo dalla base fornita dalla prima norma sopra citata, alla quale aggiungeremo gli interventi operati con la seconda.

Entrambi gli articoli si aprono con la definizione di "dato personale", indicato alla *lett. A)* come "*qualsiasi informazione concernente una persona fisica identificata o identificabile, persona interessata; si considera identificabile la persona che può essere*

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini. V. il comunicato stampa del 4 maggio 2016.
Il 5 maggio 2016 è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni. Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018. Vedi il comunicato stampa del 24 maggio 2016. In *www.garanteprivacy.it*.

[31] 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.

identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"[32], la novità introdotta dall'art. 4 del Regolamento n. 679 del 2016 e che ovviamente risulta condizionato dal progredire della tecnologia, attiene al fatto che l'identificazione si possa avere anche attraverso un identificativo *on-line*[33].

Le norme proseguono poi con la definizione di "trattamento" alla *lett. b)* dell'art. 2 della Direttiva 95/46 e al *par.2* dell'art. 4 del Regolamento n. 679 del 2016, in questo caso, si può rilevare una esatta ripetizione definitoria che fa salvo il senso del disposto anche alla luce di alcune modifiche terminologiche. Pertanto il trattamento è definito 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"*[34].

Dal confronto dei due articoli in parola è possibile evincere una mancanza di corrispondenza in quanto alla *lett. c*) la Direttiva 95/46 definisce cosa si debba intendere per "Archivio", mentre, nel Regolamento n. 679 del 2016, prima di definire ciò, si rinvengono ulteriori tre (nuove) definizioni che non trovano riscontro all'interno della Direttiva medesima.

Le nuove definizioni introdotte dal Regolamento sono le seguenti:

1. limitazione di trattamento: *il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;*

2. profilazione: *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali,*

[32] Cfr. Art. 2, par. 1 lett. a) della 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.

[33] Cfr. Art 4, par. 1 lett. a) del 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.

[34] Regolamento n. 679 del 2016 art. 4 par.2.

gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

3. pseudonimizzazione: *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*.

Soltanto al *par.6* dell'art. 4 del Regolamento si rinviene la definizione di "Archivio" che ricalca esattamente quella contenuta nel predetto articolo della Direttiva di raffronto, pertanto con tale termine si intende, *qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*.

A questo punto le due disposizioni continuano con la definizione dei soggetti che pongono in essere le operazioni di trattamento dei dati personali ai quali si rinvia *infr*a. Premesso ciò, si giunge al *par. 10* dell'art. 4 del Regolamento n. 679 del 2016 che, nel definire il "Terzo", ossia "*la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile",* si rifà alla Direttiva 95/46.

Discorso diverso invece per ciò che attiene al "Consenso dell'Interessato", il quale alla *lett. h*) dell'art. 2 della Direttiva 96/46 viene definito come "*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento"*. Mentre il rispettivo *par. 11* dell'art 4 del Regolamento n. 679 del 2016, ne dà una più precisa definizione, "*si tratta di qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".*

Ora, prima di giungere alle fondamentali definizioni dei soggetti che operano nel sistema di trattamento dei dati personali, è necessario porre l'attenzione sulla considerevole evoluzione intervenuta nel disciplinare la materia della protezione dei dati personali che si evince dalle definizioni ulteriori, che il Regolamento n. 679 del 2016, a differenza della Direttiva 95/46 introduce.

Poiché è possibile notare che l'art. 4 del Regolamento presenta quindici ulteriori nozioni, le quali sono:

1. violazione dei dati personali: *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati";*

2. dati genetici: *"i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione";*

3. dati biometrici: *"i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici";*

4. dati relativi alla salute: *"i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute";*

5. stabilimento principale:

a. "per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale";

b. "con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento";

6. rappresentante: *"la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi*

dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento";

7. impresa: *"la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica";*

8. gruppo imprenditoriale: *"un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate";*

9. norme vincolanti d'impresa: *"le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più Paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune";*

10. autorità di controllo: *"l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51";*

11. autorità di controllo interessata: *"un'autorità di controllo interessata dal trattamento di dati personali in quanto:*

a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c. un reclamo è stato proposto a tale autorità di controllo;

12. trattamento transfrontaliero*:*

a. "trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b. "trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro";

13. obiezione pertinente e motivata: *"un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente Regolamento, oppure che l'azione prevista*

in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati, e ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione";

14. servizio della società dell'informazione*: "il servizio definito all'articolo 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio";*

15. organizzazione internazionale: *"un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati".*

A questo punto della trattazione, occorre analizzare l'aspetto che, oltre ad essere il più importante, è quello che alla luce delle traduzioni operate per rendere fruibili i testi della Direttiva e del Regolamento in parola ha portato con sé considerevoli errori di traduzione che hanno dato luogo a forti dubbi interpretativi.

Ci si riferisce al problema derivante dalle definizioni fornite per responsabile e incaricato del trattamento, alla luce dell'art. 2 della Direttiva 95/46 (rispettivamente *lett. d*) e *lett. e*), e quelle di titolare e responsabile del trattamento fornite rispettivamente dai *Parr. 7* e *8* dell'art. 4 del Regolamento n. 679 del 2016.

Se si leggono tali definizioni la Direttiva stabilisce che il responsabile è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario".*

Mentre l'incaricato è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento".*

Se si sposta l'attenzione dalla parte del Regolamento, questo definisce il titolare del trattamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i*

criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"; mentre per responsabile del trattamento si intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*.

Ad una prima lettura dei due testi normativi è possibile evincere due sostanziali differenze che possono destabilizzare l'operatore del diritto che si trova a doverle interpretare. In primo luogo sembra che il Regolamento abbia sostituito la figura dell'incaricato con quella del responsabile, e in secondo luogo che i compiti della figura del responsabile abbiano subito un totale ribaltamento, ossia da colui che determinava le finalità e i mezzi del trattamento dei dati personali (secondo la Direttiva 95/46), a colui che esegue materialmente il trattamento dei dati personali (secondo il Regolamento n. 679 del 2016).

Per dirimere ogni (giustificato) dubbio interpretativo dunque, è necessario rifarsi ai due testi normativi redatti in lingua originale (inglese), poiché colui che nella Direttiva 95/46 assumeva la qualifica di *Controller,* soggetto preposto alla determinazione delle finalità del trattamento, alla luce del Regolamento n. 679 del 2016 rispecchia sempre le medesime caratteristiche e qualifiche.

Lo stesso discorso vale per il *Processor,* colui che trattava (alla luce della Direttiva) e tratta (alla luce del Regolamento) i dati personali.

Dunque, in definitiva, notando la carenza nel testo italiano del Regolamento del termine "incaricato del trattamento" è possibile concludere che la confusione interpretativa deriva semplicemente da un errore di traduzione, poiché con responsabile del trattamento si intenderà sempre colui che tratta i dati personali secondo le disposizioni fornite dal titolare del trattamento, il quale sarà sempre colui che determina le finalità e i mezzi di trattamento dei dati personali.

Infine, l'ulteriore soggetto che fa parte delle operazioni di trattamento dei dati personali è il "Destinatario". Si tratta di una figura la cui definizione non ha subito una modificazione dal passaggio dalla Direttiva (art. 2 *lett. g*) al Regolamento (art. 4 *par. 9*), poiché per destinatario si intende in ambo i casi "*la persona fisica o giuridica, l'Autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le Autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento*

di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento".

§ 2.1. Gli obblighi generali del titolare e del responsabile del trattamento

Sulla base della grande importanza che ha assunto la protezione del diritto alla tutela dei dati personali durante il loro trasferimento e trattamento, per dovere di completezza, un ultimo aspetto che merita di essere analizzato è quello che riguarda la responsabilità del titolare e del responsabile del trattamento[35].

L'evoluzione che ha avuto questo diritto, si respira anche dall'importanza che ha assunto questo aspetto nel Regolamento n. 679 del 2016 rispetto alla Direttiva 95/46. Sul punto occorre rilevare che la Direttiva dedica solo una disposizione, peraltro al quanto povera di contenuti in merito gli obblighi ed alle responsabilità.

Dalla lettura dell'art. 23 della Direttiva 95/46 si evince che gli "*Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della Direttiva medesima abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento* (alla luce dell'analisi operata nel paragrafo precedente, per una corretta interpretazione della norma, è necessario sostituire durante la lettura, il termine responsabile con titolare del trattamento), *il quale può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile"*.

Appare dunque evidente che una tale disposizione non fissi gli obblighi che il titolare del trattamento (e il responsabile) debba rispettare per non incorrere in violazioni che diano luogo a risarcimento del danno.

Tale lacuna legislativa viene colmata dal Regolamento, il quale fissa in due distinte disposizioni le responsabilità del titolare e del responsabile del trattamento, rispettivamente agli artt. 24 e 28[36] del GDPR.

---

[35] Per una completa trattazione dell'argomento si veda il Capitolo IV in merito all'*accountability*.

[36] Circa il titolare del trattamento, l'art. 24 del Regolamento n. 679 del 2016 dispone che:
"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado

di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento".
Mentre, il responsabile del trattamento dovrà rispettare gli obblighi di cui all'art. 28 del Regolamento n. 679 del 2016, secondo il quale: *"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.*
2 Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3 I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a)tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.
4 Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale

§ 3. La "Direttiva Madre" 95/46 e il "Gruppo di lavoro *ex* art. 29" in riferimento delle B.C.R.

§ 3.1. I principi fondamentali della "Direttiva Madre"

Come abbiamo anticipato, la Direttiva 95/46, costituiva il testo di riferimento in materia di protezione dei dati personali e assumeva un ruolo fondamentale anche nella determinazione della libera (e sicura) circolazione dei dati all'interno dell'Unione Europea. Sotto questo aspetto, nel testo della Direttiva furono fissati limiti precisi per la raccolta e l'utilizzazione dei dati personali da un lato, dall'altro, si prescriveva a carico di ciascuno Stato Membro di istituire un organismo nazionale indipendente, incaricato della sorveglianza di ogni attività associata al trattamento dei dati personali[37].

Sebbene la Direttiva in parola si riferisse a tutti gli aspetti che riguardano il trattamento di dati personali e il loro trasferimento, per la specificità di questa trattazione, appare superfluo analizzare in modo approfondito tutti questi aspetti. Pertanto ci limiteremo a fornire i lineamenti che possano descrivere i principi che hanno ispirato il documento e quindi comprendere le ragioni che con esso hanno limitato i trasferimenti verso "paesi terzi" che non garantivano un elevato livello di protezione.

---

conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
5 L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.
6 Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.
7 La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
8 Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.
9 Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10 Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente Regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione ".
[37]eur-lex.europa.eu

Ripercorrendo il testo della Direttiva si è più volte evinto che questa imponesse agli Stati membri di adottare misure volte a garantire "*la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali*" (art. 1 paragrafo 1). Inoltre allo stesso tempo si vietava la contrazione della libera circolazione dei dati personali all'interno dell'Unione Europea (art. 1 paragrafo 2).

L'ambito applicativo della Direttiva, lo si rinveniva nel trattamento, automatizzato, dei dati personali e di quelli contenuti in archivi non automatizzati (ad esempio differenti dalle banche dati informatiche). Era escluso invece nell'ambito del trattamento effettuato da una persona fisica durante l'esercizio di attività a carattere strettamente personale e domestico, ovvero nel contesto ove venissero poste in essere tutte quelle attività che non rientrano nel campo di applicazione del diritto comunitario, come ad esempio la pubblica sicurezza, la difesa e la sicurezza dello Stato (art. 3).

Una volta chiarito che lo scopo della Direttiva fosse quello di tutelare la riservatezza dei dati personali e allo stesso tempo garantire, un loro rapido e dinamico spostamento da uno Stato membro all'altro (procedimento che viene definito trattamento), occorre analizzare i principi in essa enunciati che hanno fatto da parametro di liceità di questo trattamento ed i criteri chiave che lo hanno legittimato.

L'art. 6, disponeva che i dati personali devono essere trattati alla luce di finalità già determinate e non in contrasto con l'ordinamento interno degli Stati e che la qualità dei dati raccolti doveva essere in linea con la finalità che il medesimo trattamento intendeva perseguire. Infine, una volta operata la raccolta dei dati in questione, questi dovevano essere conservati in modo da consentire l'identificazione delle persone interessate per un lasso di tempo non superiore a quello necessario per arrivare alle finalità per cui il trattamento era stato disposto, e qualora i dati fossero stati conservati oltre questo termine, gli stessi Stati dovevano fornire tutte le garanzie necessarie volte a dimostrare un'adeguata protezione di questi dati per finalità storico-statistiche.

Anch'esso fondato sui caratteri di liceità e legittimità del trattamento dei dati, l'art. 7 sanciva che il trattamento doveva essere disposto dagli Stati membri solo quando la persona interessata avesse manifestato il proprio consenso in maniera inequivocabile, ovvero il trattamento fosse necessario al fine dell'esecuzione di un contratto concluso con la persona interessata, oppure di misure precontrattuali assunte su richiesta del soggetto medesimo.

La legittimità del trattamento, era rinvenibile anche nel caso in cui fosse necessario adempiere ad un obbligo legale al quale era soggetto il responsabile del trattamento, oppure quando il trattamento fosse stato teso a salvaguardare un interesse vitale della persona interessata.

Infine, l'articolo concludeva, prevedendo la legittimazione del trattamento in ordine al perseguimento di un legittimo interesse del responsabile del trattamento, ovvero dei terzi a cui venissero comunicati i dati. L'ipotesi descritta tuttavia, risultava temperata dal fatto che gli interessi, i diritti o le libertà fondamentali della persona interessata non fossero messi a repentaglio.

Per dovere di completezza occorre rilevare che suddetti caratteri di liceità e legittimità del trattamento, oltre ai criteri chiave che lo distinguono, si rinvengono anche negli articoli del nuovo Regolamento del 2016 n. 679, i quali sono enunciati agli artt. 5 e 6[38].

[38] Cfr. Art. 5 del GDPR "Principi applicabili al trattamento di dati personali":
1.I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distribuzione o dal danno accidentale (integrità e riservatezza).
2 Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»);
e l'art. art. 6 del GDPR - Liceità del trattamento:
1.Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

In ordine poi ai principi fondamentali, abbiamo notato come l'art. 3 della citata Direttiva, si limitava a delineare solo l'ambito di applicazione materiale, per altro confermato dal Regolamento all'art.2[39], al quale, nel nuovo documento comunitario, fa

---

e) 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;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.
2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a) dal diritto dell'Unione; o
b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.
La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.
4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione".

[39]Cfr. art. 2 del GDPR – "Ambito di applicazione materiale"
1.Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento non si applica ai trattamenti di dati personali:
a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

seguito una demarcazione anche di carattere territoriale, poiché all'art. 3 del Regolamento del 2016 n. 679 stabilisce che il GDPR si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, prescindendo dal fatto che il trattamento sia effettuato o meno nel territorio dell'Unione.

Il citato articolo 3, al paragrafo 2 prescrive ancora l'applicazione del GDPR ai trattamenti dei dati personali degli interessati che si trovano nell'Unione, posti in essere da titolari o da responsabili del trattamento che non sono stabiliti nel territorio dell'Unione, specificando che tale prescrizione si ha quando le attività di trattamento hanno ad oggetto l'offerta di beni o la prestazione di servizi ai suddetti interessati, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure quando il trattamento posto in essere dai suddetti titolari o responsabili abbiano ad oggetto il monitoraggio del comportamento degli interessati nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Infine l'obbligo di applicazione del GDPR lo si rinviene sempre in forza del citato articolo 3 ai trattamenti dei dati personali effettuato da un titolare del trattamento che non è stabilito nel territorio dell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

---

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
3.Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.
4.Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva".

§ 3.2. Il trasferimento dei dati verso Paesi terzi: gli artt. 25 e 26 della Direttiva 95/46. L'operatività delle B.C.R. per fornire le "garanzie adeguate"

In ordine al trattamento dei dati personali che le multinazionali compiono, il ruolo fondamentale in questo scenario, è sicuramente rappresentato da trasferimenti dei dati da una filiale sita in un determinato stato ad una che si trova in uno diverso.

Ovviamente, considerato il grande sforzo operato dalla normativa di derivazione comunitaria che si è succeduta nel tempo, suddetto trasferimento da uno Stato membro all'altro risulta agevole e dinamico proprio in ragione di un comune standard di tutela di cui l'Unione Europea si è dotata.

Il problema e le criticità maggiori si rinvengono invece, allorché un'impresa debba operare un trasferimento dati in un paese terzo e che per di più non presenta un adeguato livello di protezione dei dati personali. Prima di guardare alle soluzioni, elaborate nella Direttiva Madre, occorre rilevare cosa si intende per trasferimento. Ebbene, questo concetto non è affatto sviscerato né tantomeno definito dalle fonti europee (e conseguentemente da quelle nazionali di recepimento). Le quali si limitano a vietarne con assoluta determinatezza il verificarsi, salvo il ricorrere di ben precise condizioni.

Per trasferimento del dato ad esempio, può ben intendersi la comunicazione di informazioni afferenti al personale dipendente fra le sedi italiane o comunque europee e sedi estere di un gruppo multinazionale strutturato[40].

Abbiamo accennato come la "migrazione" del dato dal territorio europeo a quello estero ingenererebbe rischi collegati alla mancata applicazione delle norme e delle tutele individuate dalla normativa europea, con la pericolosa conseguenza che i dati solo per il fatto di circolare al di fuori del territorio europeo sarebbero di fatto sprovvisti delle idonee garanzie preposte a loro tutela.

In questo senso, gli artt. 25 e 26 della Direttiva 95/46 hanno chiarito rispettivamente quali sono i principi che hanno regolano il trasferimento di dati verso paesi terzi sino alla data del 24 maggio scorso, ovvero quali siano state le deroghe che questi abbiano subito sino a tale date.

[40] Documento Digitale: *APPLICAZIONE DELLE BCR: DAL WORKING PARTY ART.29 LE INDICAZIONI*, marzo 2015, di **Valentina Frediani.**

L'art. 25 delineando i suddetti principi, stabiliva la possibilità per gli Stati membri di poter disporre il trasferimento verso un paese terzo di dati personali, oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento, soltanto se il paese terzo interessato dal trasferimento fosse dotato di strumenti legislativi tali da poter garantire un livello di protezione adeguato, fatte salve le misure nazionali delle altre disposizioni contemplate nella Direttiva Madre.

La suddetta adeguatezza di protezione richiesta a carico della legislazione del paese terzo, era vagliata con particolare attenzione alle circostanze relative al trasferimento o ad una categoria di trasferimenti di dati; nello specifico venivano considerate la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di destinazione del trasferimento, nonché le misure di sicurezza e le regole professionali ivi osservate.

Il dettato dell'art. 26 nel suo continuo descriveva e disciplinava l'*iter* di comunicazioni tra gli Stati membri e la Commissione qualora, a loro parere, un paese terzo non garantisse un livello di protezione adeguato ai sensi del paragrafo 2. In tal caso, qualora la Commissione constatasse, secondo quanto previsto dalla procedura dell'articolo 31, paragrafo 2, che un paese terzo non fornisse idonei livello di tutela ai sensi del paragrafo 2 dell'articolo in parola, gli Stati membri erano tenuti ad adottare le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.

Al verificarsi di tali eventi la Commissione avviava, secondo quanto previsto dall'articolo di cui si discorre, i negoziati per rimediare alla situazione risultante dalla constatazione prevista al paragrafo 4 dell'art. 25 della Direttiva Madre.

La Commissione quindi, al fine di dare effettiva tutela ai diritti di protezione della vita privata o delle libertà fondamentali della persona, verificava il citato livello di garanzie avendo riguardo della legislazione o degli impegni internazionali, con rilevante attenzione a quelli assunti in seguito ai negoziati di cui al paragrafo 5 dell'art. 25 della Direttiva Madre. Tale verifica, i cui esiti erano volti a dare impulso agli Stati membri affinché i medesimi adottassero le necessarie misure per conformarsi alle decisioni della Commissione, avveniva mediante secondo quanto previsto dalla procedura *ex* art. 31 paragrafo 2 di cui si è detto.

Ovviamente, questi principi, volti a garanzia dei trattamenti dei dati personali all'interno dell'Unione Europea, si sono scontrati con le necessità di ordine pratico che si rinvengono nelle operazioni che svolgono le multinazionali che, ovviamente, essendo

queste spesso caratterizzate da una dislocazione territoriale extra europea, è chiaro quindi, che per svolgere le loro operazioni di trasferimento, necessitano in non pochi casi di allocare fuori dai confini europei i dati in questione. Pertanto, qualora questa allocazione fosse avvenuta all'interno di un contesto extracomunitario, privo dell'adeguato livello di tutele di cui si è detto, allora trovava applicazione l'art. 26[41] della Direttiva 95/46.

Sulla base del discorso che stiamo conducendo, il punto focale su cui si vuole porre l'attenzione è rappresentato da quanto disposto nel Paragrafo 2 dell'art 26, poiché mediante tale norma, le multinazionali accedevano al trasferimento e alla trattazione dei dati personali anche in paesi terzi privi di un adeguato livello di protezione. Ciò a patto che le medesime, nel disporre il trasferimento fossero in grado di fornire adeguate garanzie mediante apposite clausole contrattuali.

Le suddette clausole contrattuali o anche note con l'acronimo di BCR (*Binding Corporate Rules*), previste prima nella Direttiva Madre, ora nel GDPR, assolvono al

[41] Cfr. ARTICOLO. 26 della direttiva 45/96. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:
a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.
Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.
Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.
In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo 31, paragrafo 2.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
Qualora la Commissione decida, secondo la procedura di cui all'articolo 31, paragrafo 2, che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al paragrafo 2, gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

suddetto compito, creando le condizioni affinché il diritto alla tutela dei dati personali di un cittadino di uno Stato membro sia garantito anche in paesi ove tale diritto potrebbe essere violato da una legislazione nazionale non adeguata.

Si tratta quindi, di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato membro verso paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo d'impresa. Le BCR si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*)[42].

L'importanza della tutela di questo diritto, si rinviene anche alla luce delle elaborazioni fornite dal Working Party art. 29 Dir. 95/46.

Uno dei contributi fondamentali del suddetto *Working Party* è rappresentato dal documento rivisto il 22 Maggio 2015 intitolato *"Explanatory Document on the Processor Binding Corporate Rules"*[43].

Questo documento individua due tipologie di BCR: le BCR *for Controllers* e le BCR *for Processors.* Esse si riferiscono rispettivamente (secondo la nomenclatura della Direttiva) alle clausole contrattuali che deve rispettare il responsabile del trattamento ovvero quelle redatte per l'incaricato del trattamento.

Circa le prime il WP29 chiarisce che si tratta di clausole, intese a regolare i trasferimenti dei dati personali che, in origine, sono trattati dallo stesso *Controller* (indicato come "responsabile" nella Direttiva Madre e come "titolare" nel GDPR) presso una sede diversa del medesimo. La peculiarità attiene al fatto che assolvono ad una duplice funzione, a seconda delle necessità, poiché da un lato possono obbligare in sede di destinazione ad assicurare degli standard di tutela già presenti presso il *Controller* del trattamento originario, ovvero possono introdurre un adeguato sistema di garanzie che mancava sin dall'inizio.

Discorso diverso invece per le BCR *for Processors,* le quali sono uno strumento che, regolando sempre i trattamenti e i trasferimenti internazionali fuori dai confini dell'UE, si riferisce ad operazioni definibili di *"secondo grado"*, in quanto i dati originariamente trattati (all'interno dell'UE) da un *processor* (indicato come "incaricato" nella Direttiva Madre e come "responsabile" nel GDPR) del trattamento per conto del *Controller*, vengono trasferiti ad un ulteriore *(sub) processor* al di fuori dei confini sopra citati.

---

[42] www.garanteprivacy.it

[43] Cfr. Working Party article 29,*"Explanatory Document on the Processor Binding Corporate Rules",* adottato il 19 aprile 2013ma rivisto il 22 maggio 2015, WP n. 204 rev. 1.

Alla luce di questo intervento possiamo sottolineare, una volta di più, come sulla scia di consentire una libera circolazione del dato, soprattutto in favore dei gruppi multinazionali collocati in diversi paesi del mondo, il modello contrattuale elaborato è rappresentato dalle c.d. *Binding Corporate Rules.*

Il divieto al trasferimento viene pertanto superato, attraverso la previsione in un unico documento contrattuale, vincolante per le diverse società appartenenti al medesimo gruppo, secondo quanto predisposto nei modelli elaborati dal Working Party article 29.

Anche se tali elaborati non hanno forza di legge, il loro contenuto viene assiduamente seguito ed applicato dai Garanti europei nella concessione delle autorizzazioni nazionali al trasferimento, nonché nell'interpretazione della normativa. Non soltanto le BCR costituiscono la *privacy policy* delle multinazionali in materia di trasferimenti e trattamenti fuori dall'UE dei dati personali, ma potrebbero, e di fatto questo accade, essere elevate a strumento di policy riguardante i trattamenti generalmente intesi effettuati dall'impresa stessa.

Sul contenuto, gli elaborati prodotti sono molteplici. Dall'elaborato del WP29 n. 74 del 3 giugno 2003 fino al n. 154 del 24 giugno 2008 che costituisce un modello esemplificativo della costruzione di un testo adeguato di BCR: tutti individuano i requisiti e gli elementi che dovranno essere previsti od implementati dalle aziende. Innanzitutto, lo strumento contrattuale di BCR adottato dovrà essere reso vincolante per tutte le società facenti parte della compagine societaria del gruppo. Tale efficacia potrà ben essere conferita mediante molteplici strumenti: contratti infragruppo, dichiarazioni rilasciate o impegni assunti unilateralmente dalla controllante che siano vincolanti per tutti i membri, obblighi contenuti nei documenti statutari, integrazione delle norme in materia di protezione dei dati personali all'interno dei principi aziendali dell'organizzazione, sostenute da politiche, controlli e sanzioni adeguati[44].

[44] Documento Digitale: *APPLICAZIONE DELLE BCR: DAL WORKING PARTY ART.29 LE INDICAZIONI*, marzo 2015, di **Valentina Frediani**.

§ 3.3. Il Working Party art. 29, Direttiva 95/46. Il WP114: "Working document on a common interpretation of Article 26 of Directive 95/46"

Il Working Party article 29, era un organo consultivo e indipendente il cui compito fondamentale era rappresentato dalla formulazione di pareri e raccomandazioni su qualsiasi questione riguardante la tutela dei dati personali all'interno dell'UE.

Ovviamente il problema della tutela dei dati personali si acuisce allorché questi vengano trasferiti e trattati al di fuori dei confini comunitari. Pertanto, si rinviene la necessità di valutare se il livello di protezione fornito dai paesi terzi sia adeguato rispetto agli standard europei.

Le elaborazioni del Working Party article 29 si riferiscono principalmente all'interpretazione che doveva essere data degli artt. 25 e 26 della Direttiva 95/46 sino al 24 maggio (e che tracciano le linee guida nell'interpretazione degli artt. 46 e 47 del GDPR, di cui *infra*), i quali come abbiamo visto attengono ai profili dinamici dei dati personali; tuttavia, prima di valutare questi interventi occorre chiarire quali siano stati i profili caratteristici di questo organo (anch'esso cessato di esistere con il 25 maggio 2018 ed è stato sostituito dall'EDPB, ossia dall'European Data Protection Board)[45].

Secondo l'art. 29 della Direttiva 95/46, il Gruppo aveva carattere consultivo e indipendente. Esso era composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della o delle autorità create

[45] www.edpb.europa.eu. E' il vero organo europeo titolare del compito fondamentale di garantire la applicazione del Regolamento europeo: è chiamato a controllare che le Autorità nazionali applichino correttamente la nuova regolazione europea. Di conseguenza ha cessato la sua attività *il Working Party art*.29, istituito dall'art.29 della Direttiva 46/95 CE, che per più di venti anni ha svolto una eccezionale attività di coordinamento e supporto tra le Autorità nazionali, per consentire una applicazione più uniforme possibile delle leggi nazionali in vigore fino alla piena attuazione del GDPR. Il Working Party non aveva dignità di soggetto autonomo, anche se la Direttiva ne garantiva la indipendenza. Dopo la entrata in vigore del GDPR, il 25 maggio 2016, il WP29 ha fatto un lavoro eccezionale di preparazione, producendo un elevato numero di pareri e Linee guida relative ai concetti e agli istituti più innovativi della nuova Regolazione. Dobbiamo dunque essere molto grati al WP29 per l'enorme lavoro svolto e per il grande patrimonio di costruzione giuridica accumulato in questi anni. Una attività che spesso lo ha portato ad avere una influenza determinante anche sull'attività della Commissione e sui rapporti tra UE e paesi terzi, primi fra tutti gli Stati Uniti. Il nuovo Comitato europeo per la protezione dei dati (EDPB) ha poteri e compiti molto più ampi, in coerenza con quelli assegnati alle Autorità di controllo dal nuovo GDPR. Esso è il perno essenziale del nuovo sistema dei rapporti tra le Autorità di controllo nazionali, regolato dai principi di cooperazione e coerenza disciplinati nel Capo VII del GDPR e la sua importanza sistemica è facilmente comprensibile. Il Regolamento richiede una attuazione uniforme su tutto il territorio dell'Unione ma, allo stesso tempo, consente ampi poteri alle Autorità nazionali, sia in materia di codici di condotta che di certificazioni. Inoltre esse sono chiamate ad adottare Linee guida in molti settori.

per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione. Ogni membro del Gruppo era designato dall'istituzione oppure dalla o dalle autorità che rappresentava. Qualora uno Stato membro avesse designato più autorità di controllo, queste procedevano alla nomina di un rappresentante comune. Lo stesso valeva per le autorità create per le istituzioni e gli organismi comunitari. Il Gruppo adottava le sue decisioni a maggioranza semplice dei rappresentanti delle Autorità di controllo. Eleggeva il proprio presidente il cui mandato era di due anni con la possibilità di rinnovo.

Alla nomina del segretariato del gruppo provvedeva la Commissione europea. Il Gruppo era dotato di autonomia regolamentare ed esaminava le questioni iscritte all'ordine del giorno predisposto dal suo presidente, su iniziativa di questo o su richiesta di un rappresentante delle autorità di controllo oppure su richiesta della Commissione.

Circa i compiti che era chiamato ad assolvere il Working Party art. 29, questi erano sanciti nel successivo articolo 30 e ricomprendevano:

(i) l'esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della Direttiva Madre per contribuire alla loro applicazione omogenea;

(ii) formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi;

(iii) consigliare la Commissione in merito a ogni progetto di modifica della Direttiva Madre, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che avessero potuto incidere su tali diritti e libertà;

(iiii) formulare pareri circa i codici di condotta elaborati a livello comunitario.

L'articolo appena citato, stabiliva al secondo paragrafo, che il Gruppo era tenuto ad informare la Commissione, qualora avesse constatato che tra le legislazioni o prassi degli Stati membri si fossero manifestate divergenze tali da pregiudicare l'equivalenza della tutela delle persone in materia di trattamento dei dati personali nella Comunità.

Nel terzo paragrafo invece veniva sancita la possibilità per il Gruppo di formulare di propria iniziativa raccomandazioni, trasmesse poi alla Commissione e al Comitato richiamato all'articolo 31 della Direttiva Madre, su qualsiasi questione riguardante la tutela delle persone nei confronti del trattamento di dati personali nella Comunità.

La Commissione mediante una relazione, oggetto poi di pubblicazione, trasmessa anche al Parlamento europeo e al Consiglio, era tenuta ad informare il Gruppo circa il seguito da essa dato ai pareri e alle raccomandazioni pervenute dal Gruppo medesimo. Al Gruppo spettava ancora il compito di redigere una relazione annuale sullo stato della tutela delle persone fisiche con riguardo al trattamento dei dati personali nella Comunità e nei paesi terzi. Tale relazione, oggetto anche di pubblicazione, era poi trasmessa alla Commissione, al Parlamento europeo e al Consiglio.

Una volta chiariti i caratteri e i compiti del WP 29, possiamo analizzare come i suoi interventi siano stati oltremodo necessari, al fine di chiarire le criticità e le discordanze che si potevano rinvenire nella Direttiva 95/46 alla luce dei sopracitati artt. 25 e 26.

Dalla lettura dei due articoli appena richiamati, si può cogliere una differenza di regole sul trasferimento dei dati personali che ha potuto di certo mettere l'interprete in difficoltà dando adito ad incomprensioni. Se si analizzano le due norme si noterà come da un lato l'art. 25 parr. 1 e 6 e l'art. 26 par. 2 mirassero a salvaguardare un adeguato livello di tutela dei dati una volta trasferiti nel paese di destinazione. Quindi detti trasferimenti potevano avvenire sia perché il quadro giuridico del paese terzo verso cui il trasferimento era rivolto prevedeva una protezione adeguata, o perché tale protezione era garantita da clausole contrattuali standard o da altri tipi di garanzie adeguate, come la conclusione di un contratto al cui interno erano presenti dei riferimenti alle BCR.

Dall'altro lato invece, si possono rinvenire una seconda serie di disposizioni contenute nell' art. 26 par. 1, che prevedevano delle modalità molto meno gravose per trasferire i dati personali in un paese terzo. Poiché alla luce della formulazione normativa, il *Controller* del trattamento, non era tenuto ad assicurarsi che il destinatario fornisse una protezione adeguata, non avendo tra l'altro neanche bisogno di ottenere alcun tipo di autorizzazione preventiva per il trasferimento dalle autorità competenti, sempre che tale procedura risultasse applicabile alla luce delle varie ipotesi considerate nella norma di cui si discorre.

Pertanto, la formulazione letterale della Direttiva ben avrebbe potuto condurre alla conclusione che vi fosse una notevole mancanza di coerenza nelle due disposizioni sui trasferimenti di dati personali presso paesi terzi. Infatti, la logica del principio di protezione adeguata, sancito dall'articolo 25 parr. 1 e 6 e dall'art. 26 par. 2, consisteva nel garantire che gli individui continuassero a beneficiare dei diritti e delle libertà fondamentali che ad essi erano concessi in relazione al trattamento dei loro dati

all'interno dell'Unione Europea, anche quando questi dati fossero stati trasferiti in un paese terzo. Inoltre questo gruppo di disposizioni mirava ad impedire che la protezione fornita dalla legislazione europea in materia di protezione dei dati personali venisse di fatto aggirata proprio mediante il trasferimento dei dati personali verso paesi terzi.

Principio questo che risulterebbe assente da una prima lettura dell'art. 26 par. 1 Dir. 95/46.

La spiegazione di questa apparente lacuna normativa nello scudo di protezione del trattamento dei dati personali, è stata fornita dall'elaborato redatto dal Working Party *ex* art. 29 il 25 novembre 2005, il quale aveva come scopo proprio quello di fornire una *"common interpretation of article 26 of Directive 95/46".* Ebbene, in questo documento il Working Party art. 29 precisò che l'art. 26 par. 1, è stato progettato per affrontare *"a limited number of situations in which an exemption from the "adequacy" requirement for third country transfers was considered to be appropriate"*[46].

Tuttavia, proseguendo nel testo si rinviene che, gli Stati membri potevano far prevalere il loro diritto nazionale, caratterizzato da adeguati livelli di protezione, sulle deroghe di cui all'art. 26 par. 1 Dir. 95/46 in alcuni casi particolari. È il caso ove si fosse reso necessario proteggere gruppi di individui particolarmente vulnerabili, come ad esempio i lavoratori o i pazienti.

Per evitare ovviamente gli abusi sull'utilizzo delle deroghe in questione, lo sforzo maggiore che fu compiuto dal Gruppo in questo elaborato è stato proprio quello di fornire una chiara e comune interpretazione delle deroghe suddette attraverso un rigoroso esercizio di comprensione.

Il chiaro esempio di questa "interpretazione orientata" si ha sulla base del fatto che le disposizioni della Direttiva 95/46 non potevano essere applicate separatamente, poiché come era espressamente previsto all'articolo 25, paragrafo 1, queste disposizioni dovevano essere applicate "*fatte salve le disposizioni nazionali adottate in conformità delle altre disposizioni della presente Direttiva*".

La portata di quanto appena descritto, implicava che, indipendentemente dalle disposizioni invocate ai fini del trasferimento di dati ad un paese terzo, fosse comunque necessario rispettare le altre disposizioni pertinenti della Direttiva. Quindi, qualora dati sensibili fossero stati coinvolti nel trasferimento, sarebbe occorso soddisfare i requisiti di cui all'articolo 8 della Direttiva medesima. Ciò comportando che un trasferimento

[46] WP 29, Working document on a common interpretation of Article 26 of Directive 95/46"- WP 114.

specifico poteva basarsi solo sull'articolo 26, paragrafo 1, se le condizioni dell'articolo 8 fossero state soddisfatte. In altre parole, anche se la legislazione nazionale non fosse stata allineata alle limitazioni dell'ambito di applicazione dell'art. 26, par. 1, per talune categorie di casi, vi sarebbero potute ancora essere restrizioni supplementari derivanti da altre disposizioni della Direttiva 95/46, come appunto quelle che erano considerate nel dettato dell'articolo 8.

