IAIC MiBACT DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA
Alberto M. Gambino

COMITATO DI DIREZIONE
Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

30 novembre 2018

I servizi di *cloud computing* e l'ambito di applicazione del Regolamento (UE) n. 2016/679: verso l'avvicinamento del modello europeo e statunitense?

Veronica Gallo

COMITATO SCIENTIFICO
Guido Alpa, Fernando Bocchini, Giovanni Comandè, Gianluca Contaldi,
Vincenzo Di Cataldo, Giorgio Floridia, Gianpiero Gamaleri, Gustavo Ghidini,
Andrea Guaccero, Mario Libertini, Francesco Macario, Roberto Mastroianni,
Giorgio Meo, Cesare Mirabelli, Enrico Moscati, Alberto Musso, Luca Nivarra,
Gustavo Olivieri, Cristoforo Osti, Roberto Pardolesi, Giuliana Scognamiglio,
Giuseppe Sena, Vincenzo Zeno-Zencovich, Andrea Zoppini
E
Margarita Castilla Barea, Cristophe Geiger, Reto Hilty, Ian Kerr, Jay P. Kesan,
David Lametti, Fiona MacMillan, Maximiliano Marzetti, Ana Ramalho,
Maria Pàz Garcia Rubio, Patrick Van Eecke, Hong Xue

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA). Tutti i diritti sono dell'IAIC.

Comitato dei Valutazione Scientifica

EMANUELA AREZZO (Un. Teramo), EMANUELE BILOTTI (Un. Europea di Roma), FERNANDO BOCCHINI (Un. Federico II), ROBERTO BOCCHINI (Un. Parthenope), ORESTE CALLIANO (Un. Torino), LOREDANA CARPENTIERI (Un. Parthenope), LUCIANA D'ACUNTO (Un. Federico II), VIRGILIO D'ANTONIO (Un. Salerno), FRANCESCO DI CIOMMO (Luiss), PHILIPP FABBIO (Un. Reggio Calabria), MARILENA FILIPPELLI (Un. Tuscia), CESARE GALLI (Un. Parma), MARCO MAUGERI (Un. Europea di Roma), ENRICO MINERVINI (Seconda Un.), MARIA CECILIA PAGLIETTI (Un. Roma Tre), ANNA PAPA (Un. Parthenope), ANDREA RENDA (Un. Cattolica), ANNARITA RICCI (Un. Chieti), FRANCESCO RICCI (Un. LUM), GIOVANNI MARIA RICCIO (Un. Salerno), CRISTINA SCHEPISI (Un. Parthenope), BENEDETTA SIRGIOVANNI (Un. Tor Vergata), GIORGIO SPEDICATO (Un. Bologna), ANTONELLA TARTAGLIA POLCINI (Un. Sannio), RAFFAELE TREQUATTRINI (Un. Cassino), DANIELA VALENTINO (Un. Salerno), FILIPPO VARI (Un. Europea di Roma), ALESSIO ZACCARIA (Un. Verona).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Comitato di Redazione – www.dimt.it – dimt@unier.it

ALESSANDRO ALBANESE GINAMMI, MARCO BASSINI, CHANTAL BOMPREZZI, FRANCESCA CORRADO, CATERINA ESPOSITO, GIORGIO GIANNONE CODIGLIONE, FERNANDA FAINI, MONICA LA PIETRA, SILVIA MARTINELLI, DAVIDE MULA (Coordinatore), ALESSIO PERSIANI, ROSARIA PETTI, MARTINA PROVENZANO (Vice-Coordinatore), MATILDE RATTI, CECILIA SERTOLI, SILVIA SCALZINI, ANDREA STAZI (Coordinatore)

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

I servizi di *cloud computing* e l'ambito di applicazione del Regolamento (UE) n. 2016/679: verso l'avvicinamento del modello europeo e statunitense?

Veronica Gallo
InnoLawLab – Università Europea di Roma

Sommario: 1. Introduzione – 2. La tutela della privacy in Europa e negli Stati Uniti d'America – 3. L'applicazione territoriale del Regolamento UE n. 679/2016 e i servizi di *cloud computing*; 3.1 Il trattamento dei dati personali sulle piattaforme *cloud*; 3.2 La protezione dei dati personali sulle nuvole informatiche – 4. I presupposti di legittimità al trasferimento dei dati personali; 4.1 Il trasferimento dei dati verso gli Stati Uniti; 4.2 La questione Brexit e il suo impatto sul trasferimento transfrontaliero dei dati – 5. Conclusioni: verso l'avvicinamento del modello europeo e statunitense

1. Introduzione

L'analisi che segue prende le mosse dalla disamina comparatistica della differente concezione del diritto alla privacy in ambito europeo e statunitense in relazione all'evoluzione tecnologica con particolare riferimento all'odierno scenario *cloud* e *big data oriented*. Si cercherà di delineare le caratteristiche dei due distinti modelli che si sono nel tempo affermati, differenziandosi con approcci diametralmente opposti: l'uno, quello statunitense, attribuendo un ruolo preminente ai giudici; l'altro, quello europeo, affidando un ruolo maggioritario alle Autorità indipendenti di settore.