Al fine di evitare abusi quindi, il WP 29, attraverso l'elaborato WP 114, elaborò un'interpretazione rigorosa delle ipotesi di cui all'art. 26 par.1 che consentivano una deroga al rispetto del principio di adeguatezza della tutela nel trasferimento verso Paesi terzi.

Per ragioni di sintesi ovviamente, non possiamo riprodurre l'intero documento prodotto, ma ci limiteremo a riportare l'interpretazione che fornì il WP 29 sul "consenso" (art. 26 par.1 *lett. a*) proprio al fine di chiarire i confini entro cui il diritto alla tutela dei dati personali può subire una contrazione e per sottolineare come, attraverso questa interpretazione rigorosa e orientata, il diritto alla tutela dei dati personali rappresenta un punto fondamentale nel contesto dei diritti della personalità.

Abbiamo detto che nell'articolo 26, paragrafo 1, lettera a), veniva affermato che un trasferimento di dati personali può essere effettuato in un paese che non garantiva un adeguato livello di protezione a condizione che "la persona interessata *avesse* manifestato il proprio consenso in modo inequivocabile al trasferimento previsto".

In questo contesto il documento WP 114, delinea il "consenso" come una manifestazione di volontà chiara e non ambigua, poiché la sua importanza costituisce un atto positivo che esclude, quindi, qualsiasi ipotesi in base alla quale l'interessato avrebbe il diritto di opporsi al trasferimento una volta che questo fosse avvenuto. Qualsiasi dubbio sul fatto che il consenso fosse stato effettivamente concesso avrebbe reso inapplicabile la deroga considerata. Così, come affermò il WP 29 (anche) nel suo documento WP 12, "*questo significa probabilmente che molte situazioni in cui il consenso sia implicito (per esempio perché ad un individuo è stato reso noto un trasferimento al quale non si sia opposto) non sarebbe riconducibile a questa deroga.*" Inoltre, nel suo parere sull'interpretazione dell'articolo 13 della Direttiva relativa alla vita privata e alle comunicazioni elettroniche[47], che ha introdotto un sistema uniforme per la comunicazione

[47] Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell´articolo 13 della direttiva 2002/58/CE del 27 febbraio 2004 - WP 90. Il parere intende fornire una

diretta a singoli individui, il Gruppo ha fornito indicazioni sull'interpretazione della nozione di "*consenso preventivo*" nel contesto delle comunicazioni elettroniche, in particolare su internet, che di fatto pone in luce la distinzione con il consenso qui in discorso.

Il documento continua poi, specificando che il consenso deve essere dato liberamente. In quanto non può essere considerato valido il consenso dato da un soggetto che non ha avuto l'opportunità di fare una scelta effettiva. Per questo motivo, il Gruppo discusse se il consenso potesse essere considerato valido per trasferire le informazioni di prenotazione delle compagnie aeree europee (PNR- *Passenger Name Record*)[48] alle autorità statunitensi. Il quesito che si pose atteneva al fatto se il consenso dei passeggeri potesse esser dato liberamente, poiché la circostanza che le compagnie aeree, essendo obbligate ad inviare i dati prima della partenza del volo, escludeva la possibilità per i passeggeri di avere una libera ed effettiva scelta, qualora avessero nel caso deciso di volare[49]. Ancora, il WP 29 volle richiamare l'attenzione sul fatto che potrebbero verificarsi una criticità nel qualificare il consenso del soggetto interessato, come liberamente manifestato, in un contesto di lavoro, a causa del rapporto di subordinazione tra datore di lavoro e dipendente[50]. Il consenso, per essere valido e liberamente manifestato, in un tale contesto, dovrebbe poter comportare che il dipendente abbia una reale opportunità di trattenere il suo consenso senza subire alcun danno, o ritirarlo in seguito qualora vi fosse un ripensamento. In tali situazioni di subordinazione quindi, il rifiuto o le riserve di un

---

interpretazione comune dell´art. 13 della direttiva 2002/58/CE riguardo ad alcuni aspetti che potrebbero dare luogo a soluzioni divergenti in sede di recepimento o di applicazione della normativa nei diversi Stati membri. Secondo il Gruppo, il concetto di e-mail deve essere interpretato nel senso di ritenere che si configura una comunicazione elettronica ogni qualvolta non sia richiesta la simultanea partecipazione del mittente e del destinatario. Il requisito del previo consenso ("*opt-in*"), poi, può essere derogato solo nel caso in cui i dati siano stati già forniti nell´ambito di un rapporto commerciale preesistente ed il marketing si riferisca a prodotti o servizi che, eventualmente riguardati anche dal punto di vista obiettivo del destinatario della comunicazione, siano "simili" a quelli oggetto del rapporto, nei termini suggeriti dal parere.

[48] I dati relativi ai codici di protezione (PNR) sono raccolti dai vettori aerei durante il processo di prenotazione e includono nomi, indirizzi, dati delle carte di credito e numeri di posto dei passeggeri. Ai sensi della normativa statunitense, le compagnie aeree sono obbligate a rendere disponibili tali dati al dipartimento per la Sicurezza interna prima della partenza dei passeggeri. Allo scopo di garantire adeguata protezione ai dati PNR, conformemente a quanto stabiliva la direttiva 95/46, è stato adottato, nel 2004 un "pacchetto PNR" che prevedeva l'adeguatezza del trattamento dei dati effettuato dal dipartimento per la Sicurezza interna degli Stati Uniti (US Departmennt of Homeland Security – DHS).

[49] *Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States*.

[50] *Opinion 8/2001 on the processing of personal data in the employment context and executive summary, dated 13 September 2001*.

dipendente ad un trasferimento di dati, qualora queste non vengano prese in considerazione, potrebbero in effetti causare un danno allo spirito della legislazione europea in materia di protezione dei dati personali anche alla luce della recente normativa introdotta con il GDPR.

Inoltre, alla luce dell'esperienza, il WP 29 osservò come il consenso non è (da solo) in grado di fornire un quadro adeguato a lungo termine per i *Controllers* dei dati in caso di trasferimenti ripetuti o addirittura strutturali per il trattamento in questione. Infatti, in particolare se il trasferimento costituisce una parte intrinseca di una trasformazione principale (ad esempio, la centralizzazione di una banca dati mondiale di risorse umane, che deve essere alimentata da trasferimenti di dati continui e sistematici per essere operativa), i *Controllers* dei trattamenti potrebbero trovarsi in situazioni in cui un soggetto interessato possa successivamente decidere di ritirare il suo consenso. In tale ipotesi, i dati relativi a una persona che decida di ritirare il proprio consenso, di fatto fa venir meno la condizione che i medesimi dati possano esser trasferiti; pertanto, il trasferimento continuerebbe a essere (parzialmente) basato sul consenso del soggetto interessato, ma di fatto si renderebbe necessario trovare una soluzione alternativa (come ad esempio l'ausilio di B.C.R. all'interno del contratto ove si manifesta il consenso dell'interessato).

Basarsi dunque solo sul consenso, al fine di trasferire dati presso Paesi terzi che non garantiscono un adeguato livello di protezione può esser considerata una *"false good solution",* poiché la detta soluzione a prima vista potrebbe sembrare semplice e dinamica, ma in caso di simili patologie può risultare oltremodo ingombrante e ostativa.

Infine, secondo quanto si può evincere dal WP 114 le ulteriori caratteristiche che il consenso deve avere, per ammettere una deroga alle adeguate garanzie di tutela, sono la sua specificità e il fatto che debba essere "informato".

In relazione alla prima, per costituire una valida base giuridica per un eventuale trasferimento di dati, il consenso deve essere dato dal soggetto interessato, specificatamente per una data operazione.

Ovvero il consenso deve essere "informato" e questa condizione è particolarmente importante, poiché impone che gli interessati siano adeguatamente informati in anticipo sulle circostante specifiche del trasferimento (come ad esempio, scopo, identità e dettagli del destinatario).

Il WP 29 sottolineò anche che, secondo il principio generale di fedeltà, le informazioni fornite agli interessati devono inoltre includere il rischio specifico derivante dal fatto che i loro dati saranno trasferiti in un paese che non fornisce una protezione adeguata. Pertanto, solo qualora siano fornite anche queste informazioni i soggetti interessati potranno acconsentire in piena consapevolezza.

§ 4. Dalla Direttiva 95/46 al Regolamento del 2016 n. 679: l'analisi dei Considerande

Il confronto tra la prospettiva in cui si colloca la Direttiva e quella che caratterizza il nuovo Regolamento, consente di comprendere bene le finalità e le caratteristiche di tipo sistematico di questa nuova normativa, e le sue differenze rispetto a quella precedente.

Si noti che, la scelta di sostituire un sistema basato su una Direttiva di armonizzazione con uno basato su un Regolamento immediatamente applicabile, trova la sua ragion d'essere, da un lato nelle trasformazioni economiche, sociali e tecnologiche che hanno interessato i dei due decenni successivi alla emanazione della Direttiva 95/46, e dall'altro, nella centralità assunta "dall'interesse pubblico europeo"[51] nella protezione dei dati.

Il Regolamento si colloca in una prospettiva molto diversa da quella in cui si poneva la Direttiva[52], in quanto esso pur operando in un contesto ove la tutela dei dati personali è riconosciuta dalla Carta dei diritti fondamentali, pone in relazione il rispetto di tale diritto con la sua funzione sociale e con la necessità di contemperarlo con altri diritti di pari rango, proprio in ossequio al principio di proporzionalità.

Si tratta quindi di una visione che muove da un approccio sistematico e realistico, che dunque colloca la protezione dei dati personali all'interno di un insieme di relazioni che

[51] **CONSIDERANDO n. 4**, Regolamento n. 679/2016: "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. […]".

[52] **CONSIDERANDO n. 2**, Direttiva 95/46: "[…] 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".

ha come punti fondamentali, la sua funzione sociale e il rapporto con tutto il sistema dei diritti fondamentali.

Per comprendere questa nuova impostazione, occorre analizzare tre disposizioni del Regolamento che appaiono essere significative a riguardo.

La prima è l'art. 24, par. 1 del GDPR, che impone al titolare del trattamento di assicurare, attraverso l'applicazione di tutte le misure tecniche ed organizzative adeguate, un trattamento conforme a quanto auspicato dal Regolamento. Nel fare ciò, il titolare del trattamento dovrà avere riguardo della natura, del contesto e dell'ambito di applicazione del trattamento avendo considerazione dei probabili rischi per i diritti e le libertà delle persone fisiche che il trattamento potrebbe presupporre.

La seconda è l'art. 33[53] che, nel disciplinare l'obbligo di notifica della violazione di dati personali da parte del titolare del trattamento all'Autorità di controllo, fissa anche dei termini particolarmente brevi e gli elementi che al riguardo devono essere resi noti.

La terza, infine, è l'art. 34 che, disciplinando la notificazione della violazione all'interessato, prevede la sua obbligatorietà, da parte del titolare del trattamento, nell'ipotesi in cui la violazione dei dati comporti un rischio elevato per diritti e le libertà del medesimo; nonché obbligo di comunicazione che può essere richiesto anche dall'Autorità di controllo.

Dall'interpretazione sistematica e dall'analisi incrociata delle tre disposizioni testé citate, emerge chiara la tutela del diritto individuale come aspetto dell'interesse pubblico generale e la conseguente forte discrasia tra Direttiva 95/46 e Regolamento 679/2016: le violazioni dei dati che mettano a repentaglio i diritti e le libertà delle persone fisiche devono obbligatoriamente essere denunciate all'Autorità di controllo, mentre le stesse, soltanto quando il rischio è "elevato", devono essere comunicate anche alla persona fisica interessata.

---

[53] ***Paragrafo 1°***: "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. […]";
Paragrafo 3°: *"*La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

§ 4.1. La base giuridica del Regolamento 2016/679

Al fine di individuare la base normativa dalla quale muove il Regolamento occorre prendere le mosse dai Considerando1 e 12, alla luce dei quali analizzare gli ulteriori Considerando 3, 9 e 11. Infine, attenta analisi merita anche il Considerando 170.

Il Considerando 1 richiama la normativa di "rango costituzionale" (in realtà si tratta di rango internazionale pattizio, poiché fa riferimento al Trattato di Lisbona del 2009) che caratterizza i diritti alla protezione dei dati personali.

Ricorda infatti che la protezione dei dati delle persone fisiche è un diritto fondamentale riconosciuto dall'art. 8, comma 1 della Carta dei Diritti Fondamentali dell'Unione Europea e dall'art. 16 par. 1 del TFUE[54].

Tale affermazione è ripresa anche dal Considerando 12 che richiamando, invece, il par. 2 dell'art. 16 TFUE, sottolinea che esso "conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati".

Quindi alla luce di queste disposizioni, la base normativa sulla quale poggia il potere e il dovere dell'UE di assicurare un'adeguata protezione normativa al diritto in esame, è dunque, solidamente definita.

Tuttavia, ciò non basta per giustificare il superamento e l'abrogazione della Direttiva a favore del Regolamento, poiché anche nella prima, sia attraverso il lavoro del Working Party article 29 e sia attraverso l'opera di armonizzazione del diritto nazionale, veniva garantita la tutela del diritto medesimo.

Infatti, quanto detto è confermato dal Considerando 3, che richiamando la Direttiva[55], riconosce il suo scopo di tutela dei dati personali, seppur attraverso un'opera di armonizzazione.

---

[54] Il Trattato di Lisbona è definito in termini ufficiali *"Trattato di Lisbona che modifica il trattato sull'Unione Europee il trattato che istituisce la Comunità europea".* E' stato firmato a Lisbona il 13 dicembre 2007 ed è entrato ufficialmente in vigore il 1° dicembre 2009. In realtà a Lisbona la Carta de Diritti dell'Unione è stata nuovamente proclamata, per la seconda volta, il 12 dicembre 2007, dopo la prima proclamazione, avvenuta a Nizza il 7 dicembre 2000. Tuttavia l'art. 6 del Trattato sull'Unione europea riconosce e attribuisce alla Carta dei Diritti lo stesso valore giuridico dei Trattati, e dunque si può dire che anch'essa sia entrata a far parte del Trattato di Lisbona, sia pure per interposto riconoscimento del suo valore giuridico vincolante alla stessa stregua del Trattato stesso.

Pertanto alla luce di ciò, si comprende che anche il Regolamento riconosce di inserirsi in un settore non già sconosciuto e privo di disciplina, perciò, per comprendere le ragioni che possono motivare la scelta di adottare un nuovo atto normativo occorre guardare al gruppo di Considerando che vanno dal primo al tredicesimo, in particolare, come anticipato, i Considerando 9 e 11.

Dalla lettura di entrambi, si evincono chiaramente le motivazioni giuridiche che sottendono l'adozione del nuovo Regolamento.

Il Considerando 9, in particolare, sottolinea che la Direttiva, proprio per il suo carattere di normativa di armonizzazione, contenente essenzialmente disposizioni di "principio" o di "quadro" non è stata in grado di impedire "*la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione*", né è riuscita a eliminare o ridurre l'incertezza giuridica e la convinzione, ampiamente diffusa tra il pubblico, della rischiosità delle operazioni *on-line* per quanto riguarda la diffusione di dati personali[56]. Da qui dunque, la necessità di adottare una nuova disciplina per la materia sotto forma di Regolamento, attraverso il quale poter assicurare un livello uniforme, coerente ed elevato di protezione delle persone fisiche rimuovendo gli ostacoli alla circolazione dei dati personali all'interno dell'Unione[57], e tale da garantire, come specificato dal Considerando 11 "[…] il rafforzamento […] dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri".

Alla luce di questa analisi, occorre rilevare, inoltre, un ampliamento della base normativa su cui poggia il Regolamento.

---

[55] La Direttiva 95/46 era unicamente una Direttiva di armonizzazione basata solo (e non tanto) sul riconoscimento della protezione dei dati personali come diritto fondamentale (aspetto questo estraneo alla competenza della Comunità Economica Europea), quanto sulla necessità di armonizzare le legislazioni degli Stati membri in materia di tutela dei dati personali per assicurare la loro libera circolazione all'interno della CEE. Cfr. **F. Pizzetti**, *Intelligenza artificiale, protezione dei dati personali e regolazione*, in *I diritti nella "rete" della rete*, Giappichelli, 2018.

[56] **CONSIDERANDO n. 9**, Regolamento 679/2016: "[…] La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. […]".

[57] **CONSIDERANDO n. 10**, paragrafo 1, Regolamento 679/2016: "Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione.[…]".

Questa di fatto non si esaurisce nel richiamo dell'art. 16 del TFUE ovvero dell'art. 8 della Carta dei diritti fondamentali ma, assume un particolare "spessore" sostanziale, legato alla necessità di innalzare il livello di tutela attraverso uno strumento normativo che, per la sua posizione nelle fonti del diritto dell'Unione europea, assicuri una disciplina omogenea[58] e poteri di controllo equivalenti in tutti gli Stati membri[59].

[58] **CONSIDERANDO n. 170**, Regolamento 679/2016: "Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo".

[59] **F. Pizzetti**, "*Privacy e il diritto europeo alla protezione dei dati personali*", Collana I diritti nella "rete" della rete, Giappichelli, Torino 2016.

Capitolo II: Le B.C.R.

§ 1. La necessità di applicazione delle Binding Corporate Rules: la disomogeneità del contesto legislativo

Nel febbraio del 2010, l'autorevole settimanale *"The Economist"* ha definito l'enorme mole di dati con cui le multinazionali si sono trovate a lavorare *"il diluvio di dati"*. Infatti si sostiene che il mondo stia attraversando un'esplosione informatica senza precedenti e che la nostra società si trova costretta ad essere sempre più dipendente da questi dati informatici.

Sulla base di questo fenomeno gli scienziati e gli ingegneri informatici hanno coniato l'espressione *"the big data"*. Si noti di fatto, che ovunque si rivolga l'attenzione, la quantità di informazioni digitali presenti nel mondo è considerevolmente aumentata, secondo una stima, l'umanità ha creato centocinquanta *esabyte* di dati nel 2005 e il numero è cresciuto nel 2011 fino a milleduecento *esabyte*.

Ovviamente, soltanto la scelta (per lo più discrezionale) su quali informazioni conservare, quali potrebbero essere utili e quali no, risulta alquanto ardua. Tale *"diluvio di dati"* ha già cominciato a condizionare e trasformare gli affari, l'approccio che i legislatori hanno nei loro confronti oltre che la vita quotidiana, sta di fatto che (seppur abnorme) la presenza di dati personali informatizzati presenta grandi potenzialità per lo sviluppo trasversale della società, a condizione che i consumatori, le multinazionali ed i governi facciano le scelte giuste su quando limitare il flusso di tali dati e quando invece questo andrà incoraggiato.

Sebbene la Direttiva 95/46 sia stata emanata in un periodo anteriore a questo considerevole fenomeno sociologico, appare ben chiaro attraverso i suoi obiettivi che, *in primis* la Comunità europea, operava al fine di garantire un'adeguata protezione dei dati personali. Infatti la finalità della Direttiva era rappresentata dal fatto che l'istituzione e il funzionamento del mercato europeo avrebbe, da un lato portato ad un aumento sostanziale dei flussi transfrontalieri dei dati personali tra gli Stati membri per finalità economiche, e dall'altro lato, avrebbe consentito la protezione dei dati in questione da usi *contra ius* proprio facilitando il loro spostamento all'interno dell'Unione Europea attraverso un opera di armonizzazione delle leggi statali in materia di protezione dei dati personali.

Il dato caratteristico, che andremo ad approfondire nel corso di questo capitolo, è che con la Direttiva prima, e il Regolamento poi, il tentativo di proteggere (attraverso tali normative) gli stessi dati durante un trasferimento al di fuori dei confini dell'UE è risultato fallace qualora il paese di destinazione non presentasse (attraverso la sua legislazione interna) degli adeguati standard di garanzia[60].

Si noti quindi che le regole per il trasferimento dei dati create dall'UE hanno spinto molti paesi extracomunitari ad adottare una legislazione sulla protezione dei dati adeguata agli standard europei proprio per preservare i rapporti economici con i paesi europei. È evidente quindi, che quanto appena detto, mette in evidenza che gli ideali protezionisti del Legislatore europeo hanno fatto breccia anche al di fuori dei confini comunitari; tuttavia, la linea di pensiero che consente il trasferimento di dati personali solo verso Stati che garantiscono un adeguato livello di protezione (alla luce dei canoni europei), si scontra con il pensiero dei rappresentanti di alcuni paesi extra-UE, sostenitori del fatto che la disciplina comunitaria (nel caso specifico la Direttiva 95/46) ha prodotto un improprio effetto extraterritoriale[61].

Sebbene le normative nazionali regolano la stessa materia, ciò che ovviamente presenta delle difformità tra un Stato dell'UE ed uno stato terzo, è la modalità e il grado con cui viene garantita la protezione dei dati personali. Ad esempio, all'interno dell'UE i diritti degli individui in materia di trattamento dei dati personali assurgono a diritti fondamentali[62], mentre in altre giurisdizioni è stata scelta una differente e più tenue forma di protezione fino ad arrivare al caso limite di paesi che, in materia di protezione dei dati personali, presentano un grave vuoto legislativo. Vi sono paesi, però, come gli Stati Uniti d'America, ove è presente un diverso regime di protezione, poiché, ad esempio la normativa in materia di elaborazione dei dati nel settore privato si limita a riconoscere solo a determinate società la capacità di porre in essere tali trattamenti, limitandosi ad introdurre degli obblighi di notifica solo in caso di violazioni di determinate categorie di dati personali.

[60] **E. M. L. Moerel:** *Binding corporate rules: Fixing the regulatory patchwork of data protection. Tilburg University,* 2011.
[61] Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners (TCM Asser Press 2006).
[62] Sul punto si legga in combinato gli artt. 16 TFUE e 8 della Carta dei Diritti Fondamentali dell'UE.

§ 1.1. Dal patchwork legislativo alla circolazione di dati tra le varie società del medesimo gruppo

Sulla base delle difformità che abbiamo precedentemente sottolineato, possiamo rilevare come, ad oggi, la normativa sulla protezione dei dati personali in tutto il mondo rappresenta, nella migliore delle ipotesi, un *patchwork* dai colori al quanto differenziati, i quali sono il precipitato delle radicali differenze normative tra gli Stati.

Ora, avendo delineato il contesto nel quale deve essere garantito il diritto alla protezione dei dati personali, si può comprendere come la Direttiva 95/46 sia stata cucita su di un modello che prevedeva un aumento di flussi di dati prevalentemente verso gli Stati membri e meno da questi a paesi terzi. Tuttavia, l'era digitale di cui si è parlato in apertura di capitolo ha prodotto un continuo flusso di dati che sempre più spesso attraversano i confini europei. Tale fenomeno è espressione di diversi fattori scatenanti: da un lato abbiamo una circolazione di dati che sebbene sia trattato dalla medesima società (multinazionale), questa può inviare i dati da trattare presso una filiale del gruppo che, trovandosi in un paese terzo, non si trova sottoposta ai medesimi standard di protezione presenti all'interno dell'Unione Europea. Ovvero l'ulteriore fattore può essere ricondotto alle operazioni di *"esternalizzazione"* con cui le predette multinazionali inviano i dati dei propri dipendenti a società preposte al loro trattamento, ed in tal caso le operazioni che si posso compiere sono le più varie, come ad esempio il pagamento del salario, la valutazione delle prestazioni lavorative, ovvero la pianificazione e la gestione delle risorse umane.

O ancora, il trasferimento di dati verso paesi terzi si può avere allorché le multinazionali che vendono prodotti di consumo necessitino di elaborare i dati personali dei loro clienti. Oppure multinazionali coinvolte in transazioni *business to business* che attraverso il trattamento elaborano i dati dei rispettivi fornitori, clienti aziendali e altri partner commerciali.

Si può inoltre pensare a multinazionali che operano in settori particolari, come quello farmaceutico, contesto ove è richiesta l'elaborazione di specifiche categorie di dati personali nel corso della ricerca scientifica.

Il problema che dunque si pone in luce nel quadro degli esempi sopra citati, attiene al fatto che, a causa della globalizzazione, le attività di queste multinazionali, e quindi il

prodotto dell'elaborazione dei dati, non è fruibile solo da una società del gruppo nel quale magari, il dipendente è assunto. Ma può accadere molto spesso che persone giuridiche di queste dimensioni, presentino una struttura interna ove la gestione delle informazioni di un determinato dipendente, magari dislocato in una filiale presso uno Stato membro, sia deferita ad una filiale che si trova al di fuori dei confini europei perché magari il dipendente in questione risponde a quella determinata unità. Tutto ciò ovviamente può esporre il diritto alla protezione dei dati personali a utilizzazioni rischiose allorché lo Stato di destinazione non presenti degli adeguati standard di tutela.

A questa rischiosa esposizione della tutela dei dati personali si può aggiungere un altro punto sensibile, derivante in questo caso dell'enorme flusso di dati che le multinazionali si trovano a dover compiere.

Come abbiamo evidenziato, la crescita esponenziale di dati personali digitalizzati, rende il trasferimento dei medesimi, attraverso sistemi *point-to-point*, alquanto obsoleta, pertanto tali multinazionali hanno di fatto modificato il trasferimento di dati attraverso il collegamento dei vari *computers* a sistemi di reti private, e ad oggi non elaborano più i dati dei loro dipendenti e dei loro clienti attraverso Sistemi Informatici Locali ma utilizzano dei Sistemi di IT (*Information Technologie*s) centralizzati. Ovviamente, se da un lato questo comporta un più veloce scambio di dati, dall'altro li rende maggiormente esposti ai rischi di cui sopra.

Ciò detto, è evidente che un sistema IT, seppur trattando un flusso di dati di notevoli dimensioni rende comunque agevole il controllo sugli standard di protezione durante il trattamento dei medesimi.

La questione invece, si complica ulteriormente quando questi sistemi IT, in principio centralizzati presso la multinazionale, vengono *esternalizzati* e quindi i dati vengono trattati da società esterne che forniscono questo tipo di trattamento ovviamente al di fuori dei confini comunitari.

Il punto è che questo fenomeno di esternalizzazione (*offshoring*) può far sì che i dati non solo siano trasferiti dalla multinazionale al fornitore del servizio di trattamento, ma che questo possa ulteriormente trasferirli presso altri centri di trattamento da lui controllati. Tutto questo ovviamente sottopone il diritto alla protezione dei dati a diverse legislazioni, esponendo quindi il soggetto a cui questi si riferiscono a continue contrazioni e dilatazioni del diritto medesimo.

In queste ipotesi, per individuare a quante legislazioni diverse sia sottoposto il

trattamento dei dati, occorre muovere dalle modalità con cui tale fornitore (o anche la medesima multinazionale che sposta i dati dei propri dipendenti da una sede all'altra) del servizio muove i dati che riceve. Ebbene, ad oggi le tecniche utilizzate per operare i flussi di dati sono: il *dynamic routing*[63] e il *cloud computing*[64].

Quanto al primo, per definirlo occorre partire dalla definizione di *static routing,* con il quale si stabilisce che per operare il trattamento dei dati, questi seguono un percorso attraverso i vari *network* già prestabilito; mentre il *dynamic routing* non considera un sentiero prestabilito in cui i dati devono esser fatti circolare.

Il secondo metodo invece attiene ad un modello che consente l'accesso al network nel quale si può fare richiesta di condividere risorse (e quindi dati); si tratta di una metodologia molto rapida e con un minimo sforzo gestionale ovvero con minimi rapporti da intrattenere con il fornitore del servizio. Alla luce di tali modalità di trattamento dei dati personali, appare una volta di più evidente come, un diritto tutelato in tutte le sue sfaccettature all'interno dell'UE, si trovi in balia di costanti rischi una volta che i dati che ne costituiscono l'oggetto, si trovano a viaggiare velocemente nel flusso che li sposta da un paese all'altro al di fuori dei confini comunitari. Pertanto alla luce di ciò, non sarà più prevedibile ipotizzare come i dati verranno indirizzati su Internet e dove poi saranno, in ultima istanza, analizzati.

Pertanto la maggiore sfida per le multinazionali (che abbiano o meno sede all'interno dell'UE) è cercare di conciliare il rispetto di tutte le legislazioni nazionali in materia di protezione dei dati personali con la stringente normativa comunitaria. In questo contesto dunque, occorre rilevare, che molti paesi hanno seguito l'esempio dell'UE che con la Direttiva 95/46 prima, e il Regolamento n. 679 del 2016 poi, ha imposto le predette restrizioni al trasferimento dei dati personali verso Stati che non presentino adeguati standard di protezione.

La conseguenza di ciò è che molte società multinazionali si sono trovate costrette ad adottare politiche di protezione che, rispondenti agli standard di cui si è detto, devono

---

[63] Per un approfondimento si veda:
- **L. Coslovich**: *Dynamic vehicle routing and dispatching: heuristic techniques for people and freight transportation*, Trieste, 2005;
- **Ash G. R**..: *Dynamic routing in telecommunications networks*, New York, 1998.

[64] Per un approfondimento si veda:
- **Rossi**: *Cloud computing per la piccola e media impresa: la gestione dell'IT nella nuvola: approccio pratico e vantaggi*, Milano, Tecniche nuove, 2015;
- **Brunetti**: *Windows Azure: il sistema operativo e la piattaforma per il cloud computing*, Mondadori informatica, 2009.

essere applicate a tutte le società del gruppo, mirando così ad assicurare un'adeguata uniformità di trattamento qualunque sia il paese in cui questo avvenga.

È ovvio che il *patchwork* riscontrabile nell'area della protezione dei dati, fa sì che le multinazionali che trasferiscono gli stessi da una società all'altra del gruppo, in qualche modo accettano il rischio di non conformità rispetto agli standard di adeguatezza puntando di fatto volontariamente all'applicazione di normative che lasciano una maggiore libertà di movimento. Ovvero, come nella maggior parte dei casi avviene, tali società ignorano le regole per il trasferimento dei dati al loro interno, sia attraverso gli strumenti di *dynamic routing, cloud computing* ovvero *offshoring*.

A tal riguardo, è ovvio che le Autorità di controllo dei dati nei vari Stati membri dell'UE (DPA acronimo di *Data Protection Authority*) fossero ben consapevoli del fatto che le multinazionali scambiassero (e scambino) i dati personali su scala mondiale ed esternalizzassero (e esternalizzano) l'IT in paesi senza un sistema adeguato di protezione dei dati[65].

Tuttavia l'esperienza pratica dimostra che l'utilizzo degli strumenti delle DPA non sono sufficienti per garantire il rispetto degli standard di protezione presenti all'interno dell'UE, sia per mancanza di un'efficiente cooperazione tra gli Stati membri, che per la mancanza di pragmatici strumenti a disposizione delle DPA[66] medesime.

Alla luce di ciò è evidente dunque che le multinazionali, per evitare di incorrere in violazioni della normativa europea in materia di protezione dei dati personali e nelle relative sanzioni, abbiano iniziato ad esercitare forti pressioni sulle varie DPA affinché queste riconoscessero che le politiche interne (*policy*) da queste adottate nel trasferimento dei dati personali da una società del gruppo (sita nel territorio dell'UE) ad un'altra (collocata in uno stato terzo), fossero e siano riconosciute come operazioni che, sebbene avessero ed abbiano come fonte per regolare il flusso di dati un Regolamento interno, risultino ossequiose degli standard comunitari di adeguatezza.

Si tratta in definitiva di riconoscere, che l'elaborazione e il trattamento dei dati personali in tutte le società del gruppo, anche qualora questo avvenga in un paese che non garantisce un adeguato livello di protezione, avviene nel rispetto della normativa aziendale in materia da un lato, e della normativa comunitaria dall'altro.

---

[65] Sul punto si veda il primo rapporto della Commissione europea sulla Direttiva CE 95/46 del 15 marzo 2003 n. 265.

[66] **E. M. L. Moerel,** *Binding corporate rules: Fixing the regulatory patchwork of data protection*,Tilburg University, 2011.

§ 2. Le Binding Corporate Rules: uno strumento necessario

Prima dell'entrata in vigore del Regolamento UE n. 679/2016, una volta individuata la necessità di uno strumento di derivazione "aziendale" che potesse far rispettare gli standard di adeguatezza della protezione dei dati durante il loro trattamento, occorreva chiedersi quale strumento potesse assolvere a tale ruolo, ovvero quale fosse il titolo che lo legittimasse a porsi come metro di adeguatezza tra la disciplina comunitaria e il trattamento dei dati personali.

Partendo dal secondo quesito, concernente il titolo, il grande lavoro per far sì che uno strumento di derivazione aziendale possa divenire parametro legislativo, è stato operato dal già citato Working Party article 29, il quale, essendo stato preposto all'elaborazione di pareri in materia di trasferimenti *ex* art 26 della Direttiva 95/46, ha riconosciuto il valore di tale regolamentazione transnazionale privata[67] proprio in considerazione delle lacune presenti nel sistema di trasferimento dei dati.

Ovviamente il lavoro del WP 29 ha avuto come base di studio soltanto la Direttiva 95/46 e non anche il Regolamento n. 679 del 2016, tuttavia alla luce dell'ancora attuale applicazione dello strumento di cui si dirà a breve è d'uopo supporre che il nuovo testo legislativo non abbia modificato la situazione.

Muovendo ora dal primo quesito, concernente lo strumento normativo più adeguato, sempre sulla scorta del lavoro operato dal WP 29, sono stati fissati i criteri per queste "regole aziendali" in materia di trattamento, proprio al fine di garantire un livello adeguato di protezione. Primo tra questi criteri è che le norme aziendali in materia devono essere "vincolanti all'interno dell'organizzazione" (quindi su tutte le società del gruppo e su tutti i dipendenti).

Quindi, lo strumento che allo stesso tempo è vincolante all'interno della multinazionale e parametro con il quale confrontare il rispetto degli standard minimi di protezione è stato definito dal WP 29 come BCR, acronimo di *Binding Corporate Rules* (Norme Vincolanti d'Impresa).

---

[67] WP 107 a sua volta modificato dal Documento di Lavoro che stabilisce un modello di *Checklist* per l´approvazione delle *Binding Corporate Rules* del 14 aprile 2005 - WP 108. Questi integra e completa il documento WP 107, fornendo indicazioni specifiche sui contenuti delle regole vincolanti nell´impresa. Il Gruppo ha elaborato una sorta di "*checklist*" che le imprese devono utilizzare per verificare che le rispettive BCR rispondano ai principi fissati nella direttiva n. 95/46/CE. In particolare, deve essere dimostrata l´effettiva vincolatività delle norme, sia rispetto all´interno del gruppo (controllate, collegate, dipendenti, terzi fornitori), sia rispetto all´esterno, soprattutto ai fini dell´esercizio dei diritti riconosciuti agli interessati.

Ora il problema che restava da risolvere, atteneva alla comparazione, cioè a quale legislazione del *patchwork* (in questo caso europeo) le BCR dovevano attenersi. Ebbene sempre il WP 29 introdusse la possibilità di una supervisione centrale della conformità mondiale sui metodi di trattamento. Poiché lo stesso documento WP 107 riconosce alle società di un gruppo la possibilità di far valutare le proprie BCR da una sola DPA europea, invece che riferirsi a tutte quante. Così facendo si concorderà con quest'ultima le regole vincolanti da applicarsi all'interno dell'impresa e anche nei confronti dell'interessato, che di fatto soddisfavano il livello di adeguatezza della protezione accordata[68].

Con l'introduzione di tali BCR, il Gruppo di Lavoro *ex* art. 29 ha creato un complesso sistema di regolazione dei trasferimenti verso paesi terzi, nel quale si combinano da un lato, l'autoregolamentazione transfrontaliera (cioè le politiche aziendali), e dall'altro gli accordi pubblici (cioè la DPA scelta convalida tali *policy* aziendali e fornisce una supervisione durante l'esecuzione del trattamento)[69].

Sulla base del *patchwork* legislativo, si può sostenere che le BCR non solo rappresentano uno strumento per garantire un adeguato livello di protezione dei dati personali durante il loro trasferimento ma, costituiscono anche uno strumento che eserciti un collegamento tra i vari sistemi giuridici.

Poiché come si evince da quanto sopra descritto gli Stati attuavano normative molto diverse in materia ma, tuttavia, le varie legislazioni si potevano ricondurre a due approcci diversi per regolare il trasferimento: l'uno basato su un approccio territoriale (tipico degli strumenti legislativi comunitari) e l'altro basato sulla natura organizzativa del Gruppo.

§ 2.1. Valutazione del regime delle BCR da diverse dimensioni: come forma di regolamentazione privata transnazionale

Alla luce di quanto detto sopra, vale la pena di analizzare se, il regime delle BCR, così come introdotto dal WP 29, rappresenti nel modo più completo lo strumento per ottenere la tutela del diritto alla protezione dei dati personali. A tal fine il regime BCR può essere visto e valutato nel contesto di una serie di dimensioni diverse. Si tratta di punti di vista

[68] **G. Finocchiaro**, *Binding Corporare Rules*, in Contratto e Impresa, Vol. II, 2006, p. 1436 ss.
[69] **E. M. L. Moerel,** Tilburg University, 2011.

che saranno approfonditi nel corso dei seguenti capitoli ma, per necessità di completezza, è bene accennarli in questo discorso.

La prima guarda alle BCR come una regolamentazione privata transazionale (TPR, cioè *Transnational Private Regulation*), in questo casi i legislatori che vogliono regolare il sistema di trasferimento dei dati da una società all'altra del medesimo gruppo possono optare per tale TPR piuttosto che introdurre una regolamentazione di diritto pubblico la quale, ovviamente, porterebbe con se tutta una serie di limitazioni intrinseche in materia di competenza giurisdizionale.

Sul punto, la disciplina di come regolare al meglio gli strumenti per il trasferimento dei dati personali verso paesi terzi è conosciuta nell'UE come *"better regulation"* (BR). Pertanto alla luce della concezione del Legislatore europeo nel rapporto tra BR e TPR, vengono sollevate le seguenti questioni:

- l'idoneità del TPR a disciplinare i diritti umani (tra i quali appunto la protezione dei dati personali);
- quali delle diverse forme di regolazione sarebbe più idonea a regolare la TPR;
- la legittimità del TPR rispetto alla normativa pubblica degli Stati comunitari ed extracomunitari;
- come adattare la TPR ai principi convenzionali del diritto contrattuale.

§ 2.1.1. Valutazione delle BCR come implementazione della responsabilità aziendale

Lo scopo principale delle BCR, come implementazione della "responsabilità" aziendale, consiste nell'utilizzare gli strumenti legislativi per valutare se le imprese, durante il loro processo di trattamento dei dati personali, rispettino effettivamente, attraverso l'ausilio delle BCR, i parametri di adeguata protezione imposti dal Legislatore europeo. In altre parole, si tratta di incoraggiare le imprese, attraverso diversi meccanismi, a far sì che la loro *governance* sia espressione del rispetto di tali standard.

Per far sì che ciò avvenga, il WP 29 propose che questo principio di responsabilità fosse incluso nella revisione della Direttiva 95/46 sulla protezione dei dati personali. Infatti la stessa Commissione europea comunicò la volontà di inserire il

principio di responsabilità nel progetto di revisione della Direttiva 95/46[70]. Ciò ha comportato che, oltre all'obbligo di conformarsi agli standard sulla protezione dei dati richiesti dall'UE, fosse introdotto un obbligo indipendente, proprio per attuare un adeguato programma di conformità alla protezione dei dati. Ed è proprio in quest'ottica che sono state intese le BCR, menzionate dal WP 29 nei suoi elaborati, cioè come strumenti primari che, rappresentano nel migliore dei modi, quest'ulteriore assunzione di responsabilità da parte delle imprese.

§ 2.2. I requisiti delle BCR

Come abbiamo avuto modo di analizzare nei paragrafi precedenti, i contrasti sorti tra le multinazionali e le varie DPAs nazionali, hanno portato a riconoscere le BCR al pari delle clausole contrattuali previste dall'UE negli artt. 25 e 26 della Direttiva 95/46 prima, e negli artt. 45 e 46 del Regolamento n. 679 del 2016 poi[71].

L'obbiettivo quindi è chiaro: snellire e facilitare il trasferimento dei dati personali all'interno del medesimo gruppo societario[72].

Le linee guida dalle quali muovono le multinazionali, nella redazione di BCR che possano superare il vaglio di ammissibilità della DPA prescelta, si ispirano il più delle volte ai principi dell'OECD (*Organisation for Economic Co-operation and Development*) in materia di protezione dei dati personali.

Ovviamente, nel contesto che stiamo analizzando, il trattamento di dati che coinvolge per forza di cose anche trasferimenti in sedi dislocate in paesi terzi, privi dunque di un adeguato sistema di protezione dei dati personali, non è passato di certo inosservato agli occhi del WP 29 e delle DPAs, i quali dovettero prendere atto che gli strumenti convenzionali non erano sufficienti per mantenere degli standard di uniformità e conformità richiesti. Pertanto, il WP 29 riconobbe il valore aggiunto dell'autoregolamentazione aziendale transnazionale nel settore della protezione dei dati, anche alla luce delle carenze Direttiva 95/46 sulla protezione dei dati personali. Inoltre riconobbe questa autoregolamentazione aziendale, proprio come metodo alternativo per

[70] Sul punto: Commissione europea, comunicazione sulla revisione della Direttiva 95/46 (n 34), pp. 11-12.
[71] V. *par. 3*.
[72] **Lokke Moerel**, *Privacy without Borders*, in Dutch Financial Times 3 April 2003.

rispettare le regole in materia di protezione dati[73].

In definitiva, il WP 29 ha approvato un sistema volontario di autoregolamentazione, validazione e applicazione delle BCR che, per certi versi, aprì la strada alla regolamentazione che oggi troviamo all'interno dell'art. 47 del Regolamento n. 679 del 2016[74].

Significativi sono stati i pareri che il WP 29 ha adottato nel corso della sua incessante attività, pareri nei quali sono definiti i criteri che le politiche aziendali, in materia di protezione dati, devono attuare per rispettare gli standard europei e per far sì che le loro BCR possano essere approvate.[75] Un altro aspetto che suddetti pareri sottolineavano era il chiaro riconoscimento da parte delle DPAs alle BCR come strumento convenzionale per il trasferimento dei dati verso paesi terzi[76]. Sulla base del testo della Direttiva 95/45, le BCR non erano affatto riconosciute come strumento avente la capacità di consentire un "sicuro" trasferimento di dati verso paesi terzi, poiché spettava alle DPAs e alle procedure nazionali valutare di volta in volta la possibilità di ricorrere all'utilizzo di tale strumento. Ad oggi invece, alla luce del Regolamento n. 679 del 2016, la valutazione sulle BCR si sposta ad un livello diverso, in quanto non viene più messo in discussione il loro utilizzo, dando per certa la possibilità di ricorrervi, ciò che potrebbe essere invece oggetto di censura da parte della DPA prescelta è il contenuto delle stesse BCR, ossia le modalità con le quali garantiscono la protezione dei dati personali[77].

Ciò che occorre ora analizzare, sono i profili sostanziali delle BCR, cioè i requisiti che, alla luce dei pareri del WP 29, queste devono avere per poter garantire al meglio il diritto alla protezione dei dati personali anche al di fuori dei confini comunitari.

Tuttavia, come anche più volte aveva precisato il WP 29, suddetti requisiti non sono *"craved in the stone"* ma, possono essere rivisti e modificati[78].

Esempio di ciò sono le modalità con le quali si è arrivati a tali elaborazioni, infatti i lavori si sono aperti con una consultazione alla quale presero parte rappresentanti di

[73] Sul punto WP 29, elaborato n. WP 74, V. *infra* Nota 78.

[74] V. par. 3.3.

[75] A titolo esemplificativo e non esaustivo si vedano tra gli altri i Pareri del WP 29: WP 74, WP 107, WP 108, WP 133, WP 153, WP154, WP 155

[76] V. elaborato del Working party Article 29 "Documento di Lavoro che stabilisce un modello di Checklist per l'approvazione delle Binding Corporate Rules", del 14 aprile 2005 - WP 108.

[77] Art. 47 Regolamento n. 679 del 2016.

[78] V. WP 29, elaborato del Working party Article 29"Documento di lavoro: trasferimenti di dati personali ai paesi terzi: applicazione dell'Articolo 26 (2) della Direttiva Europea sulla protezione dei dati alle Binding Corporate Rules (Norme d'impresa vincolanti) per il trasferimento internazionale di dati", del 3 giugno 2003 - WP 74.

diverse multinazionali, e una pubblica audizione che vide la partecipazione di oltre trenta rappresentanti della "*business community*" (così viene definita nel W74). Inoltre, anche alcune DPAs (ad esempio quella del Regno Unito e dell'Austria) hanno pubblicato ulteriori contributi sui requisiti che devono possedere le BCR redatte dalle multinazionali.

I principali requisiti, fissati dal WP29 sono dunque i seguenti:

- se la sede della multinazionale non è stabilita all'interno dell'UE, la multinazionale dovrebbe nominare una società del gruppo, con sede nell'UE, alla quale verrà delegata la responsabilità in materia di protezione dei dati;
- le BCR devono essere presentate per l'approvazione, alla DPA dello Stato membro in cui ha sede la multinazionale pertinente. Se la multinazionale non ha sede dell'Unione europea, le BCR devono essere presentate alla DPA "più appropriata", che nella maggior parte dei casi sarà la DPA della sede centrale delegata dell'UE (Lead DPA)[79];
- la portata geografica ed il contenuto delle BCR, dovrebbero essere chiarite solo se le BCR si applicassero a livello mondiale o solo ai dati originati all'interno dell'UE;
- le BCR dovrebbero descrivere la natura dei dati elaborati (vale a dire categorie di dati particolari c.d. sensibilità), gli scopi per cui sono stati elaborati e l'estensione dei trasferimenti internazionali dei dati all'interno del gruppo;
- le BCR dovrebbero incorporare i principi di trattamento dei dati materiali (Trasparenza, correttezza, limitazione delle finalità, qualità dei dati, diritti degli individui e la sicurezza) e le restrizioni al trasferimento verso terzi al di fuori del gruppo[80];
- le BCR dovrebbero essere vincolanti sia all'interno dell'organizzazione (in tutte le società del gruppo e dei suoi dipendenti) che esternamente vincolanti per il beneficio degli interessati;
- le BCR dovrebbero prevedere una rete di responsabilità per la tutela del diritto alla protezione dei dati con la quale gestire i reclami e il rispetto delle regole;
- un meccanismo interno per la gestione degli illeciti;
- la sede centrale europea (delegata) dovrebbe accertare le responsabilità per il pagamento e il rimedio alle violazioni delle BCR;
- l'onere della prova, in relazione ad una presunta violazione delle BCR dovrebbe

[79] Sul punto, vedi *supra* nota 69.

[80] V. l'elaborato del Working Party Article 29, WP154"*Working Document Setting up a frame work for the structure of Binding Corporate rules. Adopted on 24 June 2008*".

gravare sulla sede delegata all'interno dell'UE;

- le società del gruppo dovrebbero avere il dovere di collaborare con la "*lead*" DPA per rispettare i suoi indirizzi sull'incremento dei requisiti delle BCR[81];
- le BCR dovrebbero prevedere un programma di *audit* che copra tutti i loro aspetti, compresi i metodi per garantire la loro correzione, infatti sul punto sono state intraprese diverse azioni. Ad esempio, le verifiche devono svolgersi regolarmente (da parte di revisori interni o esterni accreditati) o in corso di specifica richiesta. Le BCR dovrebbero prevedere che i risultati della revisione vengano comunicati alla Lead DPA, la quale allo stesso tempo dovrebbe avere il diritto ad accedere ai risultati di tali verifiche;
- i soggetti interessati dovrebbero avere un accesso facilitato alle BCR e in particolare un accesso facilitato alle informazioni sui loro diritti;
- i dipendenti che elaborano il programma dei dati dovrebbero godere di una adeguata formazione;
- dovrebbe esserci un meccanismo di aggiornamento delle BCR, che comprenda anche il meccanismo per segnalare tali aggiornamenti alla Lead DPA;
- le società del gruppo dovrebbero essere obbligate ad essere "trasparenti".

In definitiva sono questi i requisiti "minimi" che, alla luce degli elaborati del WP 29, le BCR realizzate dalle multinazionali devono rispettare per far sì che possa avvenire il trasferimento e il trattamento dei dati personali verso paesi terzi. Il tutto ovviamente ricreando quelle adeguate garanzie che tutelano il diritto alla protezione dei dati personali all'interno dell'UE.

Ovviamente, come abbiamo più volte sottolineato, tali requisiti, rappresentano solo delle linee guida, e ciò è reso ancora più chiaro dalla scelta verbale che il WP 29 fa all'interno dei suoi documenti, poiché con *"should"* non si impone alle multinazionali di operare in una determinata direzione, ma si consiglia di operare in modo che le norme vincolanti superino il vaglio di ammissibilità della Lead DPA.

[81] Questo requisito è stato anche criticato dalle società che chiedono di porre in essere lo strumento BCR, poiché non tutte le DPA hanno il diritto di revisione ai sensi della loro legislazione nazionale. In definitiva, le DPA di base, accettano che il diritto di accedere ai risultati delle verifiche è concesso solo alla Lead DPA. Mentre le altre DPA mantengono i propri diritti di accesso e diritti di revisione nella misura in cui esse dispongono di queste sulla base delle proprie leggi nazionali.

§ 3. Il contesto delle *corporates* e le problematiche nell'applicazione della disciplina comunitaria

Ora che abbiamo analizzato quelli che sono i requisiti che le BCR dovrebbero avere, per garantire il rispetto degli standard europei in materia di protezione dei dati personali nel trasferimento verso paesi terzi, occorre capire quelle che sono le esigenze aziendali delle multinazionali e le ragioni che hanno portato alla loro adozione.

Con l'avvento di internet[82], l'era digitale ha portato ad un livello senza precedenti i flussi globali di dati, sia all'interno delle varie società di un medesimo gruppo, sia all'esterno di queste con i fornitori esterni del servizio di trattamento.

Questa enorme mole di trasferimenti è dovuta a tre fattori specifici che svolgono un ruolo fondamentale.

Il primo fattore è rappresentato dalla *"centralizzazione delle ICT"* (*Information and Communication Technologie*), poiché le aziende multinazionali hanno operato in questa direzione proprio per facilitare lo stoccaggio dei dati dei loro dipendenti, clienti e consumatori, affinché inoltre tali dati siano fruibili dallo stesso gruppo da qualsiasi parte del mondo.

Il secondo fattore riguarda sempre le ICT ma in una prospettiva diversa, poiché attraverso l'ausilio di strumenti come l'*outsourcing*[83]e l'*off-shoring* le multinazionali hanno *"esternalizzato"* tali ICT a fornitori di servizi di trattamento dati esterni i quali, elaborano tali dati dei dipendenti e clienti della multinazionale stessa. È chiaro però, che per abbattere i costi, le aziende affidano tale pratica a fornitori dislocati fuori dai confini dell'UE.

Il terzo ed ultimo fattore, riguarda i sistemi di *routing dinamico* e *cloud computing* i quali, come abbiamo già avuto modo di analizzare, lasciano dei dubbi sul percorso che i

[82] Internet è nata negli anni Sessanta come progetto del Dipartimento della Difesa statunitense per lo sviluppo di una rete che permettesse, anche in caso di guerra, di tenere attivi i collegamenti tra i vari settori delle forze armate. All'inizio degli anni Novanta, è stata messa a disposizione di impieghi civili, collegando dapprima i principali centri universitari e successivamente in modo sempre più ampio, l'utenza istituzionale e privata. Oggi internet collega centinaia di milioni di PC divenendo, un potente mezzo per comunicare, fare affari, promuovere nuove forme di socializzazione e di istruzione. Cfr. **A. Caperna,** *Introduzione alla Information Communication Technology (ICT),* in PISM, Roma, 2008.

[83] Per un approfondimento si veda:

- **Carpenter, Robert H. Jr**: *Walking from Cloud to Cloud: The Portability Issue in Cloud Computing*, Washington Journal of Law, Technology& Arts, Vol. 6, Issue 1 (2010);
- F. **Gilbert**: *Use of Cloud Computing in a Law Office*, Practical Lawyer, Vol. 60, Issue 2 (April 2014),

dati seguono per essere analizzati. Inoltre, lo stoccaggio dei dati attraverso il *cloud computing* lascia l'ulteriore dubbio su dove, la mole dei dati aziendali, saranno archiviati[84].

La conseguenza di queste pratiche e di questi sviluppi è che un tale stoccaggio e una tale elaborazione di dati in tutto il mondo, sposterebbe di volta in volta la tutela al diritto alla protezione dei dati personali sotto l'egida di ciascuna legge nazionale, ciò quindi comporterebbe una tutela per l'individuo che si espande e si restringe a seconda della legislazione di riferimento. Il caso limite, è rappresentato da alcuni paesi federali, come il Canada, che non dispongono di una legislazione in materia uniforme e ciò ovviamente si pone come uno scoglio eccessivamente alto per le multinazionali durante le loro operazioni di trasferimento dei dati personali.

Si tratta pertanto di problemi che le multinazionali sono state costrette ad affrontare allorché si sono trovate soggette a diverse giurisdizioni.

Ad esempio, far convergere verso una disciplina uniforme tutti i trasferimenti di dati che operava una multinazionale sarebbe una pratica impossibile prima dell'ingresso del GDPR, poiché è certo che le varie leggi nazionali previgenti a quest'ultimo, seppur simili tra loro potevano divergere su diversi punti.

Il problema si acuiva qualora una multinazionale avesse perfezionato un sistema centrale per l'elaborazione dei dati dei propri dipendenti e dei propri clienti. Poiché, per esempio, anche all'interno della stessa UE, molte leggi statali imponevano obblighi atti a garantire che suddetti dati fossero protetti sia dalla perdita che dalla loro alterazione imponendo addirittura specifici requisiti tecnici da seguire. Tuttavia, nel caso appunto di un sistema centrale sarebbe stato possibile creare solo un insieme di norme di sicurezza, mentre le singole sfumature legislative locali sarebbero potute non essere percorribili. Quindi così facendo un solo standard non può essere considerato come riferimento a dispetto di tutti gli altri, creando di fatto situazioni di incertezza. Si pensi per un attimo alla Germania, la cui legge statale obbligava a registrare anche gli orientamenti religiosi dei dipendenti occupati nelle multinazionali ma, allo stesso tempo, l'elaborazione di queste tipologie di dati era vietata nel resto degli Stati membri.

Occorre poi sottolineare che molte leggi nazionali si distinguono per un'eccellente completezza di regolamentazione, in quanto evitano possibili lacune legislative nella

[84] **Lieneke Viergever**, *Privacy in the Clouds*, 2010.

protezione dei dati personali che, oltre a creare situazioni di incertezza, possono condurre ad elusioni dolose del rispetto della tutela medesima.

Si noti ancora che si può addirittura giungere ad una patologia dell'iter di protezione dei dati personali allorquando si possono verificare delle situazioni impreviste, come una violazione della sicurezza.

Ad esempio, a causa proprio della centralizzazione dell'ICT, se assumiamo come fattore scatenante della patologia un'ipotetica violazione della sicurezza, con conseguente dispersione di dati, sarà difficile per la multinazionale capire in quale esatto paese si sia verificata tale violazione e soprattutto individuare l'esatta competenza giurisdizionale se si tratta di dati di individui cittadini dei più diversi Stati del mondo. Ciò ovviamente comporterebbe delle evidenti difficoltà di notifica a tutti i soggetti coinvolti, poiché questi possono essere sottoposti alle più diverse legislazioni nazionali.

Ulteriore difficoltà per le multinazionali si ha in ordine alla certezza del diritto applicabile, al fine di garantire un adeguato standard di protezione, sempre nei casi di trasferimenti tra società del medesimo gruppo con sedi all'interno e all'esterno dell'UE. Poiché di base, resta percorribile la via che in un tale trasferimento la normativa applicabile sia quella dell'Unione Europea ma, si tratterebbe di una soluzione tutt'altro che pratica per le multinazionali, le quali si trovano continuamente a scambiare numerose quantità di dati tra tutte le società del gruppo globalmente dislocate. Infatti, ciò porterebbe alla conclusione quotidiana di centinaia (e a volte migliaia) di accordi tra le aziende stesse, non solo, poiché le operazioni di elaborazione e trasferimento di dati sono soggette a cambiamenti continui, anche tali contratti richiederebbero degli aggiornamenti continui.

Sul punto si è espressa in passato anche la International Chamber of Commerce – ICC, la quale, attraverso un rapporto sull'importanza delle BCR come strumento che possa allo stesso tempo snellire le operazioni di trasferimento dati e allo stesso tempo garantire una adeguata protezione legislativa, ha individuato e analizzato le debolezze e i difetti che portava con sé la allora disciplina applicabile. Tale rapporto prende ad analisi la Direttiva 95/46, la quale presentava le regole in generale sul trasferimento dei dati verso paesi terzi come *"outmoded"* e gli strumenti che tale normativa riconosceva come applicabili per consentire tali trasferimenti come *"cumbersome"*[85].

[85] 28 October 2004 (ICC Report on BCR), at 11, to be found at www.iccwbo.org.

§ 4. La regolazione delle BCR all'interno del Regolamento n. 679 del 2016: la valutazione preliminare di "Adequacy" *ex* art. 45

Come specificato in precedenza, il trasferimento verso paesi terzi è ammesso (attraverso gli strumenti forniti dal Legislatore comunitario) solo ed esclusivamente quando lo stato di destinazione presenti degli standard di protezione dei dati personali, durante il loro trattamento, che siano adeguati. Orbene, prima di capire come le BCR possano dar luogo a trasferimenti verso paesi che non rispettino questi standard occorre chiarire cosa si intenda per adeguatezza nella protezione e chi è l'organo preposto alla sua valutazione.

La risposta a ciò viene fornita dalla lettura dell'art. 45 del Regolamento n. 679 del 2016, il quale, rubricato *"Trasferimento sulla base di una decisione di adeguatezza"*, dispone che:

"1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:

a) *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;*

b) *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;

c) *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 loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.*

3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale, e ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della Direttiva 95/46/CE.

5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3.

Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 93, paragrafo 3.

6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.

7. Una decisione ai sensi del paragrafo 5 del presente articolo lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 46 a 49.

8. La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.

9. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della Direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo. "

Spetta dunque alla Commissione, decidere, caso per caso, se il livello di protezione garantito dallo Stato, o dal soggetto terzo, sia adeguato. Si tratta quindi di una decisione che la Commissione deve assumere tenendo in considerazione gli specifici requisiti indicati al *par. 2.*

Per obbligo di sintesi, in questo paragrafo, ciò che occorre sottolineare sono le condizioni che la Commissione deve verificare e cioè:

1. la garanzia che il paese terzo o i soggetti terzi rispettino i principi dello Stato di diritto;
2. la previsione di un ricorso effettivo in sede amministrativa o giurisdizionale che gli interessati, i cui dati sono oggetto di trattamento, possano attivare;
3. l'esistenza di una o più Autorità di controllo indipendenti;
4. l'adeguata valutazione degli eventuali impegni che i paesi terzi hanno rispetto ad altri paesi o soggetti internazionali, come pure la loro partecipazione a sistemi

multilaterali o regionali che possano mettere in pericolo la protezione dei dati personali eventualmente trasferiti nel loro territorio[86].

§ 4.1. La mancanza di una dichiarazione di adeguatezza: Art. 46 del Regolamento n. 679 del 2016

A questo punto il quesito che bisogna porsi è: cosa succede quando il trasferimento verso un determinato paese terzo sia escluso proprio per la carenza di una dichiarazione di adeguatezza.

La soluzione a questa defezione è fornita dall'art. 46 del Regolamento n. 679 del 2016, il quale dispone che:

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le norme vincolanti d'impresa in conformità dell'articolo 47;

c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o

[86] **F. Pizzetti**, *Privacy e il diritto europeo alla protezione dei dati personali*, collana I diritti nella "rete" della rete, Giappichelli, Torino 2016.

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

a) 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; o

b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

4. L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo.

5. Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della Direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della Direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo.

Il punto fondamentale che occorre sottolineare, è che tale articolo detta una disciplina più evoluta rispetto all'art. 26 della Direttiva 95/46 poiché, mentre quest'ultimo riunisce in un'unica norma tutte quelle che definisce "deroghe" al criterio generale dell'adeguatezza contenute nell'art. 25 Direttiva 95/46, il Regolamento prevede ber tre diverse situazioni nelle quali il trasferimento a paesi terzi (o organizzazioni internazionali) è legittimo anche in carenza di tale requisito.

Esso disciplina infatti il caso nel quale sussistano "garanzie adeguate" (art.46), quello relativo alle BCR (art. 47), e infine, elenca le deroghe, intese come casi in cui i trattamenti possono essere autorizzati anche in assenza di altre condizioni.

Pertanto, alla luce di ciò devono essere letti il secondo e terzo paragrafo dell'art. 46. Poiché entrambi infatti indicano le condizioni in presenza delle quali il trasferimento può essere considerato come assistito da garanzie adeguate.

Tuttavia, la differenza che intercorre tra i due attiene al fatto che, il terzo paragrafo indica le ipotesi nelle quali le garanzie adeguate richiedono l'autorizzazione della DPA.

Mentre il secondo paragrafo, indica i criteri e le condizioni in presenza delle quali, le garanzie adeguate sussistono automaticamente, senza la necessità di una specifica autorizzazione della DPA. Nel fare ciò però, tale paragrafo, produce una seconda differenziazione, perché contenendo dalla lettera "a" alla lettera "f" le condizioni in presenza delle quali, anche senza specifica autorizzazione, si deve ritenere che il titolare o il responsabile del trattamento fornisca le garanzie adeguate; distingue trasferimenti posti in essere tra autorità pubbliche (per i quali è necessario uno strumento "giuridicamente vincolante" e avente efficacia esecutiva, *lett. A*), e casi rivolti essenzialmente ai trattamenti che vedono protagonisti anche i privati.

Tra le garanzie adeguate, che riguardano proprio questa seconda categoria, sono richiamate le BCR alle quali viene poi dedicato il successivo art. 47 Regolamento n. 679 del 2016.

§ 4.2. Art. 47 del Regolamento n.679 del 2016: Norme Vincolanti d'Impresa (B.C.R.)

Con l'introduzione dell'articolo 47 del Regolamento 679/2016 si è profondamente innovata la normativa precedente individuando una soluzione pragmatica al problema del patchwork legislativo nel quale si imbattono le multinazionali durante il trasferimento dei dati personali. Ma anche perché la sua introduzione dà la misura della grande evoluzione che ha interessato la digitalizzazione dei dati medesimi e la necessità di individuare strumenti adeguati che ne consentano un veloce e sicuro trasferimento.

Si noti che l'art. 47 Regolamento n. 679 del 2016, non definisce il concetto di norme vincolanti d'impresa (BCR), poiché tale compito è assolto dall'art. 4 del medesimo Regolamento. Questo, al *par*.1, specifica che sono norme vincolanti d'impresa: *"le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento* o *responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento* o *al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune"*.

Una volta appreso cosa siano tali BCR, occorre analizzare come queste possono fornire delle "adeguate garanzie" nel trasferimento di dati personali in paesi terzi che non hanno uno standard adeguato. Tale compito è appunto assolto dall'art. 47[87] che attribuisce

[87] Ai sensi dell'Art. 47 del Regolamento 2016/679:
1. L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:
a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e
c) soddisfino i requisiti di cui al paragrafo 2.
2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno:
a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;
b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei Paesi terzi in questione;
c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;
d) l'applicazione dei principi generali di protezione dei dati, in particolare 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;
e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, 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;
f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;
g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;
h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 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;
i) le procedure di reclamo;
j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;
k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;
l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune,

alle DPA il potere di valutare se queste "politiche interne aziendali" (o clausole) siano conformi agli standard europei e quindi se viene rispettato il meccanismo di coerenza previsto all'art 63 del presente Regolamento. Quello che occorre sottolineare, guardando al *par.* 1*,* è che l'introduzione di questa norma costituisce un forte salto in avanti, coerente con la volontà di adeguare la normativa al trasferimento di dati all'estero alle esigenze del mondo digitale e all'evoluzione delle nuove forme organizzative che il sistema economico ha sviluppato[88].

Esempio di ciò è che le BCR devono essere approvate dalla DPA competente in conformità con il meccanismo di coerenza previsto dall'art. 63 Reg. n. 679 del 2016, che coinvolge anche le altre DPA e la Commissione.

Così facendo il Regolamento conferma il suo doppio obiettivo, cioè di dettare una normativa uniforme e consentire forme di flessibilità agli Stati membri. Infatti, tali BCR non devono essere approvate necessariamente dalla Commissione, poiché è consentito anche alle singole DPA approvarle.

Questo è un forte elemento di flessibilità, in quanto molto spesso vi sono imprese che hanno solo una dimensione nazionale o subnazionale, ma tuttavia, anche in questo caso la DPA competente (cioè quella alla quale l'impresa si rivolge), deve attuare il meccanismo di competenza *ex* art. 63, coinvolgendo anche le altre DPA.

Così facendo tutte le Autorità sono in grado di partecipare all'attività di ciascuna di esse e, allo stesso tempo, laddove le BCR riguardino gruppi di imprese multinazionali, tale meccanismo di coerenza assicura la necessaria uniformità di adozione.

Abbiamo detto che il *par.*1 indica le condizioni sulla base delle quali le norme, autonomamente proposte dalle imprese, possono essere adottate dalle DPA; a ciò fa seguito il *par.* 2 che indica i requisiti in base ai quali può avvenire tale approvazione.

---

in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);

m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

3. La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

[88]**F. Pizzetti**, *Privacy e il diritto europeo alla protezione dei dati personali*, *collana I diritti nella "rete" della rete,* Giappichelli, Torino, 2016.

Sebbene l'elenco sia particolarmente minuzioso non è esaustivo, poiché questi possono essere implementati su richiesta della stessa DPA, sulla base delle necessità del caso specifico.

Tuttavia il contenuto essenziale e comune che tutte le BCR devono rispettare riguarda degli aspetti facilmente individuabili. In primo luogo devono individuare i rapporti che intercorrono nel gruppo di imprese, poiché è fondamentale individuare chi abbia il dovere e l'autorizzazione a rappresentare i gruppi sia dinanzi all'Autorità, sia dinanzi agli interessati. In secondo luogo è importante che sia indicato il complesso di trasferimenti che sono oggetto di BCR, le tipologie di trattamento, le finalità, chi sono gli interessati ovvero l'indicazione del paese terzo (o dei paesi terzi).

Si noti che la conoscenza puntuale della tipologia di trasferimento è fondamentale, ad esempio, per valutare la adeguata applicazione dei principi di protezione (*lett. d*), o anche la specificazione dei diritti degli interessati rispetto al tipo e alle finalità del trattamento (*lett. e*), ovvero delle modalità con le quali il titolare e il responsabile del trattamento si assumono la responsabilità per qualunque violazione commessa da un membro interessato che non sia residente nell'UE (*lett. f*).

Ciò che infine occorre sottolineare è che, la specificazione cosi minuziosa dei requisiti, sottende una sorta di diffidenza o anche di sospetto nell'adozione di questo strumento, diffidenza che di fatto ha anche caratterizzato tutto il lavoro del Working Party art. 29[89].

Tuttavia, sul punto si può anche sostenere che, una disciplina così puntuale, segna una volta di più l'attenzione nel trovare il giusto equilibrio tra i diversi obiettivi; cioè rendere fluidi i flussi di dati tra soggetti che operano in paesi interni ed esterni all'UE, ovvero assicurare che tale flessibilità non comprometta la tutela del diritto alla protezione dei dati personali.

[89] Sul punto si veda WP 29, *Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union. Adopted on 18 January 2005 – WP 106*; e WP 29, Documento di Lavoro che stabilisce un modello di Checklist per l'approvazione delle Binding Corporate Rules, 14 aprile 2005 - WP 108.

§ 5. Dalla Transnational Private Regulation (TPR) alla "privatizzazione" del regime delle BCR

Come si è anticipato nel *par.* 2.1.1 del presente capitolo, le BCR possono essere intese come una forma di regolamentazione privata transazionale (*Transnational Private Regoulation* – TPR) . Tali clausole vincolanti d'impresa possono essere intese in questa accezione sulla base di due considerazioni: la prima attiene al fatto che sono frutto di un'elaborazione da parte di privati che dovrà ottenere una dichiarazione di ammissibilità da parte della Lead DPA; la seconda attiene al fatto che né la Direttiva 95/46 prima, né il Regolamento n. 679 del 2016 poi, quali appunto strumenti normativi di diritto pubblico, abbiano definito i requisiti che tali clausole devono possedere per garantire un'adeguata tutela del diritto alla protezione dei dati personali, infatti i requisiti delle BCR si ricavano soltanto dagli elaborati del WP 29[90].

Appare pertanto pacifico che, alla luce di queste considerazioni, le BCR costituiscono uno strumento di pura derivazione privatistica, quindi figlie di un'autoregolamentazione da parte dei soggetti che operano nell'ambito del trattamento dei dati personali.

Si tratta dunque di lasciare la tutela di un diritto fondamentale alla "*better regoulation* – BR" (migliore regolamentazione) che gli attori privati possano porre in essere. Il punto di partenza per le regole in materia di BR è l'accordo interistituzionale del 2003 stipulato tra Parlamento europeo, il Consiglio dei ministri dell'UE e la Commissione europea[91].

Il tratto caratteristico che si evince dall'accordo attiene al fatto che occorre considerare le misure poste in essere attraverso la BR come "alternative alla legislazione", si tratta dunque di una concezione che segna uno spostamento nella *governance* europea, pronta dunque a riconoscere e persino promuovere l'attivismo degli attori privati.

Si noti che il discorso in parola aderisce perfettamente al contesto delle BCR per due ordini di ragioni. La prima attiene al fatto che queste "auto-regolamentazioni" che pongono in essere le multinazionali, nel sistema delle BCR, è largamente condiviso poiché l'accordo interistituzionale fornisce una visione d'insieme dell'auto-regolamentazione e della co-regolamentazione, ossia impianti normativi derivanti da fonti pubblicistiche e privatistiche, poiché la questione fondamentale che viene in evidenza è

[90] *V. par.* 2.2.
[91] **Inter-Institutional Agreemen**, on *Better Lawmaking*, in particolare art. 16.

non già quella di "capire quale sistema prevalga" ma, piuttosto, comprendere come sistemi di regolamentazione di natura pubblicistica e privatistica possono essere coordinati in modo da coesistere ed evolvere.

Una tale visione è particolarmente rilevante nel sistema delle BCR, poiché la loro normazione non è intrapresa dal legislatore europeo, ma di fatto è frutto degli elaborati del WP 29[92].

Il secondo punto di contatto tra questa auto-regolamentazione e il regime delle BCR riguarda un quesito al quale si auspica una risposta nel più breve termine. Poiché dall'accordo interistituzionale si evince che l'auto-regolamentazione (o anche una co-regolamentazione), non può essere considerata uno strumento adeguato per disciplinare la tutela al diritto alla protezione dei dati personali quale diritto umano. Quindi il quesito appare chiaro, ossia se è possibile lasciare la tutela di questo diritto fondamentale al sistema delle BCR, ovvero se sia necessario auspicare un ulteriore intervento legislativo anche alla luce dell'intenso lavoro fatto con l'emanazione del Regolamento n. 679 del 2016.

Sulla base di questi fenomeni di auto-regolamentazione e di co-regolamentazione che danno luogo a forme di TPR è dunque possibile sostenere che il sistema di BCR presenta diversi attori che intervengono in misura diversa nel processo di normazione delle BCR a seconda del livello di regolazione di riferimento.

Suddetti attori sono rappresentati dal Legislatore europeo, dalle DPAs, dalle multinazionali quali titolari del trattamento e dai responsabili del trattamento e partner commerciali.

Circa il Legislatore europeo, occorre rilevare che questo ha adottato prima la Direttiva 95/46, poi il Regolamento n. 679 del 2016. Sebbene gli evidenti miglioramenti che il secondo testo normativo ha apportato al diritto alla protezione dei dati personali all'interno del territorio comunitario, attraverso i meccanismi di coerenza e cooperazione [93]da parte degli Stati membri nei trasferimenti di dati personali in paesi terzi che non presentano garanzie adeguate di tutela occorre rilevare però che né la Direttiva 95/46 prima, né le innovazioni del Regolamento n. 679 del 2016 poi, hanno delineato i criteri materiali, o per meglio dire, i requisiti materiali per far sì che le BCR possano fornire le adeguate garanzie.

[92] *V. par.* 2.2.
[93] *V. Cap. III par. 5*

Ad oggi dunque il Legislatore europeo non ha avviato un processo di normazione per la redazione delle BCR ed esse continuano a rimanere ancorate agli elaborati del WP 29. Ciò cambierebbe solo sé oltre all'art. 47 del Regolamento n. 679 del 2016, che prevede le BCR come strumento che possa garantire adeguate tutele nel trasferimento di dati personali verso paesi terzi, si introducessero ulteriori disposizioni atte a fissare a monte i criteri materiali[94].

Per ciò che attiene alle DPAs poi, in particolare alla Lead DPA e alle Co-Leads DPAs, Autorità responsabili della procedura di approvazione del singolo testo di BCR, ciò che occorre evidenziare nel disegno BCR quale forma di TPR è che, le DPAs verificano la conformità del sistema BCR redatto dalla multinazionale, affinché sia conforme a quanto elaborato nei lavori del WP 29.

Questo rafforza ancor di più la convinzione di descrivere le BCR come forma di TPR per due ragioni, la prima è che si evidenzia una lacuna nell'impianto normativo pubblicistico poiché il Legislatore europeo non ha fornito dei criteri materiali di riferimento all'interno del Regolamento n. 679 del 2016 (e prima ancora nella Direttiva 95/46). La seconda invece, strettamente collegata alla prima, è che una Autorità di garanzia pubblica come la DPA dovrà emanare un giudizio di ammissibilità avendo come modello di riferimento degli elaborati che, seppur autorevoli, non rappresentano una fonte di diritto.

Pertanto, sulla base di quanto appena esposto è chiaro che il reale attore della *normazione*, o più propriamente della stesura delle BCR è rappresentato dalle multinazionali, effettive destinatarie del Regolamento n. 679 del 2016 per quanto concerne i trasferimenti dei dati personali extra UE, e degli elaborati del WP 29.