Si analizzeranno in seguito le caratteristiche dei servizi *cloud* evidenziando come tale tecnologia abbia, da un lato, semplificato la modalità di trattamento dei dati mediante l'uso di strumenti elettronici ma, dall'altro, abbia privato i titolari del trattamento che vi ricorrono del potere di verifica in concreto del rispetto delle clausole da parte dei *cloud provider*. Le caratteri-

stiche dei servizi *cloud* e dei relativi contratti che hanno una dimensione intrinsecamente internazionale hanno portato alla definizione di modelli contrattuali condivisi in ambito internazionale che superano le classificazioni operate su base del solo diritto interno.

In ultimo, fornito un breve inquadramento sulla legislazione europea in materia di protezione dei dati personali di cui al Regolamento (UE) n. 2016/679, si cercherà di dare evidenza di come, a fronte dell'internazionalizzazione dei servizi *cloud* da una parte, e l'esteso ambito di applicazione del Regolamento dall'altro, paia potersi intravedere un timido ma progressivo avvicinamento, ancorché solo su base volontaria, tra il modello europeo e quello statunitense.

2. La tutela della privacy in Europa e negli Stati Uniti d'America

Il termine «*privacy*», può avere significati polisemici, potendo essere inteso come «riservatezza» consistente nel diritto di escludere altri dalla conoscenza di vicende personali e come «protezione dei dati», o «*data protection*», indicando il diritto di un soggetto a controllare l'insieme di informazioni che a lui si riferiscono e che costituiscono il suo riflesso nella Società dell'informazione.

Anteriormente allo sviluppo tecnologico nonché alla nascita dei *social network,* il concetto di privacy veniva così ad identificarsi con il diritto, di matrice statunitense, di "*essere lasciato solo*", il cd. "*the right to be let alone*" [1].

[1] S. Warren, L. Brandeis, *The right to privacy*, in *Harward Law Review*, 1890, pp. 213 e ss. A Warren e Brandeis va ricondotta la prima formulazione del "*right to privacy*" ma non la prima enunciazione dello stesso. Tale concetto fu infatti anticipato già da studi precedenti, in particolare da quello del giudice Cooley (T. M. Cooley, *A Treatise on the Law of Torts. Or the Wrongs which Arise Independent of Contract*, Chicago, 1888, p. 29) il quale, nell'analizzare il diritto alla *privacy* in relazione alla sicurezza personale, aveva affermato «*the right to one's person may be said to be a right of complete immunity: to be let alone*». È stato però notato che Cooley aveva utilizzato il concetto in questione in un'accezione diversa da quella di Warren e Brandeis, avendo infatti egli alluso alla libertà di ciascuno di rifiutarsi di esercitare una certa libertà civile e non a quello di decidere se rendere noti ad altri determinati aspetti della propria personalità e vita privata (A. Baldassarre, "*Privacy e Costituzione: l'esperienza statunitense*", Bulzoni, Roma, 1974, p. 40 ss.). In entrambi i casi venne comunque sancito il principio della *inviolate personality* che i due avvocati ritennero parte del più generale diritto all'immunità della persona, *the*

A margine del diritto alla privacy la dottrina europea sin dalla fine degli anni '60 ha teorizzato il diritto alla protezione dei dati, come diritto dei singoli a limitare l'impiego dei propri dati personali per finalità diverse rispetto a quelle per cui i dati sono stati conferiti. L'avvento delle tecnologie informatiche e telematiche e la possibilità di utilizzare i dati personali per molteplici finalità ha favorito la progressiva affermazione di questo secondo diritto nella legislazione europea. La risposta normativa europea al mutare dei contesti tecnologici di riferimento è stata, infatti, la disciplina positiva della protezione dei dati attribuendo al soggetto a cui gli interessati conferiscono i dati, ovvero il titolare del trattamento dei dati, l'obbligo di rispettare i vincoli posti e di proteggere i dati ricevuti[2].