In questo contesto poi, un ruolo fondamentale è ricoperto dai responsabili del trattamento e dai partner commerciali. Poiché seguendo la catena di approvvigionamento dei dati personali, rientrano sempre nel regime delle BCR le operazioni di elaborazione ed esternalizzazione dei dati personali che i suddetti responsabili del trattamento possono porre in essere. Quindi anche tali soggetti possono essere considerati attori del processo di *normazione* ossia regolamentazione, in quanto il regime di BCR avrà un effetto anche sul loro modello di *business*.

[94] **Curtin, Senden**: *Public accountability of Transnational Private regulation,* in Journal of Law and Society, 2011.

§ 5.1. I rischi della "privatizzazione" del regime BCR

Alla luce di coloro che sono designati come gli effettivi attori del processo di normazione (regolamentazione) delle BCR, parte della dottrina[95]ritiene che questi possano essere definiti come "regolatori di fatto". Si noti dunque, che sulla base degli elaborati del WP 29 che fissa i criteri materiali per la redazione delle BCR, lo stesso Gruppo può essere definito come il "regolatore di fatto" principale.

Una tale definizione del WP 29 riposa su tre assunti:

1. si tratta di un organo che è stato istituito per cooperare con le varie DPAs;
2. svolgeva esclusivamente delle funzioni consultive ed emette pareri per contribuire all'applicazione uniforme della Direttiva 95/46 sulla protezione dei dati personali e proponeva l'introduzione di norme comunitarie che potessero avere come oggetto la protezione dei dati personali[96];
3. contribuiva all'auto-regolamentazione mediante l'indicazione dei criteri materiali delle BCR.

Dunque, alla luce di ciò è evidente come parte della dottrina ritenga che tutto l'impianto del TPR sia il costrutto di un "regolatore di fatto".

Tuttavia, trovandosi nel contesto della tutela di un diritto fondamentale, quale è appunto la protezione dei dati personali, la legittimità del criterio di valutazione delle BCR non può essere considerato alla stregua di un processo di regolamentazione di tipo pubblicistico.

La legittimità dunque deve essere realizzata attraverso un processo legislativo che, essendo "surrogato", richiede delle attenzioni aggiuntive, come una maggiore partecipazione di quegli attori che nel processo di regolamentazione restano sullo sfondo, una maggiore trasparenza e chiarezza del processo di regolamentazione stesso, nonché

---

[95] **Follesdal, Wesse, Wouters**: *Multilevel regulation and the EU, The interplay between global, European and national normative processes*, Boston, 2008.
Curtin, Senden: *Public accountability of Transnational Private regulation*," in: 38 Journal of Law and Society, (2011).

[96] Sul punto occorre rilevare che essendo il WP 29 organo istituito a norma dell'art. 29 della Direttiva 95/46 i suoi compiti dovrebbero attenere all'elaborazione di precisazioni solo sulla normativa in oggetto. Tuttavia alla luce dell'elaborato n. WP 243 del dicembre 2016 il WP 29 ha emesso il proprio parere anche in ordine al DPO, il quale è un soggetto che è stato introdotto dal nuovo Regolamento n. 679 del 2016, pertanto si può sostenere che il lavoro del WP 29 si esteso anche sul nuovo testo legislativo. Il campo d'azione di questo Gruppo ha riguardato la tutela del diritto alla protezione dei dati personali in tutte le sue declinazioni.

una maggiore responsabilità del *"Board"* che ha preso il posto del WP 29 il quale è stato il vero "regolatore di fatto"[97].

In conclusione di quanto sostenuto appare dunque che le BCR come forma di TPR siano state frutto di un considerevole lavoro politico operato dagli attori principali quali il WP 29 come "regolatore di fatto" e le multinazionali che hanno redatto le BCR da sottoporre alle DPAs[98]. Dunque è chiaro che alla luce dei costi che le multinazionali sopportano nel corso del trasferimento e trattamento dei dati personali, la loro *policy* in materia di redazione delle BCR sarà incentrata su un effettivo contenimento degli stessi sforzi economici. Con ciò appare dunque evidente che le multinazionali abbiano un forte interesse a condizionare, secondo i propri interessi, il processo di regolamentazione delle BCR e quindi dello stesso TPR. Di conseguenza, questo comporterà un conflitto tra le varie multinazionali sulla distribuzione dei costi per la redazione dei singoli testi di BCR. Per spiegare ciò, si pensi ad esempio ad una multinazionale sita in un determinato paese (che presenta un proprio ordine di garanzie) la quale, si potrebbe trovare nella condizione di dover operare un aggiustamento al proprio regime di BCR perché magari gli standard che questo dovrà rispettare sono frutto di una tipologia di TPR diversa dalla *policy* della multinazionale in parola. Ciò comportando quindi costi aziendali ulteriori per adeguare i propri standard di garanzia al nuovo regime[99].

[97]**Wessel - Wouters**, *The Phenomenon of Multilevel Regulation: Interactions between Global, EU and National Regulatory Spheres*", in Follesdal; **Wessel - Wouters**, *Multilevel regulation and the EU, The interplay between global, European and national normative processes*, Boston, 2008.
[98]**Büthe, Mattli**: *The New Global Rulers: The Privatization of Regulation in the World Economy",* Princeton University, 2011.
[99] **Büthe, Mattli**: *The New Global Rulers: The Privatization of Regulation in the World Economy*, Princeton University, 2011.

Capitolo III: Le B.C.R. nei contratti

§ 1. Le caratteristiche della scelta contrattuale

Introducendo il discorso delle BCR quali clausole contrattuali, occorre precisare che qualsiasi trasferimento all'estero di dati personali presenta diversi profili, questi possono essere racchiusi in tre gruppi: il primo è costituito dalla fase immediatamente successiva all'operazione di raccolta di dati, il secondo attiene ad una operazione di divulgazione degli stessi ed il terzo racchiude proprio il flusso verso l'estero dei dati[100].

Per ciò che concerne all'operatività delle BCR, queste attengono esclusivamente al terzo gruppo, nel senso che, il flusso estero, cioè verso paesi terzi, se presidiato da adeguate garanzie di protezione fornite dalle BCR, sarà considerato legittimo anche se avrà come destinazione proprio un paese con una carente legislazione di protezione.

Pertanto, alla luce delle disposizioni comunitarie in precedenza analizzate (artt. 25 e 26 Direttiva 95/46 e artt. 45 e 46 Reg. n. 679 del 2016), le quali limitano il trasferimento verso paesi che non forniscono delle adeguate garanzie, la soluzione contrattuale, contenente le BCR, costituisce una delle possibili soluzioni per superare il divieto di trasferimento verso gli stati suddetti.

La particolare importanza dello strumento contrattuale, si rinviene già dai primi elaborati del WP 29, il quale sia nel 1997 che nel 1998[101], evidenziava la possibilità di adottare il contratto, sia come soluzione per disciplinare il regime di responsabilità in materia di tutela dei dati personali tra l'esportatore e l'importatore, sia proprio per garantire un adeguato livello di tutela dei dati personali in caso di trasferimenti in tali paesi terzi.

Appare dunque evidente, che la principale funzione delle disposizioni contrattuali è quella di garantire un'adeguata tutela che possa in qualche modo riempire le lacune

[100] La "migrazione" del dato dal territorio europeo a quello estero ingenererebbe rischi collegati alla mancata applicazione delle norme e delle tutele individuate dalla normativa europea, con la pericolosa conseguenza che i dati solo per il fatto di circolare al di fuori del territorio europeo sarebbero di fatto sprovvisti delle idonee garanzie preposte a loro tutela.

[101] WP 29, elaborato n. WP4 *First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy Discussion Document* adopted by the Working Party on 26 June 1997; WP 29, elaborato n. WP 7 Working Document: *Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?* Adopted by the Working Party on 14 January 1998.

legislative lasciate dalla normativa dello stato di destinazione. Inoltre, come precisato dal *Considerando n.3* di entrambi gli elaborati di cui sopra, il ricorso al contratto, e dunque alle BCR, deve soddisfare alcuni requisiti specifici, che le stesse parti contrattuali devono impegnarsi a garantire, cioè:

- l'applicazione del complesso dei principi fondamentali in materia di protezione dei dati personali costituiti da:
  - il principio della *finalità limitata,* il quale va a delimitare le finalità per le quali i dati vengono trattati dopo il trasferimento;
  - il principio di *qualità e proporzionalità,* che impone l'aggiornamento e l'esattezza dei dati;
  - il principio di *trasparenza,* che impone il rilascio alla persona interessata di alcune informazioni minime atte ad assicurare un adeguato livello di conoscenza e consapevolezza delle operazioni che verranno effettuate con i propri dati;
  - il principio della *sicurezza,* secondo cui il titolare del trattamento deve adottare misure di sicurezza tecnica ed organizzativa contro i rischi già individuati e prevedibili;
  - il principio di accesso per *l'esercizio dei diritti di accesso, rettifica, limitazione e opposizione* da parte dell'interessato;
  - il principio delle *restrizioni ai successivi trasferimenti a terzi,* salvo il caso in cui quest'ultimi, anche attraverso idonei strumenti contrattuali, assicurino agli interessati le medesime garanzie di protezione dei dati;
- l'efficacia del sistema di protezione del diritto alla tutela dei dati personali attraverso:
  - un efficiente livello di osservanza delle norme preposte, mediante un ottimo livello di conoscenza degli obblighi da parte del titolare e dei diritti degli interessati;
  - sostegno ed assistenza agli interessati, qualora essi esercitino i loro diritti;
  - una adeguata riparazione in caso di violazione dei diritti dello stesso interessato.

§ 2. BCR e clausole tipo: una panoramica sulle differenze

Come abbiamo sottolineato in precedenza, la funzione delle BCR, è quella di riempire il vuoto legislativo, lasciato da talune legislazioni extra UE, in materia di adeguate garanzie di protezione dei dati personali durante il loro trasferimento e trattamento. Ora, le clausole contrattuali possono svolgere questa funzione surrogatoria attraverso due modalità distinte delle quali è opportuno individuarne e analizzarne le differenze.

La prima è proprio attraverso le BCR, cosi come erano previste dal paragrafo 2 dell'art. 26 della Direttiva 95/46 e poi successivamente annoverate tra gli strumenti indicati all'art. 46 paragrafo 2, lett. b) del Regolamento n. 679 del 2016. Attraverso le BCR dunque, si consente alla Lead DPA prescelta di autorizzare determinati trasferimenti, quando il titolare del trattamento (alla luce della definizione fornita dal Regolamento n.679 del 2016) presenta clausole contrattuali appropriate che dunque vincolino (*Binding*) l'esportatore e l'importatore dei dati ai principi fondamentali della *data protection.*

Il secondo procedimento, invece, utilizza delle clausole, che sebbene abbiamo come scopo il medesimo delle BCR, presentano una modalità di formazione e di convalidazione del tutto diversa e che è bene analizzare onde evitare fraintendimenti.

Si tratta di clausole definite dalle fonti comunitarie *"tipo"*. Queste erano contemplate nel paragrafo 4 dell'art. 26 della Direttiva 95/46 e poi successivamente riproposte e modificate all'interno dell'art. 46 paragrafo 2 *lett. c) e lett. d)* del Regolamento n. 679 del 2016. In questo caso si tratta di clausole che, adottate dalla Commissione europea (o dall'Autorità di controllo di cui alla *lett. d*), secondo una specifica procedura, offrono (alla stregua delle BCR) garanzie di tutela sufficienti per il trasferimento dei dati personali verso paesi terzi.

Appare dunque evidente che, le clausole tipo, divengono efficaci all'interno di uno Stato membro sempre attraverso un provvedimento autorizzativo da parte della DPA (in questo caso nazionale), tuttavia, a differenza delle BCR, in questo caso, non occorre un apposito vaglio da parte di tale Autorità nazionale, in quanto tale autorizzazione può considerarsi quasi automatica.

Mentre, il discorso per le norme vincolanti d'impresa cambia, poiché le autorizzazioni fornite dalla Lead DPA (in questo caso quella prescelta dalla multinazionale), fondate sul riconoscimento dell'adeguatezza delle clausole adottate contrattualmente, dovranno

successivamente essere (semplicemente) comunicate alla Commissione europea e alle altre DPA.

§ 3. Le caratteristiche delle BCR nella catena contrattuale tra titolari e responsabili del trattamento

§ 3.1. La funzione limitativa delle BCR nella "catena di distribuzione" dei dati personali

Sebbene nel corso di tutta la trattazione fin qui svolta, le BCR siano state descritte come uno strumento proiettato alla tutela del diritto alla protezione dei dati personali, tali norme vincolanti d'impresa, possono essere analizzate anche da un'altra prospettiva. In questo caso si tratta di guardare alle BCR non come strumenti di tutela ma come strumenti limitativi.

Limitativi all'uso che i vari responsabili del trattamento possono fare dei dati personali.

Tale forza limitativa è imposta dal regime di TPR[102] nel momento in cui il titolare del trattamento, racchiude entro determinati confini, l'utilizzo materiale che i responsabili del trattamento possono fare dei dati.

In linea di massima quindi attraverso l'introduzione delle norme vincolanti d'impresa nel contratto, il titolare del trattamento opera una vera e propria gestione dei dati atta a garantire (attraverso una limitazione del loro utilizzo) la protezione di quelli relativi ai dipendenti e dei consumatori.

Pertanto, nel momento in cui, una multinazionale, pone in essere delle trattative contrattuali con una società, con sede fuori dall'UE, e oggetto del medesimo contratto siano i dati personali dei propri dipendenti ovvero consumatori, attraverso tale funzione

[102] *V. Cap. II*.

limitativa delle BCR è possibile mettere in atto delle garanzie materiali per proteggere i dati suddetti.

Per comprendere meglio questa interpretazione possiamo rifarci ad un esempio:

- si pensi ai contratti che le multinazionali concludono per gestire una flotta di auto, carte di credito aziendali o dispositivi di comunicazione.

Ebbene, in queste ipotesi, la conformità dell'elaborazione dei dati personali si avrà solo se la multinazionale impone, attraverso le BCR inserite nel contratto, sul fornitore del servizio esterno (responsabile del trattamento) limitazioni all'uso di tali dati personali nella misura delle prestazioni che sono oggetto di contratto.

Per far sì che ciò avvenga è necessario che il regime di BCR, imposto dalla multinazionale con la conclusione dell'accordo scritto, imponga degli obblighi ben precisi. Cioè oltre a far sì che le clausole contrattuali pongano in essere le garanzie adeguate in materia di trattamento dei dati personali, le BCR indicano anche i confini (e dunque i limiti) entro cui il trattamento dei dati da parte del responsabile del trattamento può essere operato.

Occorre mettere in evidenza, che da questa gestione della catena contrattuale dei dati approvvigionati dalle multinazionali, e trasferiti verso responsabili del trattamento esterni all'UE, venivano in luce tre distinte problematiche con la medesima rilevanza per le garanzie contrattuali che la multinazionale imponeva, ed oggi ancor più impone attraverso le BCR.

Il primo problema, si rinveniva nel fatto che alla luce delle disposizioni legislative sino a ieri presenti, la dottrina non riusciva ad individuare una modalità certa con la quale l'interessato potesse far valere il suo diritto alla tutela dei dati personali anche nei confronti del responsabile extra-ue se non vi fosse stata la presenza di una specifica clausola[103] che prevedesse una tutela in tal senso.

Il secondo problema era strettamente collegato al primo, in quanto, anche se il contratto concluso tra la titolare e responsabile extra-ue, includeva una clausola a favore degli interessati, la possibilità per questi di ricorrere alla tutela giurisdizionale non

[103] Sul punto emblematica è la sentenza: **Doe v. Walmart IX° circ. 2009** […] *court denied workers of a supplier of Wal-Mart the status of third party beneficiaries arguing that the clause incorporated in the contract between Wal-Mart with the supplier did not constitute a promise on behalf of Wal-Mart towards the workers, since it would have been necessary in order to establish third party beneficiary*.
In the eyes of the court, "the requirement that the suppliers were to provide sufficient working conditions and the clause that gave Wal-Mart the right to conduct inspections of the working site whether those requirements were kept, concerned purely the relationship between the two contracting parties but had no beneficial effect to the workers themselves".

appariva molto realistica soprattutto se i responsabili, fossero stati localizzati in paesi ove in caso di violazione degli obblighi contrattuali, la tutela giurisdizionale sarebbe apparsa come "un'arma spuntata".

Infine, una terza problematica di ordine più generale, sollevata dalla letteratura in materia di TPR[104], atteneva alla debolezza degli anelli della catena contrattuale rappresentati proprio dalle BCR. Tale problematica poneva l'attenzione sia al crescente fenomeno di *outsourcing,* sia a quello dei *sub*-responsabili del trattamento finale dei dati personali.

Il punto comune che si rinviene dall'analisi di queste problematiche, attiene al fatto che, nonostante un controllo sulla catena contrattuale, difficilmente prima si poteva dare attuazione alle obbligazioni che concernevano la protezione dei dati personali (in caso di mancata esecuzione della prestazione in discorso) attraverso l'intervento dell'autorità giurisdizionale.

Si noti infatti, che all'interno del rapporto contrattuale, avendo ad oggetto uno scambio di prestazioni, molto spesso le controversie sono risolte introducendo degli ulteriori scambi il più delle volte bonari e attraverso un continuo aggiustamento delle relazioni[105].

Inoltre, tenuto conto del fatto che ad oggi l'elaborazione dei dati avviene sempre più spesso *on-line*, sia all'interno delle multinazionali stesse, che tra multinazionali e i responsabili extra-ue del servizio, parti di tali rapporti contrattuali, sono tenuti a gestire i trattamenti a loro affidati rigorosamente entro il perimetro delineato nella clausola BCR dal titolare del trattamento, onde evitare tutti quei rischi, anche economici a cui altrimenti quest ultimo si troverebbe esposto. All'adire l'organo giudiziario, in caso di rischi che possano minare le stesse prestazioni contrattuali, le parti cercano di accettarli, limitarli, oppure trasferirli mediante altri contratti ad altre parti o ad altri partner[106].

Per il discorso appena affrontato, appare evidente che, sia il ruolo della multinazionale che individua le BCR da utilizzare, che la gestione della catena contrattuale attraverso le BCR e i responsabili o sub-responsabili del trattamento, avrà un ruolo sempre più importante nel raggiungimento della protezione dei dati personali nella

---

[104] **Howells – Geraint - Iain Ramsay - Thomas Wilhelmsson** (eds*). Handbook of International Consumer Law and Policy* Cheltenham: Edward Elgar 2010.

[105] **Colin David Scott**, *Enforcing Consumer Protection Laws* (July 30, 2009), UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 15/2009, disponibile su SSRN: http://ssrn.com/abstract = 1441256.

[106] **Pierre Trudel**, *Privacy Protection on the Internet*, in Serge Gutwirth et. al. (eds.), Reinventing Data Protection (Springer 2009), Cap. 19.

pratica, sia prevedendo adeguate garanzie, sia limitando le operazioni strettamente alle finalità oggetto di trattamento.

§ 3.2. L'efficacia delle BCR

La caratteristica appena analizzata, apre la strada all'analisi di un'altra che ne appare saldamente collegata, cioè l'efficacia delle BCR. Prima di capire come questa si colleghi alla tutela dei dati dei dipendenti ovvero agli stessi responsabili del trattamento, è bene analizzare i profili sostanziali dell'efficacia delle BCR.

Trattandosi di un contratto e non di una legge, il complesso delle BCR vincola solo le parti contraenti, vale a dire il titolare e il responsabile del trattamento.

Gli interessati ai quali i dati personali si riferiscono sono soggetti estranei alla conclusione delle clausole contrattuali, indipendentemente dal fatto che si tratti di clausole redatte per il trasferimento verso un responsabile con sede fuori dall'UE e dunque in un paese privo di una tutela adeguata.

Per questo motivo, talvolta le BCR possono essere concepite come disposizioni "in favore del terzo", nel senso che l'interessato potrà farle valere sia nei confronti del titolare che nei confronti del responsabile.

§ 3.2.1. Efficacia nei confronti del responsabile e tutela dei dati degli interessati

Alla luce degli elaborati del WP 29, possiamo notare, che per la natura contrattuale del rapporto tra titolare e responsabile del trattamento, non è necessaria l'introduzione di una clausola *ad hoc* a favore del terzo interessato, poiché, come abbiamo detto in precedenza il contratto si instaura tra le due parti di cui sopra. Tuttavia, essendo che il trasferimento di dati approvvigionati avviene presso un paese terzo, la sede della multinazionale all'interno dell'UE dovrà comunque presentare garanzie adeguate per la tutela dei dati personali, che consentano al "terzo" interessato di tutelare in prima persona il suo diritto alla protezione dei dati personali.

L'assenza di un obbligo specifico in questo senso, attiene al fatto che il responsabile del trattamento, seppur sottoposto alla legislazione di un paese terzo, al momento della sottoscrizione del contratto, si obbliga a rispettare gli standard di protezione europei che sono fatti salvi attraverso il contenuto delle BCR e dunque, per certi versi, si può sostenere che questi sia direttamente sottoposto alla legislazione europea.

Nella teoria questo meccanismo dovrebbe funzionare automaticamente, tuttavia nella pratica ciò potrebbe non avvenire, e per spiegare ciò possiamo rifarci ad un esempio:

- si pensi alle BCR per i dati dei dipendenti, queste spesso contengono delle limitazioni per evitare che i dati oggetto di trattamento siano utilizzati per scopi di *marketing* diretto. Qualora la multinazionale redige un contratto per l'assicurazione sanitaria dei propri dipendenti, attraverso l'introduzione di queste tipologie di BCR si possono evitare fenomeni di marketing diretto dell'assicurazione sul soggetto terzo (interessato) proprio sulla base dei dati trasferiti.

Tuttavia, appare evidente che nel momento in cui il dipendente, decida di stipulare un contratto di assicurazione individuale per un proprio familiare, in forza di un piano di benefit in tal senso rivolto, con il responsabile in questione, tale contratto potrà essere il risultato di una trattativa svolta sulla base del precedente "accordo quadro".

A ciò però si deve aggiungere che la compagnia di assicurazioni, facendo parte del medesimo gruppo societario, può essere considerata allo stesso tempo sia responsabile del trattamento che titolare del trattamento quindi, in quest'ottica, qualora non possa utilizzare i dati dei propri "dipendenti" per scopi di *marketing* diretto, potrà farlo per i dati dei propri "clienti".

Dunque è evidente che il soggetto interessato ad un ipotetica azione di *marketing* in questo caso è rappresentato dal familiare, il quale assume le vesti di cliente, ed è altrettanto chiaro che attraverso l'ausilio delle BCR si possa garantire un'adeguata tutela del diritto alla protezione dei dati personali, in un contesto come quello appena descritto, senza che il diritto si trovi a subire una contrazione. Quanto detto vincolando l'assicurazione tramite le BCR alla diffusione dell'adeguata informativa e della raccolta allo specifico consenso *marketing* nei confronti del familiare del dipendente.

§ 3.2.2. Efficacia nei confronti della multinazionale

Guardiamo ora alle caratteristiche delle BCR dal punto di vista dell'efficacia nei confronti della multinazionale.

Piuttosto che fare affidamento su una tutela per così dire *ex-post,* la dottrina in materia di tutela suggerisce una soluzione, proprio per migliorare tutta la catena contrattuale, attraverso l'imposizione di un obbligo di monitoraggio sulla multinazionale stessa[107].

La maggior parte dei contratti di trasferimento dei dati, di fatto, già contiene una disposizione relativa al monitoraggio da parte della società titolare su quella responsabile del trattamento, tuttavia si tratta di una mera possibilità che il titolare può esercitare discrezionalmente[108]. Si noti inoltre che dal momento che i rapporti di *outsourcing* posti in essere tra titolare e responsabile del trattamento, sono di norma molto simili tra loro, le parti in genere convengono che le operazioni di trattamento, proprio per dar luogo ad una sorta di monitoraggio, siano certificate da un revisore esterno proprio per tutelare ora i dati dei dipendenti ora quelli dei clienti; portando cosi, anche ad un abbattimento dei costi dei tempi per tutti i soggetti coinvolti.

Quindi piuttosto che gravare la multinazionale di un onere di monitoraggio, sull'effettiva tutela dei diritti degli interessati, tale operazione viene demandata ad un soggetto terzo[109]che dovrà presentare annualmente un *memorandum* che descriverà le operazioni di trattamento poste in essere dal responsabile di questo e valutare se queste siano conformi in primo luogo alle BCR e di conseguenza agli standard europei[110].

In definitiva dunque, il quesito che si pone è quello di valutare se il monitoraggio delle operazioni da parte della multinazionale debba restare un diritto esercitabile discrezionalmente, nelle forme appena descritte, ovvero se sia necessario individuare un obbligo vero e proprio di monitoraggio.

Sul punto, ci si potrebbe accostare al pensiero di una persuasiva dottrina, la quale non è favorevole all'introduzione di un obbligo di monitoraggio a carico della multinazionale, poiché questa, concludendo un gran numero di contratti con i vari responsabili del

[107] **F. Cafaggi,** *New Foundations of transnational private regulation*, EUI Working papers RSCAS 2010/53.
[108] **F. Cafaggi***, New Foundations of transnational private regulation*, EUI Working papers RSCAS 2010/53.
[109] Sul punto si veda Capitolo IV, paragrafo II (La figura del DPO).
[110] **E. A. Bart van Reeken** Outsourcing, *een juridische gids voor de praktijk*, third edition, Kluwer 2009.

trattamento, si troverebbe a dover fronteggiare un aumento sproporzionato di costi e di sforzi per verificare il rispetto del diritto alla tutela dei dati personali[111].

Tuttavia sarà sempre nell'interesse della multinazionale, assicurarsi che i dati trasferiti siano correttamente trattati nel rispetto delle adeguate garanzie. Quindi si può sostenere che in capo al titolare sussista un diritto al monitoraggio del trattamento, il quale oltre ad essere discrezionale nel suo utilizzo, lo sarà anche sulle modalità con cui sarà fatto valere, cioè o attraverso un revisore esterno ovvero attraverso forze messe in campo dal titolare delle stesse.

Ovviamente, fatta salva la possibilità di quale misura scegliere per verificare il rispetto del diritto alla protezione dei dati personali, sussisterà sempre, in capo alla multinazionale un *principio di responsabilità*[112] in caso di lesione del diritto dell'interessato. Il quale altro non è che un requisito del regime delle BCR, le quali ammettono che gli interessati possano agire nei confronti della multinazionale qualora questa non riesca a tutelare i diritti dei primi[113].

§ 3.3. La facoltatività delle BCR

Si può affermare che le BCR non sono obbligatorie, ma solo in determinate circostanze.

In primo luogo, il loro contenuto non è tassativo, sia perché queste possono essere integrate da altre condizioni contrattuali non contrastanti con l'obbligo di fornire le adeguate tutele, sia perché le parti possono ovviamente stabilire di modificare di volta in volta il contenuto medesimo.

Ovviamente, in quest'ultimo caso dovranno essere sottoposte al vaglio della Lead DPA prescelta, per valutare se rispettano gli standard di adeguatezza comunitari.

In secondo luogo, la facoltatività si rinviene quando il sistema legislativo del paese terzo abbia già ricevuto il riconoscimento di adeguatezza dalla Commissione europea.

[111] **E. M. L. Moerel,** Binding *corporate rules: Fixing the regulatory patchwork of data protection*. Tilburg University, 2011.
[112] *V. Cap. IV*.
[113] In materia di Responsabilità si veda *Cap. IV.*

Ad oggi, questo è il caso della Svizzera, Canada, e di tutte quelle società americane che aderiscono ai principi dello *SHIELD*[114].

Infine, tale facoltatività, sempre in ordine al contenuto, si evince anche dalla lettura dell'art. 47 del Regolamento n. 679 del 2016, il quale al paragrafo 1 fissa gli elementi per far sì che queste siano approvate dalla Lead DPA, nel fare ciò però la norma, non individua degli specifici elementi ma, delinea solo delle linee guida generali le quali sono:

- *che le BCR siano giuridicamente vincolanti e si applichino a tutti i membri del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;*
- *che conferiscano direttamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;*
- *che soddisfino i requisiti di cui al paragrafo 2.*

§ 3.4. La non esclusività delle BCR

Come si può evincere dalla lettura dell'art. 46 del Regolamento n. 679 del 2016, le BCR non sono le uniche tipologie di clausole utilizzabili per consentire il trasferimento dei dati personali verso paesi terzi, la cui legislazione non garantisca un'adeguata tutela del diritto alla protezione dei dati personali.

Poiché l'articolo in questione dà la possibilità al titolare e al responsabile del trattamento di compiere tali trasferimenti anche quando il rispetto delle adeguate garanzie sia rappresentato da:

[114] La Commissione europea ha adottato il 12 luglio 2016 una decisione in merito al *cosiddetto Privacy Shield*. Esso è l'accordo che regolamenta il trasferimento di dati tra Unione Europea e USA.
L'accordo è volto a proteggere i diritti fondamentali delle persone nell'UE i cui dati personali vengano trasferiti negli Stati Uniti, e stabilisce regole certe per le imprese che effettuano trasferimenti di dati al di là dell'Atlantico. Essa in particolare prevede: (i) obblighi di protezione stringenti per le imprese che trasferiscono dati; (ii) misure di sicurezza in materia di accesso ai dati da parte del Governo degli Stati Uniti; (iii) strumenti specifici per la tutela delle persone fisiche. Detto accordo è seguito alle indicazioni della Corte di Giustizia europea, che il 6 ottobre 2015 aveva dichiarato non valida la decisione della Commissione del 2000 sullo scambio di dati tra UE e Usa, il cosiddetto *Safe Harbour*. Cfr. **McCormac, Brian**: *Invalidation of Safe Harbor*, in Iowa Lawyer, Vol. 76, Issue 2 (March 2016); **Alvarez, Daniel**, *Safe Harbor Is Dead; Long Live the Privacy Shield*, Business Law Today, Vol. 2016, Issue 5 (May 2016). **McCusker, Shona**: *EU-US Privacy Shield: The Antidote to the Transatlantic Data Transfer Headache*, Business Law Review, Vol. 37, Issue 3 (June 2016).

- un (generico) strumento vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici (art. 46, par. 2 lett. a);
- da clausole contrattuali tipo, adottate dalla Commissione (art. 46, par. 2 lett. c);
- da clausole contrattuali tipo adottate da un'autorità di controllo (DPA) e approvate successivamente dalla Commissione (46, par. 2 lett. d);
- un codice di condotta approvato a norma dell'articolo 40 dello stesso Regolamento, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati (46, par. 2 lett. e);
- un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati (46, par. 2 lett. f).

§ 3.5. La non esaustività delle BCR

Come abbiamo avuto modo di vedere per le caratteristiche sopra citate, l'art. 47 del Regolamento n. 679 del 2016 non fornisce un modello al quale riferirsi per definire il complesso di BCR come esaustive.

Da un lato, come abbiamo visto, perché l'articolo fissa semplicemente gli elementi per far sì che le BCR redatte dalle parti siano approvate dalla Lead DPA, e dall'altro sulla base degli spunti forniti dal WP 29, il testo contrattuale una volta sottoposto al vaglio dell'organismo medesimo, questo può richiedere alle parti anche di operare modifiche alle BCR elaborate per far sì che queste possano garantire le tutele adeguate.

Tuttavia, è possibile sostenere che una tale interpretazione presta il fianco a delle riserve, ad esempio perché la Direttiva 95/46 prima, e il Regolamento n. 679 del 2016 poi, non sono fonti giuridiche familiari per le aziende soggette alla legislazione di paesi che non fanno parte dell'UE.

Questo di fatto provoca una condizione di incertezza sulla precisa interpretazione delle BCR e quindi un probabile ridimensionamento del loro ruolo.

§ 3.6. L'obbligatorietà delle BCR

Alla luce della dinamicità delle BCR che abbiamo analizzato nei paragrafi precedenti, occorre porre una particolare attenzione nello studio di questa caratteristica, poiché tale obbligatorietà interessa solo determinati contesti.

Alla luce dell'art. 47 del Regolamento n. 679 del 2016 infatti, il profilo dell'obbligatorietà rileva solo in ordine all'indirizzo che le imprese devono seguire, per far sì che le BCR possano essere approvate dalla Lead DPA, e non anche in ordine al contenuto materiale delle stesse. Quindi il concetto di obbligatorietà va inteso solo in questa accezione.

§ 4. Le parti della catena contrattuale

§ 4.1. Le BCR per i titolari del trattamento

Il regime delle BCR, sviluppato sulla base degli elaborati del WP 29, affronta come punto fondamentale gli obblighi che i titolari del trattamento devono rispettare affinché possano essere assicurate adeguate garanzie di tutela ai dati personali degli interessati. Infatti, come risulta non solo dal testo della Direttiva 95/46 ma anche dall'art. 47 del Regolamento n. 679 del 2016, gli obblighi di protezione dei dati personali sono rivolti direttamente al titolare del trattamento e non anche al responsabile.

Per fornire un esempio di quanto appena detto, possiamo notare che le multinazionali, nel corso delle loro attività commerciali trattano diversi tipi di dati, le cui principali categorie sono:

1. i dati dei dipendenti,
2. i dati personali dei clienti, de fornitori e dei partner commerciali,
3. specifiche categorie di dati.

Ad esempio, se prendiamo in considerazione l'ultima categoria di dati e le lavorazioni che su di essi svolgono le industrie farmaceutiche possiamo notare come tale azienda, avendo a disposizione una grande quantità di dati dei propri consumatori, costituirà dei

rapporti la cui controparte non può essere considerata né un dipendente, né un cliente e né un partner commerciale. Quindi è indubbio che in una tale situazione l'onere di garantire un adeguato trattamento dei dati personali graverà per forza di cose sull'azienda farmaceutica come titolare del trattamento.

Può tuttavia accadere che, in alcuni casi, le società del gruppo agiscano anche in qualità di responsabile del trattamento per conto di altri gruppi societari controllati, e questo ad esempio è il caso in cui una multinazionale ha centralizzato le sue operazioni di elaborazione in un centro di approvvigionamento dati condiviso. Ma anche in questo caso, la medesima multinazionale che svolga le operazioni di elaborazione dei dati, alla luce della disciplina delle BCR sarà sempre considerata come titolare del trattamento e quindi "garante" delle adeguate tutele per i dati degli interessati.

Tale impostazione invece, non troverà applicazione nel caso in cui la società del gruppo che elabora i dati, compirebbe tale operazione per conto di un titolare esterno, poiché in questo caso troverebbero applicazione le BCR per i responsabili.

§ 4.1.1. Il confronto tra le BCR per il trattamento dei dati dei dipendenti e quelle per il trattamento dei dati dei clienti.

A. Il modello di BCR per il trattamento dei dati dei dipendenti.

B. Il modello di BCR per il trattamento dei dati dei clienti.

Sebbene sia auspicabile, all'interno della stessa multinazionale, una politica sulla protezione dei dati durante il loro trasferimento e trattamento uniforme per tutte le categorie degli stessi nella prassi ciò non avviene, in quanto le aziende tendono a trattare i dati dei propri dipendenti e clienti separatamente.

Tale prassi è ovviamente frutto delle scelte manageriali, secondo le quali, al fine di perseguire i principi di economicità nella gestione aziendale, preferiscono operare attraverso dei modelli di tutela differenti proprio sulla base delle differenti caratteristiche che le predette tipologie di dati hanno.

Per capire queste differenze possiamo ad esempio pensare ai dati dei clienti, che possono essere trattati attraverso le regole dettate per il marketing diretto, ossia con la regola sullo specifico consenso per tale finalità oppure quando il trattamento trova la sua

leggittimità, ad esempio sull'esecuzione del contratto di lavoro del dipendente.

Da un altro punto di vista inoltre, tali distinte categorie di dati, possono essere trattati da società diverse all'interno della stessa multinazionale; ad esempio i dati dei clienti sono trattati dal reparto marketing mentre quelli dei dipendenti dal reparto delle risorse umane.

Per capire nello specifico come operano queste distinte tipologie di BCR possiamo rifarci ai due modelli di riferimento. Tali modelli incorporano tutti i requisiti necessari delle BCR che abbiamo già descritto e quindi hanno trovato approvazione anche da parte di diverse DPAs[115].

Per ragioni di sintesi in tali modelli saranno riportati solo gli articoli chiave che, alla luce del discorso che si sta conducendo, esprimono la *policy* che le multinazionali dovrebbero realizzare al fine di garantire una piena ed efficace tutela del diritto alla protezione dei dati personali durante il loro trasferimento.

[115] Nell'aprile del 2011, il WP 29 ha pubblicato un elaborato nel quale sono contenute le tipologie di BCR approvate, si tratta di clausole utilizzate da quindici differenti multinazionali che hanno trovato l'approvazione di cinque distinte Leads DPAs (Regno Unito, Francia, Lussemburgo, Olanda e Germania). (fonte: http://ec.europa.eu/justice/policies/privacy/binding_rules/bcr_cooperation_en.htm.)

A Il modello di BCR per il trattamento dei dati dei dipendenti.

[Company]

Privacy Code for Employee Data

Introduction

[Company] has committed itself to the protection of personal data of [Company] employees in the [Company] **[Code of Conduct]**.

This Privacy Code for Employee Data indicates how this principle shall be implemented. For the privacy code applicable to customer, supplier and business partner data, refer to the *Privacy Code for Customer, Supplier and Business Partner Data*. **[insert hyperlink to Code]**

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of [Company] Employees (**Employee Data**) by [Company] or a Third Party on behalf of [Company].
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Employee Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Employees keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Employee Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, this Code shall apply.
Sub-policies and notices	1.4	[Company] may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The [**Responsible Executive**] shall be responsible for compliance with this Code.
Effective Date	1.6	This Code has been adopted by the **[Head of Legal or Head of Compliance]** of **[Company Holding]** and shall enter into force as of [ ] (**Effective Date**) and shall be published on the **[Company Intranet]** and be made available to Employees upon request.
Code supersedes prior policies	1.7	This Code supersedes all [Company] privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	This Code shall be implemented in the [Company] organization based on the timeframes specified in Article 21.
Role of [Company EU Headquarters]	1.9	[Company Holding] has tasked [Company EU Headquarters] with the coordination and implementation of this Code.

Article 2 – Purposes for Processing Employee Data

Legitimate Business Purposes

2.1 Employee Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (**Business Purposes**):

(i) **[Human resources and personnel management.** This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the employment-at-will relationship, e.g. management and administration of recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, and Employee communications

(ii) **Business process execution and internal management.** This purpose addresses activities such as scheduling work, recording time, managing company assets, provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, implementing business controls, and managing and using Employee directories

(iii) **Health, safety and security.** This purpose addresses activities such as those involving occupational safety and health, the protection of company and Employee assets, and the authentication of Employee status and access rights

(iv) **Organizational analysis and development and management reporting.** This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis

(v) **Compliance with legal obligations.** This purpose addresses the Processing of Employee Data as necessary for compliance with a legal obligation to which [Company] is subject or

(vi) **Protecting the vital interests of Employees.** This is where Processing is necessary to protect the vital interests of an Employee.

list all categories of business purposes]

Where there is a question whether a Processing of Employee Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Employee consent

2.2 Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes must exist for any Processing of Employee Data. If applicable local law so requires, in addition to having a Business Purpose for the relevant Processing, [Company] shall also seek Employee consent for the Processing. If none of the Business Purposes applies, [Company] may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee.

A request for Employee consent requires the authorization of the appropriate Privacy Officer prior to seeking consent.

Denial or withdrawal of Employee consent 2.3 The Employee may both deny consent and withdraw consent at any time without consequence to his employment relationship. Where Processing is undertaken at the Employee's request (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.

When seeking Employee consent, [Company] must inform the Employee:

(i) of the purposes of the Processing for which consent is requested
(ii) of the possible consequences for the Employee of the Processing and
(iii) that he is free to refuse and withdraw consent at any time without consequence to his employment relationship.

Limitations on Processing Data of Dependants of Employees 2.4 [Company] will Process Data of Dependants of an Employee if:

(i) the Data were provided with the consent of the Employee or the Dependant
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship or
(iii) the Processing is required or permitted by applicable local law.

Article 10 – Transfer of Employee Data to Third Parties

Transfer to Third Parties 10.1 This Article sets forth requirements concerning the transfer of Employee Data from [Company] to a Third Party. Note that a transfer of Employee Data includes situations in which [Company] discloses Employee Data to Third Parties (e.g. in the context of corporate due diligence) or where [Company] provides remote access to Employee Data to a Third Party.

Third Party Controllers and Third Party Processors 10.2 There are two categories of Third Parties:

(i) **Third Party Processors**: these are Third Parties that Process Employee Data solely on behalf of [Company] and at its direction (e.g. Third Parties that Process Employee salaries on behalf of [Company])
(ii) **Third Party Controllers**: these are Third Parties that Process Employee Data and determine the purposes and means of the Processing (e.g. government authorities or service providers that provide services directly to Employees).

Transfer for applicable Business Purposes only 10.3 [Company] shall transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose for which the Employee Data are Processed (including Secondary Purposes as per Article 3 or purposes for which the Employee has provided consent in accordance with Article 2).

Third Party Controller contracts 10.4 Third Party Controllers (other than government agencies) may Process Employee Data only if they have a written contract with [Company]. In the contract, [Company] shall seek to contractually protect the data protection interests of its Employees. All such contracts shall be drafted in consultation with the appropriate Privacy Officer.

Third Party Processor contracts 10.5 Third Party Processors may Process Employee Data only if they have a written contract with [Company]. The contract with a Third Party Processor must include the following provisions:

(i) the Processor shall Process Employee Data only in accordance with [Company]'s instructions and for the purposes authorized by [Company]

(ii) the Processor shall keep the Employee Data confidential

(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Employee Data

(iv) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to [Company] without the prior written consent of [Company]

(v) [Company] has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by [Company] or any relevant government

authority

(vi) the Third Party Processor shall promptly inform [Company] of any actual or suspected security breach involving Employee Data and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide [Company] with all relevant information and assistance as requested by [Company] regarding the security breach.

Transfer of Data to a Non-Adequate Country

10.6 This Article sets forth additional rules for the transfer of Employee Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Employee Data (**Non-Adequate Country**).

Employee Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Employee, for managing the employment-at-will relationship or to take necessary steps at the request of the Employee prior to entering into a contract or an employment-at-will relationship, e.g. for processing job applications

(ii) a contract has been concluded between [Company] and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any)

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Employee between [Company] and a Third Party (e.g. in case of the booking of an airline ticket)

(iv) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection

(v) the Third Party has implemented binding corporate rules or a similar transfer control mechanisms which provide adequate safeguards under applicable law

(vi) the transfer is necessary to protect a vital interest of the Employee

(vii) the transfer is necessary for the establishment, exercise or defence of a legal claim

(viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society or

(ix) the transfer is required by any law to which the relevant Group Company is subject.

Items (viii) and (ix) above require the prior approval of the Chief Privacy Officer.

Employee consent for transfer

10.7 [Company] generally shall not seek Employee consent for a transfer of Employee Data to a Third Party located in a Non-Adequate Country. One of the grounds for transfer listed in Article 10.6 must exist. If applicable local law so requires, in addition to having one of the grounds listed in Article 10.6, [Company] shall also seek Employee consent for the relevant transfer. If none of the grounds listed in Article 10.6 exists, [Company] may request Employee consent for a transfer to a Third Party located in a Non-Adequate Country, but only if

(i) the transfer has no foreseeable adverse consequences for the Employee or
(ii) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Requesting Employee consent for a transfer requires the prior approval of the appropriate Privacy Officer. Prior to requesting Employee consent, the Employee shall be provided with the following information:

(i) the purpose of the transfer
(ii) the identity of the transferring Group Company
(iii) the identity or categories of Third Parties to which the Data will be transferred
(iv) the categories of Data that will be transferred
(v) the country to which the Data will be transferred and
(vi) the fact that the Data will be transferred to a Non-Adequate Country.

Transfers between Non-Adequate Countries

10.8 This Article sets forth additional rules for transfers of Employee Data that were collected in connection with the activities of a Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 10.6, these transfers are permitted if they are:

(i) necessary for compliance with a legal obligation to which the relevant Group Company is subject
(ii) necessary to serve the public interest or
(iii) necessary to satisfy a Business Purpose of [Company].

Article 12 – Supervision and compliance

Chief Privacy Officer

12.1 **[Company EU Headquarters] [of [Company Holding]?]** shall appoint a Chief Privacy Officer who is responsible for:

(i) supervising compliance with this Code
(ii) providing periodic reports, as appropriate, to the **[Head of Legal/Head of Compliance]** on data protection risks and compliance issues and
(iii) coordinating, in conjunction with the appropriate Privacy Officer, official investigations or inquiries into the Processing of Data by a government authority.

Privacy Council 12.2 [The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for:

(i) the development, implementation and updating of local Employee data protection policies and procedures
(ii) the development of the policies, procedures and system information (as required by Article 13)
(iii) the development, implementation and updating of the training and awareness programs
(iv) the monitoring and reporting on compliance with this Code
(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints and
(vi) determining and updating appropriate sanctions for violations of this Code (e.g. disciplinary standards).]

Privacy Officers 12.3 Each Group Company shall designate a Privacy Officer. **[The Chief Privacy Officer shall act as the Privacy Officer for [Company Holding]]** These Privacy Officers may, in turn, establish a network of Privacy Officers sufficient to direct compliance with this Code within their respective organizations.

The Privacy Officers shall:

(i) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues
(ii) maintain (or ensure access to) an inventory of the system information (as required by Article 13.2)
(iii) establish a framework for a privacy compliance program as required by the Chief Privacy Officer and
(iv) cooperate with the Chief Privacy Officer and the other Privacy Officers, and the **[[Company] Compliance Officers]**.

Responsible Executive 12.4 **[Tasks and responsibilities of Responsible Executive]**

Default Privacy Officer 12.5 If at any moment in time there is no Privacy Officer designated for a function or business, the designated **[compliance officer for the [Company] Code of Conduct]** for the relevant function or business is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position 12.6 Where a Privacy Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

B Il modello di BCR per il trattamento dei dati dei clienti.

[Company]

Privacy Code for Customer, Supplier and Business Partner Data

Introduction

[Company] has committed itself to the protection of personal data of [Company] Customers, Suppliers and Business Partners in the [Company] [Code of Conduct].

This Code indicates how this principle shall be implemented. For the rules applicable to Employee Data, refer to the *Privacy Code for Employee Data*. **[hyperlink]**

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Customers, Suppliers and Business Partners by [Company] or a Third Party on behalf of [Company]. This Code does not address the Processing of Employee Data of [Company].
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Individuals keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.
Sub-policies and notices	1.4	[Company] may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The [**Responsible Executive**] shall be responsible for compliance with this Code.
Effective	1.6	This Code has been adopted by the **[Head of Legal or Head of**

Date		**Compliance]** of **[Company Holding]** and shall enter into force as of [ ] (Effective Date) and shall be published on the [Company website and Company intranet] and be made available to Individuals upon request.
Code supersedes prior policies	1.7	This Code supersedes all [Company] privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	This Code shall be implemented in the [Company] organization based on the timeframes specified in Article 22.
Role of [Company EU Headquarters]	1.9	[Company Holding] has tasked [Company EU Headquarters] with the coordination and implementation of this Code.

Article 2 – Purposes for Processing Personal Data

Legitimate Business Purposes 2.1 Personal Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (**Business Purposes**):

[(i) **Development and improvement of products and/or services.** This purpose includes Processing that is necessary for the development and improvement of [Company] products and/or services, research and development.

(ii) **Conclusion and execution of agreements with Customers, Suppliers and Business Partners.** This purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Customers, Suppliers and Business Partners and to record and financially settle delivered services, products and materials to and from [Company]

(iii) **Relationship management and marketing.** This purpose addresses activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls and the development, execution and analysis of market surveys and marketing strategies.

(iv) **Business process execution, internal management and management reporting.** This purpose addresses activities such as managing company assets, conducting internal audits and investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes managing mergers, acquisitions and divestitures, and Processing Personal Data for management reporting and analysis.

(v) **Health, safety and security.** This purpose addresses activities such as those involving safety and health, the protection of [Company] and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights

(vi) **Compliance with legal obligations.** This purpose addresses the Processing of Personal Data necessary for compliance with a legal obligation to which [Company] is subject; or

(vii) **Protection vital interests of Individuals.** This is where Processing is necessary to protect the vital interests of an Individual.]

Where there is a question whether a Processing of Personal Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Consent 2.2 If a Business Purpose does not exist or if applicable local law so requires [Company] shall (also) seek consent from the Individual for the Processing.

Where Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.

When seeking consent, [Company] must inform the Individual:

(i) of the purposes of the Processing for which consent is required and

(ii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any) and how Individuals can exercise their rights).

Denial or withdrawal of consent 2.3 The Individual may both deny consent and withdraw consent at any time.

Article 11 – Transfer of Personal Data to Third Parties

Transfer to Third Parties 11.1 This Article sets forth requirements concerning the transfer of Personal Data from [Company] to a Third Party. Note that a transfer of Personal Data includes situations in which [Company] discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where [Company] provides remote access to Personal Data to a Third Party

Third Party Controllers and Third Party Processors 11.2 There are two categories of Third Parties:

(i) **Third Party Processors**: these are Third Parties that Process Personal Data solely on behalf of [Company] and at its direction (e.g., Third Parties that Process online registrations made by Customers)

(ii) **Third Party Controllers**: these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., [Company] Business Partners that provide their own goods or services directly to Customers).

Transfer for applicable Business Purposes only 11.3 [Company] shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 3 or purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller contracts 11.4 Third Party Controllers (other than government agencies) may Process Personal Data only if they have a written contract with [Company]. In the contract, [Company] shall seek to contractually safeguard the data protection interests of its Individuals. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. Individual Business Contact Data may be transferred to a Third Party Controller without a contract if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to Individual's job responsibilities.

Third Party Processor contracts 11.5 Third Party Processors may Process Personal Data only if they have a written contract with [Company]. The contract with a Third Party Processor must include the following provisions:

(i) the Processor shall Process Personal Data only in accordance

with [Company]'s instructions and for the purposes authorized by [Company]

(ii) the Processor shall keep the Personal Data confidential

(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data

(iv) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to [Company] without the prior written consent of [Company]

(v) [Company] has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by [Company] or any relevant government authority

(vi) the Third Party Processor shall promptly inform [Company] of any actual or suspected security breach involving Personal Data and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide [Company] with all relevant information and assistance as requested by [Company] regarding the security breach.

Transfer of Data to a Non-Adequate Country

11.6 This Article sets forth additional rules for the transfer of Personal Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Personal Data (**Non-Adequate Country**).

Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Individual, for managing a contract with Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders

(ii) a contract has been concluded between [Company] and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any)

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between [Company] and a Third Party (e.g. in case of recalls)

(iv) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection

(v) the Third Party has implemented binding corporate rules or a similar transfer control mechanisms which provide adequate safeguards under applicable law

(vi) the transfer is necessary to protect a vital interest of the Individual

(vii) the transfer is necessary for the establishment, exercise or defence of a legal claim

(viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society or

(ix) the transfer is required by any law to which the relevant Group Company is subject.

Items (viii) and (ix) above require the prior approval of the Chief Privacy Officer.

Consent for transfer 11.7 If none of the grounds listed in Article 11.6 exist or if applicable local law so requires [Company] shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country.

Prior to requesting consent, the Individual shall be provided with the following information:

(i) the purpose of the transfer
(ii) the identity of the transferring Group Company
(iii) the identity or categories of Third Parties to which the Data will be transferred
(iv) the categories of Data that will be transferred
(v) the country to which the Data will be transferred and
(vi) the fact that the Data will be transferred to a Non-Adequate Country.

Article 2.3 applies to denial or withdrawal of consent.

Transfers between Non-Adequate Countries 11.8 This Article sets forth additional rules for transfers of Personal Data that were collected in connection with the activities of a Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 11.6, these transfers are permitted if they are:

(i) necessary for compliance with a legal obligation to which the relevant Group Company is subject
(ii) necessary to serve the public interest or
(iii) necessary to satisfy a Business Purpose of [Company].

Article 13 – Supervision and compliance

Chief Privacy Officer 13.1 **[Company EU Headquarters] [of [Company Holding]?]** shall appoint a Chief Privacy Officer who is responsible for:

(i) supervising compliance with this Code
(ii) providing periodic reports, as appropriate, to the **[Head of Legal/Head of Compliance]** on data protection risks and compliance issues and
(iii) coordinating, in conjunction with the appropriate Privacy Officer, official investigations or inquiries into the Processing of Data by a government authority.

Privacy Council 13.2 [The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for:

(i) the development, implementation and updating of local Individual data protection policies and procedures
(ii) the development of the policies, procedures and system information (as required by Article 14)
(iii) the development, implementation and updating of the training and awareness programs
(iv) the monitoring and reporting on compliance with this Code
(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints and
(vi) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).]

Privacy Officers 13.3 Each Group Company shall designate a Privacy Officer. [The Chief Privacy Officer shall act as the Privacy Officer for [Company Holding]] These Privacy Officers may, in turn, establish a network of Privacy Officers sufficient to direct compliance with this Code within their respective organizations.

The Privacy Officers shall:

(i) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues

(ii) maintain (or ensure access to) an inventory of the system information (as required by Article 14.2)

(iii) establish a framework for a privacy compliance program as required by the Chief Privacy Officer and

(iv) cooperate with the Chief Privacy Officer and the other Privacy Officers, and the **[[Company] Compliance Officers]**.

Responsible Executive 13.4 **[Tasks and responsibilities of Responsible Executive]**

Default Privacy Officer 13.5 If at any moment in time there is no Privacy Officer designated for a function or business, the designated **[compliance officer for the [Company] Code of Conduct]** for the relevant function or business is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position 13.6 Where a Privacy Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

§ 4.2. Le BCR per i responsabili del trattamento

Sulla base del discorso fin ora condotto, nell'ambito di un contratto di trasferimento e di elaborazione di dati personali verso un paese terzo, si è analizzato che le BCR, le quali svolgono una funzione volta a garantire gli standard europei in ambito di trattamento dei dati personali, sono il frutto di un'elaborazione condotta dalla società del gruppo che ha sede nel territorio dell'UE. Quindi, come titolare del trattamento, sarà questa società a garantire che i dati trattati presso un'altra società del gruppo, sita fuori dall'UE, godranno sempre delle garanzie presenti entro confini europei.

Quindi, il regime delle BCR è un costrutto che per ovvie ragioni deve essere accostato al titolare del trattamento, mentre il responsabile dovrà semplicemente elaborare (e dunque trattare) i dati alla luce delle indicazioni da questo fornitegli.

Sembrerebbe quindi una forzatura individuare delle BCR con cui è lo stesso responsabile a garantire degli adeguati standard di tutela.

Tuttavia, così non è in quanto può avvenire che nell'ambito di un processo all'interno di una multinazionale vi sia l'esigenza di elaborare dei dati per conto dei propri clienti, e in questo caso si tratta di attività che vanno al di fuori del campo di applicazione delle BCR per il titolare. In questo ambito possiamo ad esempio annoverare le operazioni commerciali, come l'elaborazione di un libro paga per conto del cliente, e questa è l'ipotesi in cui la multinazionale, pur non operando come titolare ma come responsabile deve farsi garante delle adeguate tutele sui dati trattati.

Alla luce di ciò quindi, non appare destituito di fondamento, considerare la possibilità di redazione delle BCR da parte dello stesso soggetto incaricato del trattamento, nella misura in cui sarà il responsabile stesso a tutelare il rispetto delle garanzie europee nel caso in cui decida di elaborare i dati del proprio cliente presso una società del gruppo con sede al di fuori dell'UE.

§ 5. La procedura di approvazione delle BCR

Per ciò che concerne la procedura di approvazione delle BCR, questa va distinta in due momenti, il primo ha ad oggetto il rapporto che intercorre tra la multinazionale che

intende munirsi di queste clausole e l'Autorità di controllo alla quale le BCR saranno sottoposte per ottenere l'approvazione; il secondo, invece, riguarda i rapporti tra questa DPA prescelta (Lead DPA) e le Autorità di controllo degli altri Paesi europei, affinché il giudizio espresso dalla predetta DPA sia condiviso dalle altre, nell'ottica dunque di un monolitico sistema di tutele europee.

Partendo dal primo momento, in linea di principio una multinazionale dovrebbe richiedere l'approvazione delle sue BCR in tutti gli Stati membri ove sia presente un suo stabilimento. Sul punto, tuttavia, occorre rilevare che il WP 29 aveva inizialmente introdotto una c.d. "procedura di cooperazione europea"[116] con la quale appunto la multinazionale poteva sottoporre la valutazione delle sue BCR ad un'unica DPA prescelta, ovvero la Lead DPA che era quella rappresentata da quella presente nello Stato ove l'impresa aveva la maggior parte dei propri interessi. Una volta che poi l'elaborato fosse arrivato al vaglio di tale Autorità di controllo, questa l'avrebbe sottoposta all'attenzione delle altre DPAs la cui approvazione era necessaria per il definitivo riconoscimento.

Sulla base delle prime positive esperienze dovute dall'ausilio di questa procedura, si è passati ad un'evoluzione della medesima, si tratta di un modello che ad oggi non è ancora sposato da tutte le DPAs europee. Si tratta del *Mutual Recognition Procedure* - MRP, la differenza che intercorre tra le due procedure attiene al fatto che con la seconda non è più necessaria l'approvazione da parte delle altre DPAs, poiché queste riconosceranno mutualmente, come adeguate, ciascuna delle bozze di BCR che verranno sottoposte di volta in volta alle Leads DPAs senza una ulteriore revisione.

L'MRP, richiede che venga nominata una Lead DPA, la quale sarà assistita da altre due DPAs incaricate della revisione del progetto delle BCR, tali Co-Leads DPAs sono scelte tra le Autorità di controllo degli Stati ove la multinazionale abbia "una forte presenza".

La procedura di approvazione delle BCR dunque, si presenta così articolata:

1. La multinazionale presenta la sua bozza di BCR alla DPA che ritiene opportuno operi come Lead DPA;
2. La multinazionale elenca gli Stati membri ove vi sia dislocata una propria sede;

[116] WP 29, Documento di lavoro con cui si stabilisce una procedura di cooperazione per il rilascio di pareri congiunti in merito alle adeguate garanzie derivanti dalle "Norme d'impresa vincolanti" ("Binding Corporate Rules") 14 aprile 2005 - WP 107.

3. La DPA, prescelta avviserà le DPAs di cui al punto 2 della scelta operata dalla multinazionale di eleggere la prima Lead DPA e per sollecitarne il consenso;

4. Dopo il consenso ad operare come Lead DPA, questa selezionerà le Co-Leads DPAs;

5. Quindi si apre la fase della consultazione, tra la proposta della multinazionale e gli indirizzi della Lead DPA;

6. Fase dell'emendazione delle BCR (eventuale);

7. La Lead DPA approva informalmente il testo delle BCR, tenuto conto del parere delle Co-Leads DPA;

8. La Lead DPA presenta il testo alle altre DPAs del MRP che rispondono (positivamente al testo) nel termine di un mese dalla data di presentazione;

9. Infine vi è l'approvazione formale del testo da parte della Lead DPA.

Come abbiamo anticipato in apertura di paragrafo, la procedura di approvazione delle BCR, deve essere distinta in due momenti, l'uno che riguarda il rapporto che intercorre tra la multinazionale e l'approvazione del suo testo da parte delle Autorità, e l'altro invece che attiene (nello specifico) ai rapporti tra le varie Autorità di controllo nazionali.

Il meccanismo che porta all'approvazione delle BCR, nel contesto delle varie DPAs nazionali ha avuto una profonda evoluzione, il punto d'origine è ovviamente rappresentato dalla "Direttiva Madre" la quale, al Capo VII individuava nei meccanismi di cooperazione e coerenza gli strumenti con i quali le Autorità nazionali giungevano all'approvazione di documenti trasversalmente accettati. Ovviamente gli articoli in esso contenuti non riguardavano esclusivamente le BCR, ma si trattava di procedure con le quali qualsiasi misura, redatta in ambito nazionale, che avesse ad oggetto la tutela del diritto alla protezione dei dati personali, potesse essere riconosciuta in tutto il territorio dell'Unione.

Dalla disciplina 95/46, anche alla luce del meccanismo di MRP, ci si è anche se non in senso assoluto allontanati, e ad oggi il meccanismo con le quali le BCR, e tutti gli strumenti di tutela per la protezione dei dati personali, per essere riconosciuti su tutto il territorio comunitario devono rispettare le disposizioni in materia di coerenza cosi come riportate dai disposti degli artt. 60 ss. del Regolamento n. 679 del 2016.

Si tratta quindi di meccanismi, quello di cooperazione e quello di coerenza, che contribuiscono all'applicazione uniforme di tutti gli strumenti di tutela.

A questo punto dunque, analizzeremo i vari articoli del Regolamento proprio per approfondire quelle parti del procedimento di approvazione delle BCR che interessano i rapporti tra le varie DPAs.

Partendo dall'art. 60 del Regolamento n. 679 del 2016 questo stabilisce che: *"1. L'autorità di controllo capofila coopera con le altre autorità di controllo interessate conformemente al presente articolo nell'impegno per raggiungere un consenso. L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili.*

2. L'autorità di controllo capofila può chiedere in qualunque momento alle altre autorità di controllo interessate di fornire assistenza reciproca a norma dell'articolo 61 e può condurre operazioni congiunte a norma dell'articolo 62, in particolare per lo svolgimento di indagini o il controllo dell'attuazione di una misura riguardante un titolare del trattamento o responsabile del trattamento stabilito in un altro Stato membro.

3. L'autorità di controllo capofila comunica senza indugio le informazioni utili sulla questione alle altre autorità di controllo interessate. Trasmette senza indugio alle altre autorità di controllo interessate un progetto di decisione per ottenere il loro parere e tiene debitamente conto delle loro opinioni.

4. Se una delle altre autorità di controllo interessate solleva un'obiezione pertinente e motivata al progetto di decisione entro un termine di quattro settimane dopo essere stata consultata conformemente al paragrafo 3 del presente articolo, l'autorità di controllo capofila, ove non dia seguito all'obiezione pertinente e motivata o ritenga l'obiezione non pertinente o non motivata, sottopone la questione al meccanismo di coerenza di cui all'articolo 63.

5. L'autorità di controllo capofila, qualora intenda dare seguito all'obiezione pertinente e motivata sollevata, trasmette un progetto di decisione riveduto alle altre autorità di controllo interessate per ottenere il loro parere. Tale progetto di decisione riveduto è soggetto alla procedura di cui al paragrafo 4 entro un termine di due settimane.

6. Se nessuna delle altre autorità di controllo interessate ha sollevato obiezioni al progetto di decisione trasmesso dall'autorità di controllo capofila entro il termine di cui ai paragrafi 4 e 5, si deve considerare che l'autorità di controllo capofila e le autorità di controllo interessate concordano su tale progetto di decisione e sono da esso vincolate.

7. L'autorità di controllo capofila adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato la decisione in questione, compresa una sintesi dei fatti e delle motivazioni pertinenti. L'autorità di controllo cui è stato proposto un reclamo informa il reclamante riguardo alla decisione.

8. In deroga al paragrafo 7, in caso di archiviazione o di rigetto di un reclamo, l'autorità di controllo cui è stato proposto il reclamo adotta la decisione e la notifica al reclamante e ne informa il titolare del trattamento.

9. Se l'autorità di controllo capofila e le autorità di controllo interessate convengono di archiviare o rigettare parti di un reclamo e di intervenire su altre parti di tale reclamo, è adottata una decisione separata per ciascuna di tali parti della questione. L'autorità di controllo capofila adotta la decisione per la parte riguardante azioni in relazione al titolare del trattamento e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o del responsabile del trattamento sul territorio del suo Stato membro e ne informa il reclamante, mentre l'autorità di controllo del reclamante adotta la decisione per la parte riguardante l'archiviazione o il rigetto di detto reclamo, la notifica a detto reclamante e ne informa il titolare del trattamento o il responsabile del trattamento.

10. Dopo aver ricevuto la notifica della decisione dell'autorità di controllo capofila a norma dei paragrafi 7 e 9, il titolare del trattamento o responsabile del trattamento adotta le misure necessarie per garantire la conformità alla decisione per quanto riguarda le attività di trattamento nel contesto di tutti i suoi stabilimenti nell'Unione. Il titolare del trattamento o responsabile del trattamento notifica le misure adottate per conformarsi alla decisione all'autorità di controllo capofila, che ne informa le altre autorità di controllo interessate.

11. Qualora, in circostanze eccezionali, un'autorità di controllo interessata abbia motivo di ritenere che urga intervenire per tutelare gli interessi degli interessati, si applica la procedura d'urgenza di cui all'articolo 66.

12. L'autorità di controllo capofila e le altre autorità di controllo interessate si scambiano reciprocamente con mezzi elettronici, usando un modulo standard, le informazioni richieste a norma del presente articolo".

Dalla lettura dell'articolo dunque, si può evincere la stretta collaborazione che intercorre tra le varie DPA in ordine all'approvazione di un progetto tra cui quelli sulle BCR.

Tale collaborazione, o meglio, cooperazione, risulta ancor più chiara dai contributi che le DPAs estranee alle Co-Leads DPAs possono fornire prima di approvare, in questo caso un testo contenente BCR, poiché, come indicato dall'art. 61 del Regolamento n. 679 del 2016, vige un principio di assistenza reciproca, il quale fa sì che:

"1. Le autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente Regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini.

2. Ogni autorità di controllo adotta tutte le misure opportune necessarie per dare seguito alle richieste delle altre autorità di controllo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta. Tali misure possono consistere, in particolare, nella trasmissione di informazioni utili sullo svolgimento di un'indagine.

3. La richiesta di assistenza contiene tutte le informazioni necessarie, compresi lo scopo e i motivi della richiesta. Le informazioni scambiate sono utilizzate ai soli fini per cui sono state richieste.

4. L'autorità di controllo richiesta non deve rifiutare di dare seguito alla richiesta, salvo che:

A. non sia competente per trattare l'oggetto della richiesta o per le misure cui deve dare esecuzione; o

B. l'accoglimento della richiesta violi le disposizioni del presente Regolamento o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta.

5. L'autorità di controllo richiesta informa l'autorità di controllo richiedente dell'esito o, a seconda dei casi, dei progressi delle misure adottate per rispondere alla richiesta. L'autorità di controllo richiesta deve fornire le motivazioni del rigetto della richiesta.

6. Di norma, le autorità di controllo richieste forniscono con mezzi elettronici, usando un modulo standard, le informazioni richieste da altre autorità di controllo.

7. Le autorità di controllo richieste non impongono alcuna spesa per le misure da loro adottate a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare disposizioni di indennizzo reciproco per spese specifiche risultanti dalla prestazione di assistenza reciproca in circostanze eccezionali.

8. Qualora l'autorità di controllo non fornisca le informazioni di cui al paragrafo 5 del presente articolo, entro un mese dal ricevimento della richiesta di un'altra autorità di controllo, l'autorità di controllo richiedente può adottare misure provvisorie nel territorio del suo Stato membro ai sensi dell'articolo 55, paragrafo 1. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che sia necessaria una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

9. La Commissione può, mediante atti di esecuzione, specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni con mezzi elettronici tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2".

A tale procedura tra le Autorità di controllo europee, si aggiunge poi un altro tassello molto importante, cioè quello della necessità, per la Lead DPA di assumere il parere da parte del Comitato europeo per la protezione dei dati personali.

Per dovere di completezza, le modalità, e gli ulteriori casi, fuori dal regime delle BCR in cui va assunto tale parere sono riportati all'art. 64 del Regolamento n. 679 del 2016, secondo il quale:

"Il comitato emette un parere ove un'autorità di controllo competente intenda adottare una delle misure in appresso. A tal fine, l'autorità di controllo competente comunica il progetto di decisione al comitato, quando la decisione:

A. è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

B. riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente Regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;

C. è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;

D. è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 46, paragrafo 2, lettera d), e all'articolo 28, paragrafo 8;

E. è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); oppure

F. è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.

2. Qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere, in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62.

3. Nei casi di cui ai paragrafi 1 e 2, il comitato emette un parere sulla questione che gli è stata presentata, purché non abbia già emesso un parere sulla medesima questione. Tale parere è adottato entro un termine di otto settimane a maggioranza semplice dei membri del comitato. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione. Per quanto riguarda il progetto di decisione di cui al paragrafo 1 trasmesso ai membri del comitato conformemente al paragrafo 5, il membro che non abbia sollevato obiezioni entro un termine ragionevole indicato dal presidente è considerato assentire al progetto di decisione.

4.Senza ingiustificato ritardo, le autorità di controllo e la Commissione comunicano per via elettronica, usando un modulo standard, al comitato tutte le informazioni utili, in particolare, a seconda del caso, una sintesi dei fatti, il progetto di decisione, i motivi che rendono necessaria l'attuazione di tale misura e i pareri delle altre autorità di controllo interessate.

5. Il presidente del comitato informa, senza ingiustificato ritardo, con mezzi elettronici:

A. i membri del comitato e la Commissione di tutte le informazioni utili che sono state comunicate al comitato con modulo standard. Se necessario, il segretariato del comitato fornisce una traduzione delle informazioni utili; e

B. l'autorità di controllo di cui, secondo i casi, ai paragrafi 1 e 2, e la Commissione in merito al parere, che rende pubblico.

6. L'autorità di controllo competente si astiene dall'adottare il suo progetto di decisione di cui al paragrafo 1 entro il termine di cui al paragrafo 3.

7. L'autorità di controllo di cui al paragrafo 1 tiene nella massima considerazione il parere del comitato, e entro due settimane dal ricevimento del parere, comunica per via elettronica, usando un modulo standard, al presidente del comitato se intende mantenere o modificare il progetto di decisione, e se del caso, il progetto di decisione modificato.

8. Se entro il termine di cui al paragrafo 7 del presente articolo l'autorità di controllo interessata informa il presidente del comitato, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, si applica l'articolo 65, paragrafo 1".

Dalla lettura dei precedenti articoli del Regolamento n. 679 del 2016, è possibile evincere come la necessità di collaborazione da parte delle Autorità di controllo nazionali, sia al centro dell'ideale del progetto europeo, e tale sinergia si può realizzare solo facendo applicazione di tali meccanismi di cooperazione e coerenza.

Ovviamente, per il discorso che si sta conducendo, l'attenzione va posta su come il testo di BCR trovi approvazione a livello europeo sulla base di tale meccanismo.

Tuttavia, non occorre dimenticare, che i meccanismi in parola, rispondono ad esigenze più grandi, ogni qual volta che un'autorità nazionale voglia dare applicazione ad una misura vincolante che interessi anche le altre DPA dovrà farlo sotto la guida di queste procedure. Solo attraverso di esse si può giungere all'applicazione coerente ed uniforme del Regolamento sulla protezione dei dati personali in tutto il territorio dell'Unione Europea.

§ 6. La vincolatività delle BCR

§ 6.1. La vincolatività interna

Come abbiamo avuto modo di analizzare, le BCR non rappresentano solo degli strumenti per far sì che siano assicurate adeguate garanzie sulla protezione dei dati personali quando questi sono trasferiti in paesi terzi, ovvero un espediente limitativo delle operazioni che possono essere effettuate sotto l'accezione di trattamento.

Infatti le BCR, sono anche espressione dei rapporti che si instaurano all'interno della stessa multinazionale tra le varie società. A tale compito, assolve il requisito della vincolatività interna delle BCR.

Sotto questo aspetto, tale vincolatività, rileva ai fini della determinazione della responsabilità contrattuale nel caso di violazione degli obblighi di fornire adeguate garanzie di tutela. Nello specifico, anche sulla base del lavoro operato dal WP 29, la società con sede all'interno dell'UE, dunque il titolare del trattamento, sarà considerata responsabile in caso di risarcimento del danno anche qualora questo sia cagionato dal responsabile stesso durante le operazioni di elaborazione dei dati.

È in questo contesto dunque che si inserisce la vincolatività, affinché nell'ambito delle norme vincolanti d'impresa vengano inserite clausole con le quali l'eventuale risarcimento del danno, una volta corrisposto dal titolare del trattamento, dia a questo la facoltà di rivalersi sul responsabile del trattamento qualora si sia reso inadempiente.

§ 6.2. La vincolatività esterna

Circa il profilo della vincolatività esterna, questo riguarda il rapporto che intercorre tra la sede della multinazionale che ha presentato il progetto di BCR all'Autorità di controllo di un determinato Stato membro, e le altre DPAs degli altri Stati comunitari ove la multinazionale vanta la maggior parte dei propri interessi.

Si tratta di un fenomeno, che fondamentalmente ricalca il secondo profilo della procedura di approvazione delle BCR (*v. par. 5*), cioè garantire ed assicurare che il modello approvato in un determinato Stato membro sia riconosciuto a livello europeo.

Ad oggi, sulla base del lavoro effettuato con il Regolamento n. 679 del 2016, la vincolatività esterna ha perso parte della sua importanza, perché attraverso i meccanismi di cooperazione e coerenza, il riconoscimento in tutto il territorio dell'Unione, delle misure prese a livello nazionale, è uno degli aspetti fondamentali per rispettare i principi del Regolamento stesso.

Il problema dunque si poneva nel passato quando, dopo l'approvazione dell'MRP era necessario riconoscere la validità delle BCR nei paesi comunitari che non avessero aderito a questa soluzione. Quindi onde evitare l'applicazione della farraginosa "procedura di cooperazione europea", si preferiva concludere degli accordi bilaterali tra la

Lead DPA e la DPA estranea all' MRP che potessero far riconoscere la validità, e quindi la esterna vincolatività, delle BCR anche nello Stato membro non aderente alla procedura dell'MRP.

CAPITOLO IV: La responsabilità delle multinazionali nel trasferimento di dati attraverso le B.C.R.: dall'*accountability principle* al *Data Protection Officer*

§ 1. Il principio di accountability: dalla definizione all'introduzione nel Regolamento n. 679 del 2016

Nel 2009 il WP 29 insieme al WP della polizia e giustizia (Working Party Police Justice - WPPJ) hanno redatto un documento congiunto chiamato "The future of Privacy", nel quale hanno espresso il loro punto di vista circa l'impianto normativo europeo, presente nella Direttiva Madre, inerente alla protezione dei dati personali durante il loro trasferimento. Il punto sul quale i due gruppi hanno posto maggiormente l'attenzione, attiene al fatto che l'impianto normativo, cosi come formulato allora, non era in grado di assicurare un'efficiente opera di protezione dei dati attraverso i requisiti espressi nella Direttiva 95/46. Poiché la normativa comunitaria non era considerata come uno strumento sufficiente per dare attuazione ai requisiti di protezione.

Per migliorare questa situazione i due WP proposero dunque, alla Commissione europea, di introdurre un principio di "*accountability"* nella Direttiva 95/46.

Prima di analizzare le proposte di intervento che i due WP hanno suggerito, è doveroso chiarire cosa si intenda per *accountability*. Ebbene, il termine, letteralmente tradotto significa responsabilità, tuttavia è chiaro questa può essere intesa sotto una miriade di accezioni a seconda del contesto nel quale è inserita.

Quindi, nel contesto della protezione dei dati personali, il termine *accountability* racchiude il più ampio significato che la responsabilità possa abbracciare. Si tratta dunque di un principio che spazia dalla responsabilità contrattuale fino a quella aquilana. È evidente che fornire una chiara e generale definizione di questo principio è un'impresa alquanto ardua, e nel contesto che si sta analizzando, ciò che è effettivamente rilevante, è tenere ben presente solo il fatto che sarà il titolare (e il responsabile) del trattamento a dover rispettare tale principio di accountability.

Questo vuol dire che tali soggetti saranno "responsabili", durante il trasferimento di dati personali attraverso l'ausilio delle BCR, di assicurare le adeguate garanzie di protezione dei dati personali (presenti nel Regolamento n. 679 del 2016) quando il trattamento sarà operato fuori dai confini dell'UE.

La visione secondo la quale la responsabilità possa avere diverse chiavi di lettura a seconda dei differenti linguaggi e impianti legislativi, non è sfuggita neanche ai due WP, che nella necessità di evidenziare le differenze tra responsabilità e *accountability* hanno affermato:

"The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning – even though defining what exactly accountability means is complex. In general terms though, its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed"[117].

È dunque evidente che i due WP hanno preferito procedere descrivendo, le misure richieste per una corretta attuazione del principio di accountability, piuttosto che sulla definizione della medesima. In breve, i punti salienti dispongono che il titolare del trattamento abbia il compito di:

- Rendere effettive, appropriate ed efficaci le misure adottate per rendere concreto il processo di protezione dei dati cosi come indicato dalla Direttiva 95/46;
- Su richiesta della DPA presentare queste ulteriori misure di protezione.

Sia la Commissione europea, che *European Commision - EC communication* nella revisione della Direttiva 95/46 indicarono che, avrebbero valutato dei metodi che potessero assicurare che il titolare del trattamento mettesse in pratica delle politiche e dei meccanismi efficienti al fine di assicurare la conformità del trattamento dei dati alle regole sulla protezione dei medesimi. Nel fare ciò, il titolare ha dovuto sempre tener conto del dibattito riguardo alla possibilità di introdurre il principio di accountability[118].

Tale principio non è del tutto nuovo, ed è stato già applicato in altri campi giuridici. Esso è uno dei più rilevanti principi della OECD (Organisation for Economic Co-operation and Development) privacy Guidelines, APEC (Asia-Pacific Economic Cooperation), Canadian Piped, ISO DRAFT standard 29100 (il quale delinea il frame

[117] WP 29 and WPPJ: "*The Future of Privacy" Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, adopted on 01 December 2009.
[118] Proposta di revisione della Direttiva 96/46, Commissione europea, novembre 2010.

work della privacy), draft Australian privacy principles, FTC (Federal Trade Commission) Proposed Framework for Consumer Privacy.

Sulla base dunque del lavoro operato dai due WP, circa la necessità di inserire questo principio nel contesto del trasferimento dei dati personali, e sulla difficoltà di addivenire ad una precisa definizione del medesimo, il risultato è facilmente individuabile all'interno del Regolamento n. 679 del 2016 agli artt. 24 e 82.

I suddetti articoli dispongono rispettivamente che:

1. *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3.L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento".

"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2.Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente Regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente Regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso

trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5.Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6.Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2".

Dalla lettura degli articoli quindi, appaiono chiari due elementi, il primo attiene al fatto che l'*accountability* non viene definita nei suoi caratteri essenziali ma attraverso gli oneri che sussistono in capo al titolare del trattamento per far sì che siano garantite le adeguate tutele al diritto alla protezione dei dati. Il secondo invece attiene al fatto che l'*accountability*, quale principio di responsabilità che dà luogo a risarcimento del danno, abbraccia tutte le tipologie in cui questo si possa manifestare ("chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento […]").

§ 1.1. Il principio di *accountability* nel contesto delle BCR: un approccio basato sul "rischio"

L'accountability deriva da un approccio basato sul rischio, dove le compagnie stesse adeguano il loro sforzo di conformità alle disposizioni del Regolamento n. 679 del 2016 in relazione al livello di rischio in gioco. Nel caso specifico si tratta di elaborare tipologie di BCR diverse a seconda del contesto nel quale queste dovranno trovare applicazione. Questa analisi, ovviamente calza con molte indicazioni del Regolamento stesso, il quale richiede tra le altre cose, appropriate misure di sicurezza e una adeguata salvaguardia dei dati.

In linea con quanto appena detto, in passato, già il WP 29 iniziò a ragionare su un approccio basato sul rischio indicandolo come punto di partenza dei due maggiori obiettivi della Direttiva 95/46 (che di fatto sono quasi totalmente sovrapponibili a quelli del Regolamento).

Il primo obiettivo perseguito era quello di "*garantire un buon livello di conformità, riconoscendo che il cento per cento della conformità non è ottenibile nella pratica*"[119].

Il WP 29 inoltre ha applicato l'approccio basato sul rischio al contenuto delle obbligazioni relative alla protezione, cioè raccomandando misure di sicurezza più stringenti nel caso di trasferimento di dati sensibili e identificando come priorità il potenziamento delle DPAs[120].

Questo approccio basato sul rischio costituisce dunque, la maniera nella quale le multinazionali gestiscono la protezione dei propri dati personali, e i partecipati a tale network gestiscono il rischio; nel senso che lo accettano, cercano di eliminarlo ovvero minimizzarlo o trasferirlo ai responsabili del trattamento attraverso l'inserimento di particolari tipologie di BCR.

In definitiva quindi la protezione dei dati è regolata attraverso la gestione ed allocazione del rischio, visto che nel contesto di protezione dei dati sono coinvolti molteplici attori sembra impossibile per il legislatore europeo normare il flusso di dati in

---

[119] WP 29, Document n. WP 12, art. 7: *"The objectives of a data protection system are essentially threefold: 1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them"*.

[120] WP 29, Document n. WP 12, art. 28: "It would constitute guidance regarding which cases of data transfer should be considered as 'priority cases' for examination or even investigation, and thereby allow the resources available to be directed towards those transfers which raise the greatest concerns in terms of the protection of data subjects.
The Working Party considers that among those categories of transfer which pose particular risks to privacy and therefore merit particular attention are the following:
- those transfers involving certain sensitive categories of data as defined by Article 8 of the directive;
- transfers which carry the risk of financial loss (e.g. credit card payments over the Internet);
- transfers carrying a risk to personal safety;
- transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- repetitive transfers involving massive volumes of data (such as transactional data processed over telecommunications networks, the Internet etc.);
- transfers involving the collection of data using new technologies, which, for instance could be undertaken in a particularly covert or clandestine manner (e.g. Internet cookies)."

modo che, la regolamentazione imposta, non comporti un onere tale da annichilire ogni volontà, ovvero policy, aziendale della gestione del rischio nel trattamento di dati. Ciò di converso bloccherebbe ogni possibilità di trasferimento di dati al di fuori delle società stesse.

§ 1.2. Dall'approccio basato sul rischio ai livelli di apprendimento

Nel traslare il discorso normativo nella pratica, è ovviamente richiesto che i principi di tutela che regolano il trattamento dei dati e che fanno da base all'accountability, siano tradotti in istruzioni pratiche che il titolare (o il responsabile) del trattamento fornirà ai propri dipendenti in modo da istruirli su come trattare i dati personali ovvero su come redigere le BCR da inserire nel contratto di trasferimento.

I dipendenti dovranno seguire un percorso articolato in tre fasi: addestramento, conformità e monitoraggio. Affinché ciò avvenga è ovviamente necessario che le multinazionali introducano delle proprie policy e programmi di conformità.

Se questo può essere inteso come un ragionamento generale, che guarda al trattamento dei dati in tutte le sue sfaccettature, per le multinazionali che si servono delle BCR, al fine di analizzare come debba essere inteso il rispetto del principio di *accountability*, è bene guardare con maggiore attenzione alla fase dell'apprendimento.

La fase dell'apprendimento, o anche l'approccio basato sull'apprendimento, può essere inteso come il momento nel quale la multinazionale fissa i requisiti che le proprie BCR devono contenere. Questo momento viene definito dallo stesso WP 29 "*primo livello di apprendimento".*

A questo punto, prosegue il WP 29, le (ipotetiche) patologie delle BCR, che possono dar luogo ad una violazione del principio di *accountability*, si rinvengono nella mancanza di altri due livelli di apprendimento.

Il *"secondo livello di apprendimento"* dovrebbe essere caratterizzato da un'ulteriore revisione, che la multinazionale dovrebbe operare sul proprio regime di BCR, una volta che queste abbiano ricevuto l'autorizzazione da parte della Lead DPA.

Mentre il *"terzo livello di apprendimento"* sarebbe costituito dalla necessita di colmare le eventuali lacune del primo.

Appare dunque evidente che, alla luce di questo terzo livello di apprendimento, risulta agevole collegare il rischio alla violazione del principio di accountability. Poiché nel momento in cui si ammetta l'impossibilità di prevedere tutte le "patologie" che possano attaccare il regime di BCR, e quindi non fornire un primo livello di apprendimento adeguato, allora ci si muoverà in quel contesto di rischio ove, l'importanza del principio di *accountability* rischia di essere compromesso, con conseguenze ben più onerose per la multinazionale.

Il discorso appena fatto è rilevante per poter sostenere che, sebbene si sia raggiunto un buon livello di attenzione sul rispetto della protezione dei dati attraverso l'introduzione (implicita) del principio di *accountability*, ulteriori innovazioni sono ancora possibili.

La conclusione è che il raggiungimento di un efficace sviluppo delle BCR, è possibile solo nel momento in cui le multinazionali smettano di considerarle solo come uno strumento per la gestione (e valutazione) del rischio e le utilizzino anche come strumento per raggiungere il secondo livello di apprendimento.

Questo può essere affrontato introducendo, come ulteriore requisito delle BCR l'onere che vengano periodicamente riviste sotto la luce del principio di *accountability*, così da poter operare delle modifiche ove necessarie[121].

Un altro elemento che manca nell'attuale regime, è come la Commissione europea e il *Board* possano essere incluse o coinvolte in questo programma di apprendimento delle multinazionali e quindi operare una collaborazione che possa essere in grado di migliorare le strategie che portano alla redazione delle BCR (in altri termini si tratta di capire come raggiungere il terzo livello di apprendimento).

Parte di questo processo di apprendimento può essere raggiunto dalla Commissione europea organizzando gruppi di lavoro a cui può essere attribuito il compito di definire, per esempio, le finalità del principio di *accountability* nel trasferimento di dati verso paesi terzi.

Un'altra proposta potrebbe essere quella di capire se è utile includere nel regime delle BCR un più completo sistema di feedback da parte delle multinazionali riguardante la valutazione dei loro programmi di BCR in rapporto alla *compliance* che devono rispettare.

Tuttavia, sulla base della procedura di approvazione delle BCR, una tale metodologia per raggiungere il terzo livello di apprendimento potrebbe non apparire del tutto

[121] Per una più attenta analisi consulta: "Centre for Information Policy Leadership".

percorribile poiché, la Lead DPA è già incaricata di ricevere tali valutazioni, previa richiesta, in luce degli stringenti requisiti di informazione che sono ad essa riconosciuti in forza del *par. 1 lett. A)* dell'art. 58 del Regolamento n. 679 del 2016, secondo il quale: *"Ogni autorità di controllo ha tutti i poteri di indagine seguenti: a) ingiungere al titolare del trattamento e al responsabile del trattamento, e ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti".*

Dunque si potrebbe sostenere che un tale approccio andrebbe solo ad incrementare l'onere amministrativo che grava sulle multinazionali, portando inoltre, ad un sovraccarico informativo della Lead DPA.

§ 1.3. Il Rapporto tra i requisiti delle BCR e quelli del principio di accountability

§ 1.3.1. I requisiti del principio di accountability

Il WP 29, nell'analizzare il futuro della privacy, ha anche emanato un elaborato sul principio di accountability analizzando anche le sue elaborazioni pratiche[122].

Il WP 29, ha proposto la seguente indicazione concreta:

"Article X – Implementation of data protection principles

1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request".

Nel suo elaborato, il WP 29 ha evidenziato il fatto, che l'introduzione delle indicazioni di cui sopra nella Direttiva Madre non costituissero dei requisiti dell'accountability,

[122]Cfr. **P. de Hert, V. Papakonstantinou, D. Wright** and **S. Gutwirth**, *The proposed Regulation and the construction of a principles-driven system for individual data protection' (2013) 26(1-2) Innovation: The European Journal of Social Science Research 133, 139, where the authors contend that the 'discussions from a legal point of view date as far back as 2009* (emphasis added) i.e. when the Article 29 Working Party adopted an opinion on the principle of accountability (Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability' WP 173).

infatti, continua il WP 29 "*most of the requirements set out in this provision actually already exist, albeit less explicitly, under existing laws*".

Alla luce di ciò dunque, le "nuove" indicazioni non hanno lo scopo di rendere i titolari del trattamento soggetti al nuovo principio ma piuttosto assicurare de facto una efficace *compliance* con le norme già esistenti.

Come conseguenza del rispetto della *compliance* in relazione al principio di accountability, il WP 29 ha affermato che:

> *"highlights that fulfilling the accountability principle does not necessarily mean that a controller is incompliance with the substantive principles […], i.e., it does not offer a legal presumption of compliance nor does it replace any of those principles. […] In practice however, companies with a robust compliance program are according to the Working Party 29 more likely to be in compliance with the law"*[123].

Tuttavia, ben più importante è la precisazione che il WP 29 fa riguardo al fatto che il rispetto della *compliance* in riferimento al principio di accountability può giocare un ruolo fondamentale nel valutare le sanzioni che le DPAs possono impartite nelle ipotesi di violazioni dei principi sostanziali.

Dopo questa introduzione, che disegna la considerevole importanza che il principio di accountability ha nel far rispettare le previsioni del Regolamento n. 679 del 2016, è necessario cercare di delimitare i contorni di questo principio.

Come già in precedenza sostenuto, all'interno del Regolamento, il principio, sebbene di notevole importanza resta nascondo all'interno di determinate disposizioni, pertanto, al fine di coglierne le caratteristiche fondamentali è necessario rifarsi al già citato elaborato del WP 29.

Il WP 29 ha fornito una lista (non esaustiva) di requisiti del principio di accountability, si tratta di undici punti e sono i seguenti:

1. *establishing internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc).*
2. *setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc.), which should be available to data subjects.*

[123] Cfr. *supra* Nota 122.

3. mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations.

4. appointing a data protection officer and other individuals with responsibility for data protection.

5. offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.

6. setting up procedures to manage access, correction and deletion requests which should be transparent to data subjects.

7. establishing an internal complaints handling mechanism.

8. setting up internal procedures for the effective management and reporting of security breaches.

9. performing privacy impact assessments in specific circumstances.

10. implementing and supervising verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc).

The Working Party 29 further notes that "transparency is an integral part of the accountability measures, both vis-à-vis the data subjects and the public in general". Examples of transparency measures that increase accountability include

11. *publishing privacy policies on the internet, by providing transparency in regard to internal complaints procedures and through publication in annual reports.*

§ 1.3.2. Il confronto tra i requisiti delle BCR e quelli del principio di *accountability*

Avendo ora elencato i requisiti che impone il principio di *accountability* nel contesto di una corretta *compliance* del Regolamento, si può passare ora al raffronto con quelli delle BCR e valutare i punti di contatto e di distanza nel novero della tutela del diritto alla protezione dei dati personali. Inoltre, si analizzerà se è auspicabile che gli ulteriori (o differenti) requisiti presenti nel regime di *accountability* siano inclusi in quelli sulle BCR.

Sulla base di quanto già detto nei capitoli precedenti, attraverso l'elencazione dei requisiti delle BCR effettuata dal WP 29, è possibile rilevare una sostanziale sovrapposizione tra i due. Ciò è avvalorato dal fatto che nell'elaborato sul principio di *accountability* le BCR già riflettono (per la natura della loro funzione) questo principio.

Discorso inverso invece se si guarda ai requisiti designati per l'*accountability,* il cui elenco pone in luce cinque ulteriori elementi, i quali, come si vedrà, sono formulati in modo molto più esplicito e diretto.

Pertanto questi ulteriori cinque requisiti possono essere così suddivisi, quelli indicati ai numeri 1, 3 e 9 presentano una formulazione più chiara ed esplicita, mentre, quelli ai numeri 8 e 11 si presentano del tutto addizionali rispetto all'elenco elaborato per le BCR.

Partendo dai requisisti più chiari ed espliciti, dei quali si riporta il testo:

1. establishing internal procedures prior to the creation of new personal data processing operations;

2. mapping procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations;

3. *performing privacy impact assessments in specific circumstances*.

Non è messo in discussione che i requisiti appena ricordati dovrebbero essere inclusi nella *policy* di una multinazionale, così da renderla in grado di "garantire" (come *compliance*) le operazioni di trattamento dei dati. Tuttavia, sebbene fino ad ora ciò non è esplicitamente incluso come requisito della BCR, in pratica le multinazionali sono conformi con questi requisiti.

Ad oggi il regime delle BCR richiede una dettagliata descrizione del trattamento e del flusso di dati. Tuttavia per le multinazionali non è possibile giungere ad una totale applicazione dei tre principi sopra citati (quindi inserirli nel regime di BCR), poiché, la grande quantità di operazioni di trattamento che queste compiono, si pone come una discriminante insuperabile rispetto a questa completa attuazione. Si noti dunque che, per essere in grado di garantire le loro operazioni di trattamento (nel senso che sono in grado di conoscere quali sistemi adoperare e se questi sono conformi alla protezione), le multinazionali pongono in essere dei PIA (*Privacy Impact Assestment*) o DPIA (*Data Protection Impact Assestment*) meglio note come "valutazioni d'impatto", al momento dell'implementazione di nuovi sistemi di elaborazione dei dati o di modifiche di quelli già esistenti. La DPIA è una procedura finalizzata a descrivere il trattamento e a valutarne, in

particolare la necessità e la proporzionalità, così da facilitare la gestione e la minimizzazione dei rischi che ne possono derivare per i diritti e le libertà degli interessati.

Dunque è possibile considerare queste operazioni come espressione dell'applicazione della policy aziendale in materia di protezione dei dati, e in seguito a tali operazioni sarà verificata la conformità di questo PIA alle norme di protezione dati da una figura indipendente chiamata DPO (*Data Protection Officer*).

Se il DPO rileva una qualche violazione nel rispetto della *compliance* (attraverso il principio di *accountability* ovvero attraverso le BCR), il sistema di trattamento dei dati viene conseguentemente adattato.

In conclusione, non è in discussione che questi tre requisiti elencati dal WP 29 dovrebbero essere parte del programma di protezione dei dati, tuttavia non possono far parte dei requisiti delle BCR nella loro forma attuale. Da ciò dunque è possibile evincere una non totale sovrapposizione tra la protezione dei dati così come elencata e auspicata dal regime delle BCR, e i requisiti indicati dal principio di *accountability*.

Le ragioni principali per le quali questo avviene, sono che questi requisiti cosi formulati sono troppo specifici e incorporano il rischio di agire sebbene a tutela della *compliance* senza un effettivo collegamento con la medesima.

Piuttosto, le regole di *accountability* dovrebbero essere formulate come un "*framework*" per catturare la capacità delle multinazionali di organizzarsi (da sole) e renderle responsabili per il prodotto del loro trattamento in relazione all'impegno nell'assicurare una valida ed efficace *compliance*.

Come è possibile dunque collegare questi tre (più espliciti) requisiti del principio di *accountability* al regime di BCR? Si potrebbe sostenere che questi possano essere riformulati come oneri generali per le multinazionali volti ad avere dei sicuri contorni da seguire per rispettare la *compliance* del Regolamento e quindi allo stesso tempo dando la possibilità di muoversi su una valutazione del rischio che si presenta, di fatto, dinamico.

Come detto in precedenza la non totale sovrapposizione tra le due elencazioni di requisiti, riposa anche sull' esistenza di requisiti del principio di *accountability* del tutto addizionali rispetto a quelli delle BCR. I quali sono:

- *being transparent on the internal complaints procedure (assuming such transparency concerns the number and nature of the complaints filed rather than only the existence of the complaints procedure it self) and on its data protection compliance also in its annual report;*

- *setting up an internal procedures for the effective management and reporting of security breaches.*

Circa il requisito della trasparenza di cui al paragrafo precedente, sarebbe auspicabile che questo venga incluso nel regime delle BCR. Poiché, come è evidente, il volano per la *compliance* sulla protezione dei dati nelle multinazionali è la reputazione e la trasparenza delle loro operazioni, e ciò ovviamente, ricalca la valutazione delle BCR come forma di TPR (*Transnational Private Regoulation*).

Mentre invece il requisito di cui al *punto 8* del paragrafo che precede, concernente le procedure interne per la efficace gestione e notifica relativa alle varie lacune della sicurezza, si può fare lo stesso ragionamento fatto per il requisito precedente, poiché in questo caso, l'introduzione di questo requisito nel regime delle BCR, darebbe maggiore completezza al raggiungimento della più alta forma di *compliance*.

Come dunque è ragionevole pensare, questi *additional requirements*, andrebbero anche aggiunti agli elementi costitutivi delle BCR, inoltre, per avere il controllo del processo di trattazione dei dati, una multinazionale dovrebbe avere un inventario delle proprie operazioni di trattamento dei dati come anche delle sue operazione dinamiche di gestione del rischio per il rispetto della *compliance.*

§ 2. Il Data Protection Officer

Fondato sul principio di *accountability* (responsabilizzazione) il Regolamento 679/2016 ha introdotto, nel Considerando 97 la figura del *Data Protection Officer* (di seguito, "DPO") quale cardine della propria *compliance*.

Alla luce del dettato normativo emerge che per alcuni titolari e responsabili del trattamento è prescritto l'obbligo di nomina del DPO. In particolare l'autorità pubblica e gli organismi pubblici, sono tenuti alla sua nomina prescindendo dai dati oggetto del trattamento. Tale obbligo incombe anche su quelle società che come attività principale effettuano un monitoraggio regolare e su larga scala delle persone fisiche, ovvero che trattano su larga scala categorie particolari di dati personali. Inoltre, al di là delle ipotesi di obbligatorietà sopra menzionate, la nomina di un DPO può anche avvenire su base volontaria.

Si tratta di un soggetto che nell'esercizio delle sue funzioni deve godere di indipendenza e deve essere terzo rispetto al titolare o al responsabile del trattamento.

Il DPO è designato in funzione delle sue qualità professionali, in qualità di figura altamente specializzata in materia informatica e/o di elevata competenza giuridica soprattutto in materia di tutela dei diritti dei dati personali[124]. Il DPO ha il compito di valutare la gestione e l'organizzazione dei trattamenti dati al fine di garantire un'adeguata protezione dei medesimi all'interno delle società e/o degli enti pubblici. In aggiunta alle competenze prettamente professionali assumono rilevanza anche le qualità di carattere personale come l'integrità morale, lo spirito d'iniziativa, la capacità di collaborazione con i dipendenti, la capacità di organizzazione e l'abilità nella gestione di situazioni complesse[125]. Il DPO o Responsabile Protezione Dati (RDP) non è però una figura totalmente nuova. Essa era già nota nella Direttiva 95/46, la quale, però, non prescrivendone la nomina obbligatoria è di fatto rimasta inattuata sul punto[126].

Il DPO è inoltre, una figura che si collega "a doppio binario" con la società in quanto, da un lato esercita le sue funzioni per far sì che la società rispetti i caratteri dell'*accountability principle*, dall'altro, invece, si pone come una sorta di "piccolo garante" chiamato a guidare l'impresa, o l'Ente, nella realizzazione della "*compliance*": facilitando la responsabilizzazione dei soggetti per i quali opera, il DPO non solo favorisce il rispetto della normativa, ma rende maggiormente competitive le aziende.

Come sopra ricordato, la figura del DPO ha assunto notevole importanza nel passaggio dalla "Direttiva Madre" al Regolamento 679/2016: importanza che si è accentuata per la maggiore attenzione rivolta dalla normativa comunitaria alla *compliance.*

---

[124] Cfr. **A. BAMBERGER – K. MULLIGAN**, *New Governance, Chef Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Iniquity*, in Law&Policy, Vol 33, Issue 4, 2011, pp. 477-508.

[125] L' AEDP – l'autorità spagnola – è stata la prima autorità europea per la protezione dei dati che ha introdotto un quadro di riferimento per la certificazione della figura del DPO.

[126] In ambito europeo, essa era presente nelle legislazioni della Germania e dell'Austria. In ambito internazionale, una figura similare a quella del DPO di cui al Regolamento 679/2016, il *privacy officer* (agente della privacy) è stata istituita per la prima volta nel 1999 dalla Società All Advantage (USA – California), specializzata in servizi pubblicitari attraverso internet e la funzione fu ricoperta dall'Avv. Ray Everett Church, il quale in una intervista affermò: <<[…] Quando nel 1999 sono stato nominato Chef privacy officer il mio ruolo è stato il primo nel suo genere: una posizione di dirigente con il compito di vigilare su tutte le questioni legate alla privacy […]>>. V. *PRIVACY protezione e trattamento dei dati*, a cura di **M. Soffientini**, Wolters Kluwer Italia, 2016, p. 172.

A riprova di ciò è possibile citare l'art. 18 della Direttiva 95/46 dal quale emerge palese la scarsa importanza riservata al DPO, citato in maniera blanda nel paragrafo 2 e solo come uno strumento meramente alternativo alla notificazione all'Autorità di controllo.

A tale situazione, come vedremo meglio nel proseguo, ha sopperito il Regolamento 679/2016 che ha disciplinato in maniera chiara e puntuale detta figura prevedendone l'obbligatorietà in cassi specifici. Questa scelta può essere letta alla luce di una duplice finalità figlia del medesimo obiettivo: da un lato, garantire una adeguata *compliance* aziendale predisponendo valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati (strumenti di *accountability*); dall'altro, ad esso strettamente collegato, garantire un'adeguata tutela dei dati personali durante il loro trattamento che sia espressione delle tutele che il Regolamento intende applicare in modo omogeneo su tutto il territorio dell'Unione.

Il DPO, così individuato, rappresenta un *trait-d'union* fra i soggetti interessati al trattamento, l'Autorità di controllo e la divisione operative dell'ente o della società.

Inoltre, va osservato come il Regolamento 679/2016 faccia gravare al titolare ed al responsabile del trattamento la responsabilità per l'inosservanza delle sue norme: spetta, infatti, a costoro, *ex* art. 24, paragrafo 1, garantire ed essere in grado di provare che i trattamenti effettuati siano conformi al regolamento medesimo. Ulteriore onere posto a carico dei medesimi soggetti è di garantire al DPO autonomia e risorse sufficienti per adempiere in maniera efficace i propri doveri.

Il Legislatore europeo ha dedicato tre articoli del Regolamento 679/2016 alla figura del DPO: l'art. 37, che tratta principalmente della sua designazione; l'art. 38, che disciplina la sua collocazione all'interno dell'organismo aziendale o dell'ente pubblico; l'art 39, che individua i compiti chiamato ad assolvere.

§ 2.1. La designazione del DPO: Art. 37 del Regolamento n. 679 del 2016

Dalla lettura dell'art. 37 del Regolamento 679/2016 emerge che la nomina del DPO da parte del titolare e del responsabile del trattamento è obbligatoria in tre ipotesi[127]:

- se il trattamento è svolto da un'autorità pubblica o un organismo pubblico;
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
- se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati[128] o di dati personali relativi a condanne penali e reati.

Il Gruppo di lavoro *ex* art. 29 suggerì, qualora un soggetto titolare o responsabile del trattamento non sia, ai sensi della normativa europea, obbligato alla nomina di un DPO, quale norma di "*best practice*", di documentare comunque le analisi che, compiute in seno alle proprie aziende o enti, hanno portato a considerare in maniera pertinenti i fattori determinanti la nomina o meno del DPO.

La suddetta documentazione, infatti, può comunque essere oggetto di valutazione da parte dell'Autorità di controllo. A tal proposito, atteggiamento lodevole sarebbe quello di aggiornare la medesima documentazione ogni qualvolta l'azienda o l'ente ad esempio ponga in essere un trattamento dei dati riconducibile nell'alveo dei casi indicate all'art. 37, comma 1.

Gli enti e le aziende che non sono soggette alla prescrizione di nomina del DPO, rimangono tuttavia libere di avvalersi di professionisti esterni relativamente alla protezione dei dati personali, con l'unico limite di garantire che non vi siano ambiguità con il DPO, in termini di denominazione, status e compiti di queste figure.

Qualora si ricorre alla nomina del DPO su base volontaria, ad esse verrà comunque applicata la medesima disciplina prevista agli artt. 37 38 39 del Regolamento 679/2016, esattamente come ne caso di nomina obbligatoria.

---

[127] Si osservi che, in base all'articolo 37, paragrafo 4, del GDPR il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

[128] Ai sensi dell'articolo 9, Regolamento 679/2016, questi includono dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, i religiosi o credenze filosofiche, o appartenenza sindacale, e il trattamento di dati genetici, dati biometrici per il scopo di identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi al sesso di una persona fisica vita o orientamento sessuale.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un DPO e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (DPO). Tuttavia, sebbene la diversa portata della norma contenuta nella Direttiva prima, e nel Regolamento poi, facciano comprendere come si sia giunti ad un obbligo di designazione del DPO è bene considerare che la facoltatività della sua designazione potrebbe comunque creare confusione nella distinzione tra obbligatorietà e facoltatività.
La confusione di cui si parla è di derivazione totalmente aziendale, poiché è la stessa impresa che dovrà valutare se le sue caratteristiche (e quelle del trattamento che decide di porre in essere) corrispondano ad un obbligo ovvero ad una scelta di designare un DPO.

§ 2.1.1. I chiarimenti del WP 29 in ordine all'obbligo di designazione

Per sgomberare il campo in ordine a questi dubbi, il 19 dicembre 2016 il Gruppo di lavoro *ex* art. 29 è prontamente intervenuto precisando alcuni aspetti in ordine alla nomina obbligatoria del DPO.

In particolare, ha chiarito gli elementi di cui alle lett. a), b), e c) del paragrafo 1 dell'art. 37.

Innanzitutto, è dato precisare che nel Regolamento non è data alcuna definizione di "autorità pubblica" o "organismo pubblico". A tal riguardo, il Gruppo di lavoro *ex* art. 29 ha ritenuto che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico. In questi casi la nomina di un DPO è obbligatoria.
Il tratto peculiare che giustifica a pieno necessità delle linee guida elaborate anche per il DPO dal WP 29, per valutare correttamente quando la designazione è obbligatoria,

è rappresentato dal fatto che lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non necessariamente deve essere riferito a soggetti di diritto pubblico, potendo riferirsi anche ad altre persone, sia fisiche che giuridiche anche di diritto privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale. In ragione di quanto appena esposto è logico supporre che, i margini per l'interessato di decidere sul trattamento dei dati sia da considerarsi minimo o nullo. Il Gruppo ancora una volta raccomanda in termini di *best practice*, una attenta valutazione, per tutti i soggetti su menzionati per i quali tutta via non ricorre l'obbligo di nominare un DPO, al fine di una maggiore tutela e garanzia dei diritti degli interessati.

§ 2.1.2. La portata terminologica del GDPR sul DPO nei passaggi cardine per una corretta interpretazione

L'articolo 37, paragrafo 1, lettere b) e c), del Regolamento contiene, inoltre, un riferimento alle "attività principali del titolare del trattamento o del responsabile del trattamento". Nel Considerando 97 si afferma che le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un DPO.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività

principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali.

Ne consegue che anche l'impresa in oggetto deve nominare un DPO. D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

Ulteriori chiarimenti si rendono necessari per quanto riguarda *"i trattamenti su larga scala"* di cui all'articolo 37, paragrafo 1, lettere b) e c).

Come per il caso delle *"autorità pubbliche"*, anche per i trattamenti su larga scala il Regolamento 679/2016 non dà alcuna definizione, anche se il Considerando 91 fornisce indicazioni in proposito[129].

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "*larga scala*" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il Gruppo di lavoro intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un DPO.

A ogni modo, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala. Detti fattori sono:

A) il numero dei soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

[129] Il Considerando in questione vi ricomprende, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". D'altro canto, lo stesso Considerando prevede in modo specifico che "il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato". Si deve tener conto del fatto che il Considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il Considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un DPO negli stessi identici termini.

B) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
C) la durata, ovvero la persistenza, dell'attività di trattamento;
D) la portata geografica dell'attività di trattamento.

Non solo, per rendere ancor più agevole il compito per le imprese, il WP 29 indica anche un insieme di esempi di trattamenti nei quali è obbligatoria la nomina di un DPO, tra i quali si possono annoverare:

- il trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- il trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- il trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- il trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- il trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- il trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Infine, va chiarito il concetto di "*monitoraggio regolare e sistematico*". Anche in questo caso il Regolamento 679/2016, pecca di una definizione a riguardo, e un'analisi è possibile condurla soltanto alla luce di quanto disposto dal Considerando n. 24 del Regolamento medesimo che, menzionando il "*monitoraggio del comportamento di detti interessati*[130]" ricomprende al suo interno tutte le forme di tracciamento e profilazione che avvengono su Internet anche per finalità di pubblicità comportamentale.
Secondo il WP 29 l'aggettivo "regolare" ha almeno uno dei seguenti significati:
a) che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

[130] CONSIDERANDO n. 24, Regolamento 679/2016: "Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".

b) che avviene in modo ricorrente o ripetuto a intervalli costanti;
c) che avviene in modo costante o a intervalli periodici.

Mentre l'aggettivo "sistematico" sottende i significati che seguono:
a) che avviene per sistema;
b) che è predeterminato, organizzato o metodico;
c) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
d) svolto nell'ambito di una strategia.

§ 2.1.3. Le valutazioni sulla designazione obbligatoria o facoltativa

Come si evince dal *par. 1* e dal *par.* 4 dell'art. 37 del Regolamento n. 679 del 2016, la designazione del DPO, può essere rispettivamente obbligatoria ovvero facoltativa.
Tuttavia, sebbene ci si trova nelle ipotesi di cui al *par. 1,* alla luce dei chiarimenti forniti dal WP 29, appare evidente che la valutazione che l'impresa deve compiere, se munirsi (obbligatoriamente) o meno del DPO*,* presenta degli spazi discrezionali che potrebbero mettere il trattamento dei dati a rischio di carenza delle adeguate garanzie (rappresentate in questo caso dal DPO). Possiamo dunque intendere la designazione del DPO, come un impianto costituito da due diversi livelli di discrezionalità: un primo livello, costituito dalla valutazione circa le caratteristiche del trattamento alla luce dei chiarimenti forniti dal WP 29 sulle ipotesi di cui sopra; un secondo livello discrezionale che entrerà in gioco allorché la designazione sia facoltativa e il titolare valuterà se designare o meno tale figura.
Anche in questo secondo livello, la raccomandazione del WP 29 non si è fatta attendere, e nelle linee guida tracciate per il DPO[131], ha affermato che sarebbe buona regola che il titolare (e il responsabile) del trattamento, documentino l'attività di indagine e ricerca svolta per stabilire se la designazione sia necessaria o meno, anche fuori dalle ipotesi in cui questa è (ovviamente) obbligatoria.

[131] WP 29: elaborato n. W 243 Linee guida sui responsabili della protezione dei dati adottate il 13 dicembre 2016. Versione emenata e adottata in data 5 aprile 2017.

In definitiva si tratta di documentare il ragionamento che, nel caso in cui il trattamento non richieda (obbligatoriamente) la nomina del DPO, ha condotto alla scelta di non "affidarsi" a questa figura per garantire la tutela del diritto alla protezione dei dati personali.

Ovviamente, alla luce dell'*accountability principle,* che descrive tutti gli ambiti della responsabilità aziendale nel contesto della tutela del diritto alla protezione dei dati personali, sarebbe auspicabile che tutti i trattamenti di dati personali, che hanno luogo attraverso la conclusione di contratti all'interno dei quali sono presenti le BCR, siano operati sotto lo sguardo vigile di un DPO. Quindi si può immaginare che in questo contesto il principio di *accountability* si fondi anche sulla figura del DPO, che assicurerà il rispetto dei principi di garanzia che governano il trattamento dei dati personali all'interno del territorio comunitario e che sono posti a fondamento del Regolamento n. 679 del 2016.

Ovviamente, alla luce dell'*accountability principle*, che descrive tutti gli ambiti della responsabilità aziendale nel contesto della tutela del diritto alla protezione dei dati personali, sarebbe auspicabile dare un'attuazione a trecentosessanta gradi della *compliance* aziendale al GDPR, e non di meno alla nomina di un DPO. In caso di violazione delle garanzie il Regolamento 679/ 2016, non fa differenza se il DPO sia frutto di una scelta volontaria della società, ovvero la sua designazione sia obbligatoria per la natura del trattamento medesimo, poiché, in caso di violazioni troveranno sempre applicazione le sanzioni di cui all'art. 83 del Regolamento 679/2016.

§ 2.1.4. Chi è tenuto a nominare il DPO?

Attraverso la lettura della prima parte del paragrafo 1 e poi del paragrafo 2 dell'art. 37 del Regolamento 679/ 2016, è possibile rilevare che la nomina del DPO non è un compito riservato sempre e solo al medesimo soggetto**.** Seguendo la struttura dei due paragrafi dell'articolo, e attraverso i chiarimenti forniti dalle linee guida del WP 29, è possibile, infatti, rilevare che la nomina può spettare rispettivamente al titolare e

o al responsabile del trattamento o, ancora, ad un gruppo di imprenditori. Per quanto riguarda il titolare o il responsabile del trattamento, il WP 29 nelle sue linee guida ha specificato che la nomina avverrà per entrambi i soggetti solo se questi possiedono i requisiti che danno luogo ad una nomina obbligatoria, qualora invece sia soltanto uno di questi a rispettare le predette caratteristica circa la nomina obbligatoria, la nomina dovrà essere effettuata solo da questi.
Il WP 29 precisa che qualora la nomina venga effettuata da entrambi, titolare e responsabile del trattamento, i DPO sono tenuti alla reciproca collaborazione.

(segue) Nomina di un unico DPO da parte di un gruppo di imprenditori

La nomina di un medesimo DPO da parte di un gruppo di imprenditori è espressamente previsto dall'art. 37, par. 2, Regolamento 2016/679. Detta norma consente a un gruppo imprenditoriale di nominare un unico DPO a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti svolti dal DPO, in riferimento al punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente, visto che uno dei compiti consiste nell'"*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*[132]".
Allo scopo di assicurare la raggiungibilità del DPO, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal GDPR[133].
Il DPO, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati, in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire

[132] V. Articolo 39, paragrafo 1, lettera a), Regolamento 2016/679.
[133] V. articolo 12, paragrafo 1: "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori".

nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il DPO sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il DPO stesso.

Ai sensi dell'articolo 37, paragrafo 3, è ammessa la designazione di un unico DPO per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il DPO è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico DPO, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

§ 2.1.5. Conoscenze e competenze del DPO

Ai sensi dell'articolo 37, paragrafo 5, il DPO "*E' designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*".

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; dalla lettura del Considerando 97 si può desumere che il livello necessario di conoscenza specialistica deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento.

Per quanto concerne le qualità professionali auspicabili in capo al soggetto da nominare come DPO, fra queste vanno considerate certamente l'approfondita conoscenza da parte del medesimo della normativa e delle prassi nazionali ed europee in materia di protezione dei dati. Sicuramente proficua, sarebbe la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento ivi comprese le operazioni di trattamento effettuate presso la propria azienda, nonché i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Quanto appena detto, pone i presupposti affinché si abbia un'ottimale adempimento dei compiti da parte del DPO, per una maggiore tutela dei diritti degli interessati ed un adeguato e più efficace rispetto della normativa in materia di tutela dei dati personali. Tra le qualità personali dovrebbero rilevare un forte senso civico e cultura della legalità ispirati da elevati standard deontologici, affinché il designato a DPO possa promuovere il tutte le sue nomenclature la cultura della protezione dei dati personali all'interno dell'azienda o dell'ente.

§ 2.1.6. La nomina del DPO sulla base di un contratto di servizi

La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'azienda o all'ente titolare/responsabile del trattamento.

Anche in questo caso il soggetto operante quale DPO deve possedere tutti i requisiti richiesti alla Sezione 4 del GDPR, godendo lo stesso anche di tutte le prerogative e i diritti in esso previsti. In tale fattispecie di fondamentale importanza sarà quella di inserire specifiche disposizioni nel contratto di servizi, anche ad esempio nel caso di una persona giuridica, al fine di prevenire situazioni di conflitto di interessi anche all'interno del team DPO, e non soltanto il capo al medesimo.

Per una piena esplicazione delle sue funzioni vi deve essere un'opportuna ed idonea comunicazione e pubblicità dei dati di contatto del DPO. Sia il titolare che il responsabile del trattamento sono tenuti ai sensi dell'art. 37 comma 7 del GDPR a darne comunicazione all'Autorità Garante. In merito alla questione si è espresso anche il Gruppo di Lavoro *ex* art. 29 nel WP 243, il quale afferma che comunicare il nominativo del DPO all'autorità di controllo è fondamentale affinché il medesimo funga da punto di contatto fra il singolo Ente o organismo e l'Autorità di controllo stessa (articolo 39, comma 1, lettera e).

I dati di contatto del DPO dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il DPO stesso: recapito

postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Sono ipotizzabili anche ulteriori canali di comunicazione.
In base all'articolo 37, par. 7, del GDPR non è necessario pubblicare anche il nominativo del DPO. Seppur ciò rappresenti con ogni probabilità, una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso DPO stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze. In termini di buone prassi, il Gruppo *ex* WP 29 di lavoro ha raccomandato, inoltre, che il titolare e/o il responsabile del trattamento comunichi ai dipendenti il nominativo e i dati di contatto del DPO, il quale è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, par. 5, del GDPR).

§ 2.2. La posizione del DPO: Art. 38 del Regolamento n. 679 del 2016

Un altro punto che è necessario approfondire per comprendere a pieno l'importanza che la figura del DPO ha assunto nel nuovo Regolamento, riguarda il suo posizionamento all'interno dell'organismo aziendale, disciplinato dall'art. 38 del Regolamento 679/2016.

Secondo tale norma, il DPO può essere investito di tale compito o tramite un contratto di lavoro subordinato (in tal caso verrebbe a configurarsi alla stregua di un dipendente), oppure tramite un contratto di servizi (a tale ultima fattispecie si ricorre per la nomina di un soggetto esterno all'ente o società).

Ovviamente, la scelta dell'una o dell'altra formula dà luogo a considerazioni differenti se messe in relazione con il posizionamento all'interno dell'impresa.

Propendere per l'una o l'altra modalità di contrattazione comporta rilevanti considerazioni circa la sua collocazione all'interno dell'azienda, *latu sensu.* Come si è anticipato in apertura di paragrafo, il problema principale in merito al posizionamento del DPO si ha in ragione alle differenti modalità con le quali

questo soggetto svolge i suoi compiti, cioè se attraverso un contratto di servizi ovvero se si tratti di un lavoratore dipendete che assume la carica di DPO.

Qualora il DPO agisca tramite un contratto di servizi, trattandosi di fatto di un consulente esterno alla società è possibile ritenere che non sorgano conflitti di interessi nello svolgimento delle sue mansioni, poiché il requisito dell'indipendenza è facilmente assicurato dalla mancanza di un rapporto "*diretto*" con il titolare, o il responsabile del trattamento. La maggior parte dei problemi, in ordine alla genuinità del rapporto tra i compiti del DPO e il trattamento dati secondo le adeguate garanzie, sorgono nel caso in cui l'ente, o la società, e il DPO siano legati da un rapporto di lavoro di tipo subordinato. Per tali ragioni il Regolamento *in primis*, e poi anche il Gruppo di lavoro *ex* art. 29 nelle sue linee guida, hanno disciplinato e spiegato i caratteri in base ai quali, nonostante tale posizionamento, il DPO possa comunque eseguire i suoi compiti assicurando il rispetto delle dovute garanzie durante il trattamento dei dati. In forza del posizionamento del DPO all'interno della società, la prima caratteristica che implicitamente si evince dalla norma riguarda la sua indipendenza[134].

Tale requisito mira a specificare la necessaria condizione di assenza, anche potenziale, di conflitto di interesse in cui deve trovarsi il DPO per poter correttamente operare. Proprio per preservare l'indipendenza del DPO, il Regolamento prescrive che esso non riceva alcuna istruzione per quanto concerne l'esecuzione dei suoi compiti. Ciò significa che il DPO, nell'esecuzione dei compiti attribuitigli ai sensi del successivo art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico, su quali siano i risultati attesi, su come condurre gli accertamenti su un reclamo, sul se consultare o meno l'autorità di controllo, né, tantomeno l'autorità di controllo, né, tantomeno, deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Tale indipendenza e autonomia del DPO, risulta ancor più rafforzata dal fatto che, sempre il paragrafo 3 dell'art. 38, dispone che tale soggetto non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

[134] CONSIDERANDO 97, Regolamento 679/2016: "[…] Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

Il divieto di penalizzazioni menzionato nel Regolamento, si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del DPO[135]. Per esempio, un DPO può ritenere che un determinato trattamento comporti un rischio elevato, e quindi raccomandare al titolare o al responsabile del trattamento di condurre una valutazione di impatto, ma questi ultimi non concordano con la valutazione del DPO. In casi del genere non è ammissibile che il DPO sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto. Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta[136]. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al DPO in rapporto alle attività da questi svolte. Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente, o fornitore soggetto alla disciplina del rispettivo contratto nazionale, ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il DPO per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche. In questo ambito va rilevato che il Regolamento non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del DPO o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il DPO e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del DPO si svolga in modo indipendente. Tuttavia, l'autonomia del DPO non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'art. 39 del Regolamento 679/2016. Il titolare o il responsabile del trattamento, mantengono sempre la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere, pertanto, in grado di dimostrare tale osservanza.

[135] **R.C. Geissler**, Private *Eyes Watching Yuo: Google Street View and the Rhigt to an Inviolat Personality*, in Hasting Law Journal, Vl. 63, 2012, p. 897.

[136] **F. Bignami**, *Transgovemmental Networks vs. Democraticy: The Case of the European Information Privacy Network*, in Michigan Journal of Internetional Law, Vol. 26, 2005, pp. 827-830.

Se essi assumono decisioni incompatibili con il Regolamento e con le indicazioni impartite dal DPO, quest'ultimo deve avere la possibilità di manifestare il proprio dissenso al più alto livello del management dell'azienda o dell'ente. Al riguardo, l'art. 38, paragrafo 3, prevede che il DPO "*riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia costantemente aggiornato delle indicazioni e delle raccomandazioni del DPO nell'esercizio dei suoi compiti. Una volta inquadrato il posizionamento del DPO quale lavoratore dipendente del titolare, del responsabile del trattamento, l'altro punto che merita di essere analizzato è quello inerente la necessaria mancanza di conflitto di interessi con l'incarico di DPO.

Secondo il paragrafo 6 dell'art. 38, al DPO è consentito "svolgere altri compiti e funzioni", ma a condizione che "tali compiti e funzioni non diano adito a un conflitto di interessi" prontamente accertato dal titolare, o il responsabile del trattamento. L'assenza di conflitti di interessi è anch'essa strettamente connessa agli obblighi di indipendenza. Egli può svolgere altre funzioni purché non comportino conflitto. Ciò comporta che l'accertamento del conflitto vada compiuto caso per caso tenendo in considerazione la specifica struttura organizzativa del singolo titolare, o responsabile. A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un DPO esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare o del responsabile, si possono indicare le seguenti best practice:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di DPO;
- redigere regole interne onde evitare conflitti di interessi;

- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il DPO non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di DPO, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale DPO, ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il DPO sia designato fra soggetti interni o esterni all'organizzazione.

§ 2.3. I compiti del DPO: Art. 39 del Regolamento n. 679 del 2016

Alla luce di ciò dunque, appare evidente che i compiti riservati al DPO sono semplicemente il precipitato di questa interpretazione, quindi, per dovere di completezza nella descrizione di questa figura, basterà seguire il disposto dell'art. 39 del Regolamento n. 679 del 2016, il quale se pur non abbia carattere di esaustività, al paragrafo 1, specifica che il DPO deve svolgere "*almeno*" i compiti in questione. Ne consegue che niente vieta al titolare di assegnare al DPO compiti ulteriori rispetto a quelli espressamente menzionati nella norma in parola, ovvero di specificare ulteriormente i compiti ricompresi nell'articolo suddetto.
Fra questi compiti di sicuro rilievo è quello richiamato alla lettera b) del paragrafo 1 dell'art. 39, il quale affida al DPO il compito di sorvegliare l'osservanza al GDPR.
Fanno parte di questi compiti di controllo svolti dal DPO, in particolare:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità;
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Tuttavia, ciò non implica che il DPO sia responsabile in caso di inosservanza della normativa sulla protezione dei dati personali. Il GDPR lascia in capo al titolare del trattamento ogni responsabilità in tal senso, in quanto fa parte della responsabilità d'impresa del titolare del trattamento il rispetto delle norme in materia di protezione dei dati, non del DPO.

§ 2.4. Il ruolo del DPO nella valutazione di impatto sulla protezione dei dati

Per quanto concerne le valutazioni di impatto sulla protezione dei dati il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale compito. Infatti, se da una parte l'articolo 35 al par. 1 sancisce in capo al titolare l'onere di condurre ove necessario, una valutazione di impatto sulla protezione dei dati o DPIA (*Data Protection Impact Assestment*), dall'altro al paragrafo 2, prevede in modo specifico che il titolare "si consulta" con il DPO quando questo svolge una valutazione ti tale genere. A sua volta il DPO ai sensi dell'art. 39, par. 1, lettera c, è tenuto a "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35". Sarebbe auspicabile, secondo le raccomandazioni del Gruppo di lavoro *ex* art. 29, che il titolare del trattamento si consulti con il DPO, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR.

Tali sono rilevanti le indicazioni del DPO in tale ambito che è necessario che la documentazione relativa alla DPIA riporti fedelmente per iscritto, qualora vi fossero divergenze tra le indicazioni del DPO e le misure adottate dal titolare, le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni. Ulteriore compito del DPO, ai sensi dell'articolo 39, paragrafo 1, lettere d) ed e), è di "cooperare con l'Autorità di controllo" e "fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione". Tale compito permette all'Autorità di controllo per l'assolvimento dei compiti attribuitile dall'articolo 57 e ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58, di avere l'accesso a tutti i documenti e alle informazioni ritenute necessarie. L'intera attività del DPO si svolge con un approccio di tipo cautelativo, di buon senso, con un approccio basato sul rischio. Infatti, ai sensi dell'articolo 39, paragrafo 2, il DPO deve "*considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*". In altre parole, l'attività del DPO deve seguire un ordine di priorità che abbia come fuoco le questioni che presentino maggiori rischi in termini di protezione dei dati. Seguendo tali modalità il DPO ben potrà indicare e consigliare il titolare del trattamento su quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

§ 2.5. Il ruolo del DPO nella tenuta del registro delle attività di trattamento

È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali, nonché

sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE, che sono i DPO a realizzare l'inventario dei trattamenti e tenere un loro registro sulla scorta di tutte le informazioni acquisite presso i vari uffici che hanno in carico trattamenti di dati personali.
Tuttavia, ai sensi dell'art. 39, paragrafi 1 e 2 del Regolamento 679/2016, è il titolare o il responsabile del trattamento ad essere obbligato sotto la propria responsabilità a tenere un registro delle attività di trattamento dei dati personali.
Invero, niente vieta al titolare o al responsabile del trattamento di affidare al DPO il compito di tenere il registro delle attività di trattamento, fatti salvi I profili di responsabilità che continuano a permanere in capo ai soggetti obbligati alla tenuta di tale registro. Ciò è possibile in quanto l'elenco dei compiti in capo al DPO previsto ai sensi dell'art. 39 ha natura indicativa e non esaustiva.
La corretta tenuta del registro dei trattamenti dei dati personali costituisce un presupposto indispensabile ai fini dell'osservanza delle norme, e pertanto, un'efficace misura di responsabilizzazione che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del Regolamento, informazione e consulenza nei riguardi del titolare o del responsabile del trattamento dei dati personali.
Il registro del trattamento dei dati personali deve essere considerato come uno strumento che consente al titolare del trattamento e all'Autorità di controllo, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto.

§ 3. La determinazione della competenza giurisdizionale e della legge applicabile alle controversie in materia di trattamento dei dati personali

Le BCR, essendo espressione di *Transnational Private Law*, rispondono ad esigenze differenti a seconda del contesto pubblico o privato in cui operano. Inoltre, per rendere le BCR idonee a regolare il trattamento dei dati personali, è necessario che queste siano conformi alle discipline ad esse relative.

Come si evince da quanto sopra detto, il principale ambito nel quale si muovono le BCR, è rappresentato dal diritto internazionale privato. Come parte della dottrina ha sostenuto, il diritto internazionale privato è la *"queen mother of all transnational legal though"*[137].

Occorre rilevare, che il rapporto che intercorre tra le BCR e il diritto internazionale privato, corre su un duplice binario. Da un lato vi è l'assunto secondo cui nella redazione delle BCR, la scelta della legge applicabile in caso di violazione del diritto alla protezione dei dati personali e il foro giurisdizionalmente competente a giudicare sulla lesione, devono essere conformi alle disposizioni derivanti dal diritto internazionale privato.
Dall'altro lato invece, il diritto internazionale privato assurge ad una potenziale fonte di meta-regolamentazione delle BCR[138], poiché tali clausole, essendo espressione di TPR per essere ammissibili a livello nazionale, devono essere costruite partendo dall'assunzione di possedere un punto di riferimento comune con le diverse giurisdizioni nazionali[139].

Si noti pertanto, che l'utilizzo delle BCR da parte delle multinazionali, deriva da alcuni caratteri propri del diritto internazionale privato, questo assunto si ricava indirettamente da diversi elaborati del WP29, nei quali si evince che le BCR si applicano ai principali trattamenti posti in essere dalle multinazionali, fin tanto che non trovino applicazione delle normative nazionali più stringenti. Dunque, qualora troverà applicazione una normativa (nazionale) che meglio tutelerà il diritto alla protezione dei dati personali, allora alle BCR spetterà il compito di garantire un livello minimo di protezione[140].

Sempre in relazione al rapporto tra diritto internazionale privato e le BCR, il WP 29 mette in evidenza un'ulteriore legame, ossia attraverso la possibilità di inserire delle clausole aventi ad oggetto la scelta del foro al quale sottoporre la controversia, si eviterebbe una concorrenza con le disposizioni di diritto internazionale in materia, rafforzando così una volta di più la manifestazione di volontà derivante dal contratto.

---

[137] **C. Joerges**, *Rethinking European Law's Supremacy*, EUI Working Papers 2005/12 (2005);
[138] **J. Bomhoff** and **A. Meuwese**, *The Meta-Regulation of Transnational Private Regulation*, Journal of Law and Society, Vol. 38, N. 1, March 2011;

[139] **J. Bomhoff** and J. **A. Meuwese,** *The Meta-Regulation of Transnational Private Regulation*, Journal of Law and Society, Vol. 38, N. 1, March 2011.

[140] WP 29, Documento di lavoro che presenta uno schema di elementi e principi delle *Binding Corporate Rules*, 24 giugno 2008 - WP 153.

Così facendo dunque, si eviterebbe la problematica della concorrenza tra le varie giurisdizioni competenti secondo le regole di diritto internazionale privato.

Ovviamente, la concezione secondo cui, il contenuto delle BCR può avere ad oggetto anche la scelta del foro al quale devolvere un'eventuale controversia, pone dei problemi con i principi del diritto internazionale privato. Il culmine del contrasto sorge dal fatto che la maggior parte dei dati trattati dalle multinazionali, sotto il regime delle BCR, riguarda i dati personali di dipendenti e clienti che, nella maggior parte dei casi sono consumatori. Si noti che i contratti dei suddetti soggetti sono tutelati dalle regole del diritto internazionale privato, le quali creano un regime obbligatorio, sia in termini di legge sostanziale sia in termini di meccanismi di risoluzione delle controversie, che non possono essere messe da parte, a danno dei dipendenti e dei clienti, dalla scelta della legge o del foro indicato all'interno delle BCR.

Quanto appena detto, offre un'ulteriore punto di criticità del diritto internazionale privato, ossia che le multinazionali che nel trasferimento dei dati personali si servono delle BCR, tra gli altri, hanno un forte interesse nel far sì che tali clausole contengano delle regole per la designazione della legge e del foro. Il motivo di tali scelte deriva prettamente da ragioni di economicità nella gestione aziendale. Poiché è nell'interesse delle multinazionali che tutte le doglianze sorte sotto il regime delle BCR, siano gestite dalla Lead DPA prescelta, ovvero dagli organi giurisdizionali dello Stato membro ove questa si trovi, visto che il compito di esaminare l'ammissibilità delle BCR è delegato all'Autorità prescelta.

La questione secondo la quale la tutela del diritto alla protezione dei dati personali dei dipendenti e dei clienti, possa essere garantita al meglio attraverso la scelta della legge e del foro nel regime delle BCR, deve essere necessariamente presa in considerazione valutando le implicazioni che ciò può avere con il rispetto del diritto internazionale privato.

In questo preciso momento storico, nell'ambito di questo diritto fondamentale, il punto che maggiormente risulta controverso è proprio la tutela giurisdizionale ad esso riconosciuta. Le criticità, non si rinvengono nei profili sostanziali, perché come si è avuto modo di analizzare tutte le varie fonti del diritto prestano una particolare attenzione alla protezione dei dati personali. Dunque, i dubbi interpretativi riguardano essenzialmente gli aspetti processuali, poiché, se da un lato abbiamo le regole di diritto internazionale privato che indicano come operare la scelta della legge e del foro competente, dall'altro

abbiamo il superamento di una fase di transizione tra la Direttiva 95/46 e il Regolamento n. 679 del 2016, il quale ha trovato una definitiva applicazione a partire dal 25 maggio 2018. Il dubbio interpretativo che sorge, si ha soprattutto in relazione alla scelta del foro, poiché la Direttiva 95/46, non forniva alcuna indicazione in ordine alla competenza a giudicare sulle controversie che potrebbero sorgere, mentre il Regolamento n. 679 del 2016 indica chiaramente la competenza giurisdizionale a seconda che la doglianza sia proposta avverso una DPA ovvero un titolare o un responsabile del trattamento.

Alla luce di ciò dunque, in caso di violazione del diritto alla tutela dei dati personali, appare evidente che per l'interessato sarà arduo individuare l'esatta competenza giurisdizionale, poiché su questo interrogativo convoglieranno le regole di diritto internazionale privato, e dal maggio 2018, le regole dettate dal Regolamento n. 679 del 2016 e le BCR contenenti la scelta del foro e della legge applicabile.

§ 3.1. La scelta del foro

Come si è anticipato, la scelta del foro al quale devolvere la cognizione della controversia in materia di diritto alla protezione dei dati personali, rappresenta la questione che in ambito di tutela si espone ai maggiori dubbi interpretativi.

Prima di individuare le fonti del diritto che operano in questo contesto, sono doverose alcune precisazioni di natura definitoria su ciò che si intende per foro.

Con questa espressione ci si riferisce all'organo giurisdizionale *competente* a giudicare la lesione del diritto in parola. Certamente la competenza, se letta in chiave di diritto interno si riferisce alla ripartizione del potere giurisdizionale tra i diversi giudici secondo una distinzione per materia o territorio. Il discorso invece cambia in ambito di diritto internazionale privato, secondo il quale quando si parla di foro competente, non ci si riferisce alla ripartizione interna del potere di amministrazione della giustizia, ma al potere giurisdizionale dello Stato membro al quale la controversia deve essere devoluta. In altre parole, nell'ambito del diritto internazionale privato la competenza coincide e si identifica con il significato che il Legislatore italiano fornisce della giurisdizione. Alla luce di questa precisazione è dunque ora possibile analizzare l'evoluzione che ha avuto il riparto della competenza giurisdizionale secondo le diverse normative che si sono succedute. Oltre all'analisi di questa evoluzione, si analizzerà come opera questa scelta

del foro, poiché sebbene la determinazione del foro al quale devolvere la controversia possa essere oggetto di scelta tra le parti, perché vi è l'inserimento di una apposita clausola BCR nel contratto che può indicare la competenza giurisdizionale, si noterà che ciò avrà valore solo tra titolare e responsabile del trattamento in quanto parti contrattuali. Dunque si vedrà come la scelta del foro opererà nei confronti dei soggetti terzi, che nella maggior parte dei casi sono rappresentati dagli interessati.

Sulla base della Direttiva 95/46, è possibile notare che nelle sue disposizioni non vi è alcun rimando al foro competente o come le parti contrattuali potessero operare questa scelta. Infatti, in materia di ricorsi giurisdizionali è presente una singola disposizione secondo la quale: *"Fatti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all'autorità di controllo di cui all'articolo 28, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione " (art. 22 Direttiva 95/46).* Dalla lettura della norma appare evidente che la Direttiva Madre riconosceva solo la possibilità di adire l'autorità giurisdizionale ma, per stabilire quale fosse stata quella competente era necessario operare un rimando ai singoli ordinamenti nazionali. Ciò ovviamente lasciava spazio a molte incertezze e difficoltà nell'accedere alla tutela giurisdizionale per la parte che lamentava la lesione del suo diritto.

Successivamente poi, grazie all'introduzione delle norme di diritto internazionale privato, nello specifico, prima il Regolamento CE n. 44/2001[141], c.d. Bruxelles 1, e il Regolamento (UE) 1215/2012, c.d. Bruxelles 1 bis poi, che abroga e sostituisce il Regolamento n. 44/2001, il quale rende ora possibile procedere direttamente all'esecuzione forzata di una decisione esecutiva in altro Stato membro dell'Unione europea, esattamente come se fosse un provvedimento giudiziario nazionale, si raggiunge quel grado di certezza nella determinazione del foro competente che mancava con la Direttiva 95/46.

Per capire l'operatività del Regolamento Bruxelles 1 bis, è necessario distinguere le ipotesi, come si è anticipato precedentemente, in cui la doglianza venga portata alla

[141] Nel Regolamento 44/2001 ha più volte sottolineato che per luogo dove si è verificata la violazione deve intendersi il luogo dove ha avuto inizio il fatto generatore del danno, cioè quello in cui il danno si è concretato. V. Corte giust., sent. 5 giugno 2014, *Coty Germany GymbH C. First Note Perfumes NV*, causa C-360/2012, PUNTI 35-38.

cognizione del giudice da parte dell'interessato, ovvero da un soggetto parte del rapporto contrattuale.

In quest'ultima ipotesi, il Regolamento Bruxelles 1 bis è molto chiaro su quale debba essere il foro competente, ossia secondo l'art. 7 par. 1 lett. *a)*, *"all'autorità giurisdizionale del luogo di esecuzione dell'obbligazione dedotta in giudizio*".

Alla luce di ciò dunque, qualora nel contratto di trasferimento di dati personali tra titolare e responsabile del trattamento, le parti volessero inserire delle BCR che contengano anche la determinazione del foro competente al quale devolvere le future controversie che potrebbero sorgere, il contenuto di queste clausole deve rispettare la previsione dell'art 7 par.1 del Regolamento Bruxelles 1 bis.

Tuttavia tale disciplina presenta delle deroghe, previste e disciplinate dall'art. 25 del Regolamento Bruxelles 1 bis, in base al quale *"Qualora le parti, indipendentemente dal loro domicilio, abbiano convenuto la competenza di un'autorità o di autorità giurisdizionali di uno Stato membro a conoscere delle controversie, presenti o future, nate da un determinato rapporto giuridico, la competenza spetta a questa autorità giurisdizionale o alle autorità giurisdizionali di questo Stato membro, salvo che l'accordo sia nullo dal punto di vista della validità sostanziale secondo la legge di tale Stato membro. Detta competenza è esclusiva salvo diverso accordo tra le parti".*

Il discorso appare più complesso allorché la doglianza sia manifestata dall'interessato, il quale resta soggetto terzo rispetto alle BCR.

In questo caso, è inoltre necessario distinguere la tipologia di interessato, sia esso un dipendente della multinazionale i cui dati personali vengono trattati dai dipartimenti delle risorse umane, ovvero un cliente.

Nella prima ipotesi vi è una deroga a quanto previsto dall'art. 7 par.1 del Regolamento Bruxelles 1 bis, poiché l'art. 21 del Regolamento appena richiamato dispone che:

"1. Il datore di lavoro domiciliato in uno Stato membro può essere convenuto:

a) davanti alle autorità giurisdizionali dello Stato in cui è domiciliato; o

b) in un altro Stato membro:

- davanti all'autorità giurisdizionale del luogo in cui o da cui il lavoratore svolge abitualmente la propria attività o a quello dell'ultimo luogo in cui o da cui la svolgeva abitualmente; o

- qualora il lavoratore non svolga o non abbia svolto abitualmente la propria attività in un solo paese, davanti all'autorità giurisdizionale del luogo in cui è o era situata la sede d'attività presso la quale è stato assunto.

2. Il datore di lavoro non domiciliato in uno Stato membro può essere convenuto davanti a un'autorità giurisdizionale di uno Stato membro ai sensi del paragrafo 1, lettera b)".

Tuttavia, come si è avuto modo di rilevare, attraverso le BCR, in conformità dell'art. 25 del Regolamento Bruxelles 1bis è consentito scegliere un foro differente da quelli previsti dagli artt. 7, par. 1, e 21. In questa ipotesi, il punto che è necessario sottolineare è che la scelta espressa in merito al foro competente nella BCR a ciò preposta, può essere efficace anche nei confronti del *"terzo dipendente"* solo se la facoltà di scelta del foro è riconosciuta anche al lavoratore in forza di quanto disposto dall'art. 23, par. 2, del Regolamento Bruxelles 1bis. In altre parole si ammette una deroga al foro competente secondo l'art 21 sulla base di un accordo tra la multinazionale e il suo dipendente.

Per ciò che concerne le doglianze manifestate dal *"terzo cliente"* il tenore normativo è analogo a quanto detto per i dipendenti, poiché vi è una norma generale di determinazione del foro all'art. 18 del Regolamento Bruxelles 1bis[142], e la possibilità di scelta del foro, derogatoria rispetto all'art. 18, all'art. 19 del Regolamento in parola[143]. Certamente, la disciplina così presentata, alla luce del Regolamento (UE) 1215/2012, presta il fianco a problematiche questioni interpretative, poiché resta difficoltoso individuare con certezza l'autorità giurisdizionale al quale devolvere la controversia.

La questione è stata totalmente risolta, con l'emanazione del Regolamento n. 679 del 2016, nel quale è possibile rinvenire una disposizione che elimina ogni dubbio sul foro

[142] Art. 18, Regolamento Bruxelles 1bis: "1. L'azione del consumatore contro l'altra parte del contratto può essere proposta davanti alle autorità giurisdizionali dello Stato membro in cui è domiciliata tale parte o, indipendentemente dal domicilio dell'altra parte, davanti alle autorità giurisdizionali del luogo in cui è domiciliato il consumatore. 2. L'azione dell'altra parte del contratto contro il consumatore può essere proposta solo davanti alle autorità giurisdizionali dello Stato membro nel cui territorio è domiciliato il consumatore. 3. Le disposizioni del presente articolo non pregiudicano il diritto di proporre una domanda riconvenzionale davanti all'autorità giurisdizionale investita della domanda principale in conformità della presente sezione".

[143] Art. 19, Regolamento Bruxelles 1bis: "Le disposizioni della presente sezione possono essere derogate solo da una convenzione: 1) posteriore al sorgere della controversia;2) che consenta al consumatore di adire un'autorità giurisdizionale diversa da quelle indicate nella presente sezione; o 3) che, stipulata tra il consumatore e la sua controparte aventi entrambi il domicilio o la residenza abituale nel medesimo Stato membro al momento della conclusione del contratto, conferisca la competenza alle autorità giurisdizionali di tale Stato membro, sempre che la legge di quest'ultimo non vieti siffatte convenzioni".

competente per dirimere l'insorgere di una controversia. La peculiarità che introduce il GDPR, attiene al fatto, che non vi è differenza se una controversia sia stata promossa da una delle parti contrattuali, che hanno sottoscritto l'elenco delle BCR, ovvero dall'interessato. Infatti l'art. 79 del Regolamento n. 679 del 2016 dispone che: *"1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente Regolamento siano stati violati a seguito di un trattamento.*

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri".

Dalla lettura dell'articolo si può evincere come la scelta del foro può anche essere inserita all'interno delle BCR, tuttavia la determinazione dell'autorità giurisdizionale deve essere conforme all'articolo appena citato. La certezza e la sicurezza dell'individuazione del foro corretto al quale devolvere le future controversie, si ha in ragione del fatto che il testo delle BCR sarà sottoposto alla valutazione di ammissibilità della Lead DPA, la quale dovrà valutare l'aderenza delle clausole al Regolamento sulla protezione dei dati personali in tutti i suoi aspetti, compresi quelli procedurali legati all'insorgere di controversie tra le parti e o i soggetti interessati.

§ 3.2. La scelta della legge applicabile

Come sopra accennato, alle parti contrattuali è riconosciuta la possibilità di scegliere quale sia la legge in forza della quale deve essere valutato il rispetto del diritto alla protezione dei dati personali e attraverso la quale adire l'autorità giurisdizionale prescelta in caso di una controversia, mediante le norme nazionali che fanno da corollario ai contratti di trattamento dei dati personali nell'ambito della normativa regolamentare.

Poiché la volontà contrattuale si può estendere a tutti gli aspetti del contratto, anche la scelta della legge applicabile al contratto di trasferimento e trattamento dei dati personali tra titolare e responsabile del trattamento, può essere inserita all'interno delle BCR.

Tuttavia, se si segue anche in questo contesto la linea delle discipline che si sono succedute nel tempo, appare evidente che né la Direttiva 95/46 né il Regolamento n. 679 del 2016 trattano il discorso in materia di scelta della legge applicabile. Alla luce di ciò dunque, sarà necessario rifarsi esclusivamente alle regole di diritto internazionale privato.

Le disposizioni in materia di legge applicabile alle obbligazioni contrattuali, sono contenute all'interno del Regolamento CE n. 593 del 2008 – Roma 1.

Come per il discorso operato nella scelta del foro competente, anche nel caso della scelta della legge applicabile è opportuno distinguere tra i rapporti che intercorrono tra titolare e responsabile del trattamento quali parti contrattuali, ovvero i rapporti tra questi e i dipendenti e i clienti della multinazionale che opera il trattamento dei dati personali.

Circa il rapporto tra le parti contrattuali la scelta della legge applicabile all'obbligazione può essere contenuta all'interno delle BCR. La fonte di questa libertà di scelta, è contenuta all'interno dell'art. 3 del Regolamento Roma 1, il quale dispone che: "*1. Il contratto è disciplinato dalla legge scelta dalle parti. La scelta è espressa o risulta chiaramente dalle disposizioni del contratto o dalle circostanze del caso. Le parti possono designare la legge applicabile a tutto il contratto ovvero a una parte soltanto di esso.*

2. Le parti possono convenire, in qualsiasi momento, di sottoporre il contratto ad una legge diversa da quella che lo disciplinava in precedenza per effetto di una scelta anteriore effettuata ai sensi del presente articolo o per effetto di altre disposizioni del presente Regolamento. Qualsiasi modifica relativa alla determinazione della legge applicabile, intervenuta posteriormente alla conclusione del contratto, non ne inficia la validità formale ai sensi dell'articolo 11 e non pregiudica i diritti dei terzi.

3. Qualora tutti gli altri elementi pertinenti alla situazione siano ubicati, nel momento in cui si opera la scelta, in un paese diverso da quello la cui legge è stata scelta, la scelta effettuata dalle parti fa salva l'applicazione delle disposizioni alle quali la legge di tale diverso paese non permette di derogare convenzionalmente.

4. Qualora tutti gli altri elementi pertinenti alla situazione siano ubicati, nel momento in cui si opera la scelta, in uno o più Stati membri, la scelta di una legge applicabile diversa da quella di uno Stato membro ad opera delle parti fa salva l'applicazione delle

disposizioni di diritto comunitario, se del caso, come applicate nello Stato membro del foro, alle quali non è permesso derogare convenzionalmente.

5. L'esistenza e la validità del consenso delle parti sulla legge applicabile sono disciplinate dagli articoli 10, 11 e 13".

Qualora invece le parti contrattuali nelle BCR non dovessero inserire una clausola di scelta della legge applicabile, allora troverà applicazione il disposto generale dell'art. 4 del Regolamento Roma 1, secondo il quale:

"1. In mancanza di scelta esercitata ai sensi dell'articolo 3 e fatti salvi gli articoli da 5 a 8, la legge che disciplina il contratto è determinata come segue:

a) il contratto di vendita di beni è disciplinato dalla legge del paese nel quale il venditore ha la residenza abituale;

b) il contratto di prestazione di servizi è disciplinato dalla legge del paese nel quale il prestatore di servizi ha la residenza abituale;

c) il contratto avente per oggetto un diritto reale immobiliare o la locazione di un immobile è disciplinato dalla legge del paese in cui l'immobile è situato;

d) in deroga alla lettera c), la locazione di un immobile concluso per uso privato temporaneo per un periodo di non oltre sei mesi consecutivi è disciplinata dalla legge del paese nel quale il proprietario ha la residenza abituale, purché il locatario sia una persona fisica e abbia la sua residenza abituale nello stesso paese;

e) il contratto di affiliazione (franchising) è disciplinato dalla legge del paese nel quale l'affiliato ha la residenza abituale;

f) il contratto di distribuzione è disciplinato dalla legge del paese nel quale il distributore ha la residenza abituale;

g) il contratto di vendita di beni all'asta è disciplinato dalla legge del paese nel quale ha luogo la vendita all'asta, se si può determinare tale luogo;

h) il contratto concluso in un sistema multilaterale che consente o facilita l'incontro di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, quali definiti all'articolo 4, paragrafo 1, punto 17, della Direttiva 2004/39/CE, conformemente a regole non discrezionali e disciplinato da un'unica legge, è disciplinato da tale legge.

2. Se il contratto non è coperto dal paragrafo 1 o se gli elementi del contratto sono contemplati da più di una delle lettere da a) ad h), del paragrafo 1, il contratto è disciplinato dalla legge del paese nel quale la parte che deve effettuare la prestazione caratteristica del contratto ha la residenza abituale.

3. Se dal complesso delle circostanze del caso risulta chiaramente che il contratto presenta collegamenti manifestamente più stretti con un paese diverso da quello indicato ai paragrafi 1 o 2, si applica la legge di tale diverso paese.

4. Se la legge applicabile non può essere determinata a norma dei paragrafi 1 o 2, il contratto è disciplinato dalla legge del paese con il quale presenta il collegamento più stretto".

Ovviamente anche queste BCR relative alla scelta della legge applicabile, saranno sottoposte al vaglio di ammissibilità della Lead DPA, la quale dovrà valutare la loro coerenza e validità sia sostanziale che formale rispetto sempre al Regolamento Roma1. Nello specifico, per ciò che attiene alla validità sostanziale si dovrà avere riguardo all'art. 10 par.1 del Regolamento Roma 1, secondo il quale: *"1. L'esistenza e la validità del contratto o di una sua disposizione si stabiliscono in base alla legge che sarebbe applicabile in virtù del presente Regolamento se il contratto o la disposizione fossero validi".*

Mentre per ciò che concerne la validità formale, il giudizio della Lead DPA dovrà assumere come metro di giudizio l'art. 11 parr.1,2 e 3 del Regolamento Roma 1, il quale dispone che:

"1. Un contratto concluso tra persone che si trovano, o i cui intermediari si trovano, nello stesso paese al momento della conclusione è valido quanto alla forma se soddisfa i requisiti di forma della legge che ne disciplina la sostanza ai sensi del presente Regolamento o della legge del paese in cui è concluso.

2. Un contratto concluso tra persone che si trovano, o i cui intermediari si trovano, in Paesi diversi al momento della conclusione è valido quanto alla forma se soddisfa i requisiti di forma della legge che ne disciplina la sostanza ai sensi del presente Regolamento o della legge del paese in cui si trova una delle parti, o il loro intermediario, al momento della conclusione oppure della legge del paese in cui una delle parti risiedeva abitualmente in quel momento.

3. Un atto giuridico unilaterale relativo ad un contratto concluso o da concludere è valido quanto alla forma se soddisfa i requisiti di forma della legge che disciplina o disciplinerebbe la sostanza del contratto ai sensi del presente Regolamento, o della legge del paese in cui detto atto è stato compiuto, o della legge del paese in cui l'autore dell'atto risiedeva abitualmente nel momento in cui l'ha compiuto".

Alla luce di quanto detto dunque, qualora sorga una controversia tra titolare e responsabile del trattamento in luogo del contratto da questi concluso, troveranno applicazione le disposizioni appena citate.

Discorso diverso invece, si ha nel caso in cui la doglianza sia sottoposta alla cognizione del giudice da parte di un dipendente, ovvero di un cliente della multinazionale. In queste ipotesi, il punto fondamentale che occorre sottolineare, è che le BCR nelle quali si fa riferimento alla legge applicabile, non troveranno applicazione rispetto ad una controversia tra una parte contrattuale e un interessato.

La spiegazione di ciò si evince chiaramente dal fatto che l'interessato non essendo parte contrattuale non può essere sottoposto alle obbligazioni assunte da altri soggetti. Inoltre la scelta di una determinata legge all'interno delle BCR non può mettere da parte le peculiari disposizioni che il Regolamento Roma 1 riserva a dipendenti e clienti consumatori.

Ovviamente, affinché trovino applicazione queste disposizioni particolari, è necessario che il soggetto preposto al trattamento dei dati personali dell'interessato sia entrato in *contatto* con tale soggetto terzo. Risulta dunque evidente che un tale rapporto di reciprocità si può avere solo allorché vi sia la conclusione di un contratto individuale tra il titolare del trattamento e l'interessato.

In una tale circostanza, è lampante che la tipologia contrattuale sarà diversa a seconda che l'interessato sia un dipendente, ovvero un cliente consumatore.

Dunque nella prima ipotesi la legge applicabile sarà quella indicata dall'art. 8 del Regolamento Roma 1, secondo il quale:

"1. Un contratto individuale di lavoro è disciplinato dalla legge scelta dalle parti conformemente all'articolo 3. Tuttavia, tale scelta non vale a privare il lavoratore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente in virtù della legge che, in mancanza di scelta, sarebbe stata applicabile a norma dei paragrafi 2, 3 e 4 del presente articolo.

2. Nella misura in cui la legge applicabile al contratto individuale di lavoro non sia stata scelta dalle parti, il contratto è disciplinato dalla legge del paese nel quale o, in mancanza, a partire dal quale il lavoratore, in esecuzione del contratto, svolge abitualmente il suo lavoro. Il paese in cui il lavoro è abitualmente svolto non è ritenuto cambiato quando il lavoratore svolge il suo lavoro in un altro paese in modo temporaneo.

3. Qualora la legge applicabile non possa essere determinata a norma del paragrafo 2, il contratto è disciplinato dalla legge del paese nel quale si trova la sede che ha proceduto ad assumere il lavoratore.

4. Se dall'insieme delle circostanze risulta che il contratto di lavoro presenta un collegamento più stretto con un paese diverso da quello indicato ai paragrafi 2 o 3, si applica la legge di tale diverso paese".

Mentre per ciò che attiene ad un contratto individuale stipulato con il cliente consumatore, per determinare la legge applicabile, sarà necessario rifarsi a quanto disposto dall'art. 6 del Regolamento Roma 1, ossia:

"1. Fatti salvi gli articoli 5 e 7, un contratto concluso da una persona fisica per un uso che possa essere considerato estraneo alla sua attività commerciale o professionale («il consumatore») con un'altra persona che agisce nell'esercizio della sua attività commerciale o professionale(«il professionista») è disciplinato dalla legge del paese nel quale il consumatore ha la residenza abituale, a condizione che il professionista:

a) svolga le sue attività commerciali o professionali nel paese in cui il consumatore ha la residenza abituale; o

b) diriga tali attività, con qualsiasi mezzo, verso tale paese ovari paesi tra cui quest'ultimo; e il contratto rientri nell'ambito di dette attività.

2. In deroga al paragrafo 1, le parti possono scegliere la legge applicabile a un contratto che soddisfa i requisiti del paragrafo in conformità dell'articolo 3. Tuttavia, tale scelta non vale a privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente ai sensi della legge che, in mancanza di scelta, sarebbe stata applicabile a norma del paragrafo 1.

3. Se i requisiti di cui al paragrafo 1, lettere a) o b) non sono soddisfatti, la legge applicabile a un contratto tra un consumatore e un professionista è determinata a norma degli articoli 3 e 4.

4. I paragrafi 1 e 2 non si applicano ai contratti seguenti:

a) ai contratti di fornitura di servizi quando i servizi dovuti al consumatore devono essere forniti esclusivamente in un paese diverso da quello in cui egli risiede abitualmente;

b) ai contratti di trasporto diversi dai contratti riguardanti un viaggio «tutto compreso» ai sensi della Direttiva 90/314/CEE del Consiglio, del 13 giugno 1990, concernente i viaggi, le vacanze ed i circuiti «tutto compreso» (1);

c) ai contratti aventi per oggetto un diritto reale immobiliare o la locazione di un immobile diversi dai contratti riguardanti un diritto di godimento a tempo parziale ai sensi della Direttiva 94/47/CE;

d) ai diritti e obblighi che costituiscono uno strumento finanziario e ai diritti e obblighi costitutivi delle clausole e condizioni che disciplinano l'emissione o l'offerta al pubblico e le offerte pubbliche di acquisizione di valori mobiliari, e alla sottoscrizione e al riacquisto di quote di organismi di investimento collettivo, nella misura in cui tali attività non costituiscono prestazione di un servizio finanziario;

e) ai contratti conclusi nell'ambito del tipo di sistema che rientra nel campo di applicazione dell'articolo 4, paragrafo 1, lettera h)".

Conclusioni

Alla luce del discorso condotto sulle BCR, si è potuto rilevare come tali clausole hanno assunto nel corso del tempo un ruolo sempre più importante nella tutela del diritto alla protezione dei dati personali. Come si è più volte sottolineato, le BCR, come strumento di tutela, non erano previste all'interno della Direttiva 95/46 e la loro introduzione nel Regolamento n. 679 del 2016, rappresenta solo l'ultimo tassello di una crescente attenzione che il Legislatore europeo a posto sul diritto alla protezione dei dai personali. Poiché attraverso l'evoluzione della scienza e della tecnica, la dematerializzazione dei dati personali ha richiesto forme di protezione sempre più coerenti alle tipologie di trattamento di cui i dati personali possono essere oggetto. Esempio di questa costante attenzione all'evoluzione, sono stati certamente gli elaborati del WP 29, nei quali è possibile rinvenire la monolitica descrizione ed elencazione degli strumenti che sono in grado di fornire delle adeguate garanzie di tutela al diritto alla protezione dei dati personali. Sulla base di ciò dunque, si può avanzare una prima conclusione, secondo la quale, nei trattamenti di dati personali eseguiti fuori dai confini europei, l'introduzione delle BCR nei contratti di trasferimento degli stessi dati, rappresenta lo strumento che meglio assicura che il trattamento sarà operato in conformità delle garanzie comunitarie. Come si è avuto modo di apprezzare poi, la certezza che ciò avvenga, si rinviene dal fatto che tali clausole contrattuali debbano necessariamente superare un vaglio di ammissibilità da parte della Lead DPA alla quale la multinazionale decida di sottoporre il controllo delle proprie BCR. Inoltre, al fine di assicurare la corrispondenza delle BCR ai principi di tutela di questo diritto fondamentale, e affinché il *corpus* redatto abbia un uniforme riconoscimento all'interno dell'UE si è evidenziata l'evoluzione che ha avuto la procedura di approvazione delle norme vincolanti d'impresa, poiché si è passati da una farraginosa "procedura di cooperazione europea" ai più rapidi modelli di "coerenza e cooperazione". In definitiva lo strumento delle BCR si muove su tre piani distinti, ma che rappresentano gli elementi di un unico scopo, cioè la tutela del diritto alla protezione dei dati personali. Il primo è rappresentato dalle BCR proprio come strumento attraverso il quale è possibile garantire la tutela del diritto. Si tratta dunque di guardare ai requisiti materiali che tali clausole devono possedere. Su questo punto come si è osservato, la normativa

europea è ancora carente, perché sebbene con il Regolamento n. 679 del 2016, vi è stata l'introduzione di una norma che ne qualifica lo scopo, allo stesso tempo esso tace sugli elementi materiali che le BCR devono avere per raggiungerlo. In questo contesto è intervenuto una volta di più il WP 29 che, attraverso i propri elaborati ha costruito l'impianto dei requisiti materiali che le BCR devono contenere al fine di tutelare il diritto dell'interessato. Tale assunto risulta fondamentale per comprendere fino in fondo le peculiarità delle BCR, poiché alla luce del predetto lavoro operato dal WP 29 da un lato, e attraverso l'opera di redazione dei testi BCR da parte delle multinazionali dall'altro, si realizza quel fenomeno che è stato definito *Transnational Private Regoulation.* Questo fenomeno, se considerato in chiave generale può essere inteso come l'opera di regolamentazione che soggetti privati pongono in essere in relazione ad un determinato ambito del diritto. Detto in altri termini, i privati, in questo caso le multinazionali, si sostituiscono al legislatore nel compiere delle attività di *normazione.* Ovviamente, l'ausilio del termine *normazione*, non solo stride con le attività dei privati, ma in linea di principio risulta del tutto destituito di fondamento, poiché è lampante che al privato non è riconosciuto il potere di creare fonti di diritto. Tuttavia, se si prende in considerazione la lacuna del Regolamento n. 679 del 2016 in merito alla definizione dei requisiti materiali delle BCR, appare di fatto necessario trovare un espediente tecnico, che possa fornire l'inevitabile certezza del diritto di cui necessitano le operazioni di trasferimento e trattamento dei dati personali. Tale certezza, nel contesto delle BCR si raggiunge attraverso la decisione di ammissibilità che la Lead DPA emana in relazione al testo di BCR che la multinazionale presenta. Ovviamente, un singolo testo, non potrà assurgere a modello al quale altri soggetti privati possono guardare per costruire un impianto di clausole che possa fornire delle adeguate garanzie di tutela del diritto alla protezione dei dati personali. Pertanto al fine di avere una *normazione*, in questo caso dei requisiti materiali delle BCR, è necessario analizzare il fenomeno che corre sottotraccia nel corso delle singole procedure di approvazione dei singoli testi di BCR. Si noti infatti, che durante queste operazioni, viene alla luce quasi impercettibilmente, un *corpus* di requisiti comuni ad ogni singolo impianto di norme vincolanti d'impresa. Sebbene sia arduo individuare in modo tangibile un fenomeno di tale portata, delle presunzioni in questo senso risultano ammissibili se si guarda allo scopo del Regolamento

n. 679 del 2016. Si tratta del fatto di rendere in tutto il territorio dell'Unione Europea un'uniforme tutela del diritto alla protezione dei dati personali attraverso una uniforme applicazione del Regolamento stesso. Dunque, essendo lo scopo delle BCR quello di fornire delle adeguate garanzie di tutela attraverso il vaglio di ammissibilità da parte delle Lead DPA, quest'ultima, essendo organo preposto alla garanzia del diritto, necessariamente dovrà confrontarsi con le altre DPA non solo per dare attuazione ai meccanismi di coerenza e cooperazione, ma anche per raggiungere gli specifici obiettivi di uniforme applicazione del Regolamento. Alla luce di ciò, è dunque possibile concludere che questa *normazione* dei requisiti delle BCR, o per meglio dire meta-regolamentazione, derivante dal lavoro delle multinazionali, delle DPAs e del WP 29, può essere considerata come la chiave di volta per dare attuazione uniforme ai principi del Regolamento n. 679 del 2016 attraverso l'individuazione di un substrato comune del regime in cui le BCR devono essere intese e quindi redatte. In definitiva le BCR possono essere intese in due declinazioni, ossia: testo delle BCR e regime delle BCR. Il primo riguarderà il costrutto figlio del lavoro delle multinazionali, mentre il secondo sarà considerato come il frutto della *normazione*, o meta-regolamentazione, al quale la singola impresa potrà ispirarsi nella redazione del proprio testo da sottoporre alla Lead DPA prescelta. Per quanto concerne il secondo e terzo piano sul quale si muovono le norme vincolanti d'impresa, questi si presentano in stretta correlazione tra loro, poiché si tratta di contesti in cui la necessaria introduzione e applicazione delle BCR sono rivolte alla "salvaguardia" delle multinazionali che ne redigono il testo. Il secondo può essere inteso come un contesto nel quale le BCR sono redatte dal titolare del trattamento, al fine di evitare le sanzioni che possano derivare da una mancata tutela del diritto alla protezione dei dati personali. Si tratta quindi di un contesto rappresentato dal famoso principio di *accountability*, nel quale il titolare del trattamento avrà un particolare interesse a redigere un elenco di BCR che possa efficacemente prevedere tutte le patologie nel quale il trattamento dei dati personali potrà incorrere. Occorre una volta di più precisare che il principio di *accountability,* sebbene sia traducibile con il termine responsabilità, nell'ambito delle BCR è inteso in un'accezione più generale. Il problema della generalità potrebbe sollevare dubbi interpretativi poiché, essendo le BCR delle clausole che trovano nel contratto la loro sede naturale, la maggior

parte delle impostazioni codicistiche guarda alla responsabilità contrattuale come quella derivante dal mero inadempimento delle obbligazioni in esso contenute. Pertanto sarebbe naturale sostenere che per far scattare un onere al risarcimento del danno è necessaria una violazione delle semplici clausole contrattuali. Tuttavia, la natura generale dell'*accountability* oltrepassa gli argini della responsabilità contrattuale, poiché il principio, oltre al dovere di rispettare le obbligazioni contrattuali ha come obiettivo quello di dare attuazione a tutti i principi che si ritrovano nel Regolamento n. 679 del 2016. Sulla base di tale assunto dunque, non sembra essere una forzatura ammettere che l'interessato possa richiedere il risarcimento del danno non solo in caso di violazione degli oneri strettamente contrattuali, ma anche nelle ipotesi in cui il titolare (e o il responsabile) del trattamento con la sua condotta ponga in essere delle attività che contrastano con la tutela del diritto alla protezione dei dati personali. In conclusione, è quindi ammissibile sostenere che il principio di *accountability* innesta all'interno del sistema delle responsabilità contrattuale, anche il seme della clausola di responsabilità *atipica,* secondo la quale, alla luce di quanto disposto dall'art. 1383 del *Code civil* e dell'art. 2043 del Codice Civile si ammette un risarcimento del danno per *tuout fait quelconque* (qualunque fatto). Un tale assunto è poi confermato anche dallo stesso art. 24 *par. 1* del Regolamento n. 679 del 2016 che ammette il risarcimento per qualsiasi tipologia di danno, sia materiale che immateriale. Ovviamente, alla luce dei principi che ispirano il Regolamento n. 679 del 2016, l'interesse preminente è quello di tutelare il diritto alla protezione dei dati personali e non già quello di punire il titolare (e o il responsabile) del trattamento. Dunque, in questa luce vanno lette le disposizioni che disciplinano i meccanismi approvazione delle BCR, cioè attraverso il preventivo giudizio di ammissibilità fornito dalla Lead DPA, vi è una sorta di collaborazione tra l'Autorità e l'impresa al fine di rispettare i principi ispiratori del Regolamento. Infine il terzo piano, e forse il più importante, nel quale si muovono le BCR, è rappresentato dal rispetto della *compliance*. Si tratta di un profilo che riguarda lo stretto rapporto tra il trattamento dei dati personali e i principi di tutela che ispirano tutto il Regolamento 679 del 2016. Rispettare la *compliance* per una multinazionale significa dunque che le operazioni che questa pone in essere siano conformi a quanto previsto dal Regolamento in materia di tutela.

Per far sì che ciò avvenga si è evidenziata l'importantissima innovazione che ha introdotto la nuova disciplina a differenza della Direttiva 95/46, cioè l'introduzione di un soggetto terzo rispetto alla multinazionale, quale titolare e responsabile del trattamento, e l'Autorità di controllo. Si tratta del *Data Protection Officer*, ossia il soggetto responsabile della protezione dei dati personali, una figura centrale nel triangolare rapporto tra interessato, titolare (e/o responsabile) e DPAs al quale è demandato proprio il compito di cooperare con i soggetti che operano il trattamento dei dati, al fine di guidarli nelle scelte che possano garantire le adeguate tutele al diritto sulla protezione dei dati personali. Alla luce di ciò dunque, il DPO può essere considerato come il soggetto che, meglio di ogni altro possa far sì che la multinazionale presso la quale svolge le proprie funzioni, persegua e rispetti i caratteri della *compliance* tra le attività di trattamento dei dati personali e i principi derivanti dal Regolamento n. 679 del 2016. Se valutato in questa prospettiva inoltre, il DPO può essere considerato anche come un soggetto in grado di porre rimedio ai rischi derivanti dalle lacune presenti nei vari livelli di apprendimento. Come si è analizzato, i rischi che possono portare ad un mancato rispetto della *compliance*, attengono alla mancata attuazione del *secondo livello di apprendimento, del terzo livello di apprendimento* e delle lacune che invece presenta *il primo livello di apprendimento.* Per comprendere l'importanza che il DPO assume in questo contesto è necessario ricordare brevemente a cosa corrispondono i sopracitati livelli e valutare gli interventi che il DPO può porre in essere per dar luogo ad un effettivo rispetto della *compliance*. Per ciò che concerne il primo, questo ha ad oggetto le istruzioni che ricevono i dipendenti delle multinazionali sulle modalità di redazione delle BCR e gli elementi che queste devono possedere, il tutto temperato sulla valutazione della rischiosità del trattamento che dovranno regolare. In questo caso, l'intervento del DPO è auspicabile al fine di condurre il titolare del trattamento ad una comprensione maggiormente approfondita dei rischi che il trattamento presenta. Nel caso del *secondo livello di apprendimento* invece, il problema che si pone è la carenza di un'ulteriore revisione del testo delle BCR da parte della multinazionale dopo il giudizio di ammissibilità positivo pervenuto dalla Lead DPA. Ebbene, anche in questa ipotesi l'intervento del DPO significherebbe porre una volta di più l'attenzione sulle probabili patologie delle clausole a ulteriore garanzia del giudizio di ammissibilità della Lead DPA.

Infine in ordine al *terzo livello di apprendimento* come si è visto, la situazione pregiudiziale potrebbe sorgere allorché non siano colmate le eventuali lacune del *primo livello di apprendimento.* Ebbene, in questa ipotesi si coglie maggiormente il necessario apporto della figura del DPO, il quale, attraverso le proprie competenze tecniche sarebbe in grado non solo di aiutare il titolare del trattamento nel colmare le lacune dispositive. Poiché sarebbe altresì capace di porre l'attenzione su carenze che lo stesso titolare del trattamento avrebbe ignorato. In conclusione è quindi possibile sostenere che le BCR che regolano le operazioni di trattamento dei dati personali, siano il migliore strumento che possa garantire il rispetto della *compliance,* quando gli stessi dati siano oggetto di un trasferimento verso un paese terzo che non presenti adeguate garanzie di tutela. Ovviamente, la loro introduzione rappresenta un importante tassello nella costruzione di un sempre più efficace modello di protezione, ma allo stesso tempo il percorso per una loro totalmente efficace operatività è ancora lungo, ed espressione di ciò è il fatto che il nuovo Regolamento è ancora orfano di una disposizione che fissi un'elencazione dei requisiti materiali che tali clausole devono possedere. Pertanto, nel momento in cui ciò avverrà, le BCR potranno consolidare ancor di più il loro ruolo di preminenza nella tutela di un diritto fondamentale, quale il diritto alla protezione dei dati personali.

Bibliografia

1. **Alpa G.**, (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983.

2. **Alpa G.,** La *normativa sui dati personali. Modelli di lettura e problemi esegetici*, in CUFFARO V., RICCIUTO V., ZENO-ZENCOVICH V. (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1998, pp. 26 ss.

3. **Alpa G. - Bessone M.**, *Banche dati, telematica e diritti della persona*, Padova, 1984.

4. **Alpa G. - Conte G.**, *La responsabilità d'impresa*, 2015.

5. **Alvarez D**., *Safe Harbor Is Dead; Long Live the Privacy Shield*, in Business Law Today, Vol. 2016, Issue 5, 2016.

6. **Ash G. R**., *Dynamic routing in telecommunications networks*, New York, 1998.

7. **Bender D. - Ponemon L.**, *Binding corporate rules for cross-border data transfer*, Rutgers Journal of Law & Urban Policy, Vol.3, 2006.

8. **Bomhoff J. - Meuwese A.**, *The Meta-Regulation of Transnational Private Regulation*, Journal of Law and Society, Vol. 38, N. 1, March 2011.

9. **Brunetti R**., *Windows Azure: il sistema operativo e la piattaforma per il cloud computing*, Mondadori informatica, 2009.

10. **Büthe, Mattli**, *The New Global Rulers: The Privatization of Regulation in the World Economy*, Princeton University, 2011.

11. **Buttarelli G.**, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997.

12. **Cafaggi F**., *New Foundations of transnational private regulation*, EUI Working papers RSCAS 2010/53.

13. **Carpenter, R. H. Jr**., *Walking from Cloud to Cloud: The Portability Issue in Cloud Computing*, Washington Journal of Law, Technology & Arts, Vol. 6, Issue 1, 2010.

14. **Coslovich L**., *Dynamic vehicle routing and dispatching: heuristic techniques for people and freight transportation*, Trieste, 2005.

15. **Curtin, Senden**, *Public accountability of Transnational Private regulation*, in Journal of Law and Society, 2011.

16. **D'Acquisto G. – Naldi M.**, *Big data e privacy by design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, 2017, p. 33 ss.

17. **De Hert P**., **Papakonstantinou V**., **Wright D**. and **Gutwirth S**., *The proposed Regulation and the construction of a principles - driven system for individual data protection*, The European Journal of Social Science Research 2013, p. 133 ss.

18. **Finocchiaro G.**, *Binding Corporare Rules* in Contratto e Impresa, Vol. II, 2006.

19. **Frediani V.**, *Applicazione delle B.C.R.: dal Working Party Art. 29.LE INDICAZIONI*, Documento digitale, marzo 2015,

20. **Follesdal, Wesse, Wouters**, *Multilevel regulation and the EU, The interplay between global, European and national normative processes*, Boston, 2008.

21. **Geissler R. C.**, *Private Eyes Watching you: Google Street View and Right to an Inviolate Personality*, in Hasting Law Journal, Vol. 63, 2012.

22. **Gilbert F**., *Use of Cloud Computing in a Law Office*, Practical Lawyer, Vol. 60, Issue 2, 2014.

23. **Gritti F**., *La responsabilità civile nel trattamento dei dati personali*, in V. Cuffaro, V. Ricciuto, R. D'Orazio, Il Codice del trattamento dei dati personali, Torino, 2007.

24. **Gutwirth S**., *Reinventing Data Protection*, Springer, 2009.

25. **Joerges C**., *Rethinking European Law's Supremacy*, EUI Working Papers 2005.

26. **Losano M**. **G**., *La privacy nelle legislazioni europee*, 1981.

27. **Mantelero A**., *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, 2007.

28. **McCusker S.**, *EU-US Privacy Shield: The Antidote to the Transatlantic Data Transfer Headache*, Business Law Review, Vol. 37, Issue 3, 2016.

29. **McCormac B.**, *Invalidation of Safe Harbor*, Iowa Lawyer, Vol. 76, Issue 2, 2016.

30. **Mesaikou E.***, Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive: a comparative study with the Cross Border Privacy Rules developed in the APEC*, 2013.

31. **Moerel E**. **M. L.**, *Binding Corporate Rules: Fixing the regulatory patchwork of data protection*, Tilburg University, 2011.

32. **Moerel E. M. L.**, *Privacy without Borders*, in Dutch Financial Times, 3 April 2003.

33. **Panetta R**., *Libera circolazione e protezione dei dati personali*, Roma, 2006.

34. **Pizzetti F.**, *Privacy e diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I, Giappichelli, 2016

35. **Pizzetti F**., *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679,* Vol. II, Giappichelli, 2016.

36. **Poullet Y**., *pour une justification des article 25 et 26 de la directive européenne 95/46/CE en matiére de flux transfrontalièreet deprotection ds donne,* in Juris-Classeur, Chronique,n. 69, 2003, p. 9 ss.

37. **Resta G**. - **Zeno-Zenkovich** V., *La protezione transnazionale dei dati personali: dai "Safe harbour principles" al "Privacy shield"*, Roma Tre Press, 2016.

38. **Riccio G**. **M.**, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, Roma, 2016.

39. **Riccio G. M.**, *I trasferimenti di dati personali all'estero*, in V. Cuffaro, V. Ricciuto, R. D'Orazio, Il Codice del trattamento dei dati personali, Torino, 2007.

40. **Riccio G. M.**, *Data Protection Officer e altre figure*, in La nuova disciplina europea della privacy, Padova, 2016.

41. **Rossi R**., *Cloud computing per la piccola e media impresa: la gestione dell'IT nella nuvola: approccio pratico e vantaggi*, Milano, 2015.

42. **Rodotà S**., *Il diritto di avere diritti*, Laterza, Bari, 2012.

43. **Scott C. D**., *Enforcing Consumer Protection Laws*, (July 30, 2009), UCD Working Papers, Law, Criminology & Socio-Legal Studies Research Paper No. 15/2009.

44. **Stuckem M**. **– Grunes A**., *Big Data and Competition Policy*, Oxford University Press, Oxford, 2016.

45. *The privacy, data protection and cybersecurity law review*, a cura di **Alan Charles Raul**, London, 2016.

46. **Trudel P**., *Privacy Protection on the Internet*, 2012.

47. **Tzanou M.**, *The Fundamental Right to Data Protection: Normative Value in the Contest of Counter – Terrorism Surveillance,* Hart Publishing, Oxford, 2017.

48. **Van Reeken B**., Outsourcing, *Juridische gids voor de praktijk*, Wolthers Kluwer, 2009.

49. **Viergever L**., Privacy *in the Clouds*, 2010.

50. **Voss W**. **G**., *The future of transatlantic data flows: Privacy Shield or bust?,* in Journal of Internet Law, Vol. 19, Issue 11, 2016.

51. **Warren S. D. – Brandeis L. D.**, *The right to privacy*, in Harvard Law Rev., Vol. 4, Issue 5, 1890.

Atti normativi di riferimento

1. La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, integrata e modificata dai Protocolli. Roma 4.XI.1950.

2. Risoluzione del Consiglio d'Europa (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico (Adottata dal Comitato dei Ministri il 20 settembre 1974 durante la 236ma riunione dei Delegati dei Ministri).

3. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28 gennaio 1981.

4. Carta dei Diritti Fondamentali dell'Unione europea, GU C 326 del 26.10.2012.

5. Versione consolidata del Trattato sull'Unione europea, GU C 326 del 26.10.2012.

6. Versione consolidata del Trattato sul funzionamento dell'Unione europea, GU C 326 del 26.10.2012.

7. 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. GU L 281 del 23.11.1995.

8. Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, 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, GU L 8 del 12.1.2001.

9. 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) (Testo rilevante ai fini del SEE), GU L 119 del 4.5.2016.

10. Regolamento (CE) N. 593/2008 del Parlamento Europeo e del Consiglio del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali (Roma I).

11. Regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, GU L 12 del 16.1.2001.

12. Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, GU L 351 del 20.12.2012.

13. 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 dell'esercizio delle competenze di esecuzione attribuite alla Commissione, GU L 55 del 28.2.2011.

14. Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (Testo rilevante ai fini del SEE), GU L 337 del 18.12.2009.

15. Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006.

16. Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L 201 del 31.7.2002.

17. Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, 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, GU L 8 del 12.1.2001.

18. Legge n. 675 del 31 dicembre 1996 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467), Pubblicato sulla GU n. 5 dell'8 gennaio 1997.

19. Decreto legislativo 30 giugno 2003, n. 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, Pubblicato sulla GU n.174 del 29 luglio 2003.

20. Commissione Europea, Decisione della Commissione del 27 dicembre 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in paesi terzi, a norma della direttiva 95/46/CE [C(2001) 4540] (2002/16/CE).

21. Commissione Europea, comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e Sociale Europeo e al Comitato delle Regioni, Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo, Bruxelles, 25.1.2012 COM(2012) 9 finale.

22. Commissione Europea, decisone della Commissione del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE [C(2001) 1539] (2001/497/CE).

23. Commissione Europea, decisone della commissione del 27 dicembre 2004 che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi [C (2004) 5271] (2004/915/CE).

24. Commissione Europea, decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento Europeo e del Consiglio [C (2010) 593] (2010/87/UE).

25. Commissione Europea, comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e Sociale Europeo e al Comitato delle Regioni, Un approccio globale alla protezione dei dati personali nell'Unione europea, Bruxelles, 4.11.2010 COM(2010) 609 definitivo.

26. European Commission, Proposal for a "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL"on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD).

27. Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM (2015) 566 final, 6 November 2015.

28. Statement of the Article 29 Working Party on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), 16 October 2015.

29. European Parliament Directorate General for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Study for the LIBE Committee, 2015, available at: <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf> accessed 17 November 2015.

30. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 final, 27 November 2013.

31. Communication from the Commission to the European Parliament and the Council entitled Rebuilding Trust in EU-US Data Flows, COM (2013) 846 final, 27 November 2013.

32. Commission Memorandum Restoring Trust in EU-US data flows – Frequently Asked Questions, MEMO/13/1059, 27 November 2013.

33. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 25 January 2012.

34. European Commission, Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, available at: <http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf> accessed 10 November 2015.

35. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, (notified under document C(2010) 593) (Text with EEA relevance) (2010/87/EU) OJ L 39, 12.2.2010.

36. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

37. Council of the European Union, EU Counter-terrorism Strategy, 14469/4/05 REV 4, Brussels, 30 November 2005.

38. Commission Decision (2004/915/EC) of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004.

39. Decision NO 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties, [2002] OJ L183/1.

40. Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 6, 10.1.2002.

41. Commission Decision (2001/497/EC) of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001.

42. Commission Decision (2000/520/EC) of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. OJ 2000 L 215, p.7.

43. Parere del garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati (2007/C255/01).

44. Commissione Europea, Comunicazione della Commissione al Parlamento Europeo e al Consiglio, scambio e protezione dei dati personali in un mondo globalizzato, Bruxelles, 10.1.2017 COM(2017) 7 finale.

Article 29 Working Party's Document

1. Article 29 Working Party, *Discussion Document, First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy* (WP 4), 26 June 1997.

2. Article 29 Data Protection Working Party, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, at 9, (WP 168), 1 December 2009.

3. Article 29 Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), 24 July 1998.

4. Article 29 Working Party, *Working document on a common interpretation of Article 26 of Directive 95/46/EC of 24 October 1995*(WP 114), 25 November 2005.

5. Gruppo di Lavoro *ex* Articolo 29 - Gruppo di lavoro per la tutela dei dati personali - WP 90 - Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE.

6. Article 29 Working Party, *Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States (WP 66)* , 24 October 2002.

7. Article 29 Working Party, *Opinion 8/2001, on the processing of personal data in the employment context (WP 48),* 13 September 2001.

8. Article 29 Working Party, *Working Document Setting Forth a Co-Operation Procedure for Issuing Commons Opinions on Adeguate Safeguards Resulting From "Binding Corporate Rules"* (WP 107) April 14th, 2005.

9. Article 29 Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 26 of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (WP 74), 3 June 2003.

10. Article 29 Working Party, *Working document that provides a template for the Checklist for the approval of the binding Corporate Regulation* (WP 108) 14 April 2005.

11. Article 29 Working Party, *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (WP 133), 10 January 2007.

12. Article 29 Working Party, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules* (WP 153), 24 June 2008.

13. Article 29 Working Party, *Working Document setting up a framework for the structure of Binding Corporate Rules* (WP 154), 24 June 2008.

14. Article 29 Working Party, *Working Document on Frequently Asked Questions (FAQs) to Binding Corporate Rules* (WP 155), adoted on 24 June 2008, As last Revised and adopted on 8 April 2009.

15. Article 29 Working Party, *Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union* (WP 106), 18 January 2005.

16. Article 29 Working Party, Opinion 3/2010 on the principle of accountability (WP 173), 13 July 2010.

17. Article 29 Working Party, WP 169, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169), 16 February 2010.

18. Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*(WP 243 rev.01), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017.

19. Article 29 Working Party, Opinion 15/2011 on the definition of consent (WP 187), 13 July 2011.

20. Article 29 Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 1 December 2015.

21. Article 29 Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679* (WP 250), 3 October 2017.

22. Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251) 3 October 2017.

23. Article 29 Working Party, *Adequacy Referential (updated)* (WP 254), 28 November 2017.

24. Article 29 Working Party, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (for Controllers)*(WP256), 29 November 2017.

25. Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (for Processors)(WP 257), 29 November 2017.

26. Article 29 Working Party, Opinion 2/2017 on data processing at work (WP 249), 8 June 2017.

18. Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs'*)(WP 243 rev.01), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017.

19. Article 29 Working Party, Opinion 15/2011 on the definition of consent (WP 187), 13 July 2011.

20. Article 29 Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 1 December 2015.

21. Article 29 Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679* (WP 250), 3 October 2017.

22. Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251) 3 October 2017.

23. Article 29 Working Party, *Adequacy Referential (updated)* (WP 254), 28 November 2017.

24. Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (for Controllers)(WP256), 29 November 2017.

25. Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (for Processors)(WP 257), 29 November 2017.

26. Article 29 Working Party, Opinion 2/2017 on data processing at work (WP 249), 8 June 2017.

27. Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*(WP 248 rev.1) 4 April 2017, As last Revised and Adopted on 4 October 2017.