Sono *ictu oculi* evidenti le profonde differenze che caratterizzano i due modelli di tutela: da un lato vi è l'ampio diritto ad impedire turbative nella propria vita privata - diritto alla *privacy* -, che non prevede una legislazione di riferimento ed è azionabile solo in sede giudiziaria, dall'altra c'è un diritto a che i soggetti a cui i dati vengono conferiti li proteggano - *right to data protection* -, che al contrario del primo reca una analitica serie di previsioni di dettaglio e prevede strumenti rimediali anche stragiudiziali. Ciò che, parallelamente, emerge è che mentre in Europa la "*data protection*" si affianca alla tutela della "*privacy*", negli Stati Uniti d'America il diritto alla privacy non porta con se anche la protezione dei dati personali ed ha una tutela indiretta attraverso strumenti rimediali generali dell'ordinamento[3].

---

right to one's personalità, A.G. Parisi, *E-contract e privacy*, Giappichelli, Torino, 2016, p. 14

[2] Questa distinzione è rinvenibile anche nei lavori preparatori della legge del Regno Unito in materia di trattamento dei dati, ovvero il *Data Protection Act*, *Data Protection Committee Report* (noto come *Lindop Report*), 1978, p. 156.

[3] Si consideri a titolo esemplificativo come negli Stati Uniti d'America sia pacificamente riconosciuta la sussistenza del diritto alla *privacy* pur non esistendo una disciplina in materia trattamento di dati. Solo il 28 giugno 2018 in California è stato adottato il "*California Consumer Privacy Act of 2018*" che disciplina il solo trattamento dei dati svolto da soggetti privati sui dati dei consumatori californiani.

3. L'applicazione territoriale del Regolamento UE n. 679/2016 e i servizi di *cloud computing*

Lo sviluppo delle nuove tecnologie e la crescente evoluzione di Internet, il cui obiettivo, come noto, è quello di migliorare la qualità della vita di milioni di individui, necessitava di un quadro normativo di riferimento univoco che recasse regole di trattamento dei dati adeguate all'evoluto scenario tecnologico.

È proprio in questo contesto storico che si inserisce il nuovo Regolamento (UE) n. 2016/679[4] recante il "Regolamento Generale sulla Protezione dei Dati personali" (di seguito anche "Regolamento" o "RGPD") che, su ispirazione della Direttiva 95/46/CE, cd. "Direttiva madre", si prepone lo scopo di innovare la disciplina in materia di trattamento dei dati personali a livello europeo.

Infatti, anche se risulta innegabile l'enorme potenzialità e semplificazione creata da Internet e in particolar modo da vari *social networks,* di non poco conto sono gli effetti collaterali talvolta connessi ad un loro distorto e/o inconsapevole utilizzo. Così, il Regolamento nasce con l'obiettivo di rafforzare e unificare la protezione dei dati all'interno del territorio dell'Unione Europea, affrontando e regolamentando il tema dell'esportazione dei dati al di fuori del territorio europeo con lo scopo di restituire a tutti i cittadini il controllo sui propri dati personali nonché semplificare il contesto normativo dell'Unione.

[4] Il Regolamento (UE) n. 2016/679 recante il "Regolamento Generale sulla Protezione dei Dati personali" o, in inglese, "*General Data Protection Regulation*", è stato approvato dal Consiglio d'Europa e dal Parlamento europeo il 27/04/2016 e divenuto direttamente applicabile a tutti gli Stati membri dell'UE il 25/05/2018. Tale Regolamento, congiuntamente alla Direttiva UE 2016/680 in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini, è parte del cosiddetto "*Pacchetto protezione dati*", nato con l'obiettivo di definire un nuovo quadro comune all'interno del territorio europeo in materia di tutela dei dati personali e favorire la circolazione sicura dei dati personali. Il complesso sistema normativo europeo ha provveduto così a sostituire la precedente Direttiva 95/46/CEE, posta a fondamento delle normative nazionali in materia di protezione dei dati, risultante ormai inadeguata agli obiettivi di uniformità europea a seguito di nuovi e sempre più tecnologici mezzi di comunicazione.

Riprova di quanto appena osservato è rinvenibile nell'ambito di applicazione territoriale del Regolamento[5], il quale si applica al trattamento di dati personali di interessati, persone fisiche, che si trovano nell'Unione, indipendentemente da dove si trovi il titolare o il responsabile del trattamento[6]. L'operatività della norma è condizionata al fatto che le attività di trattamento da parte di un titolare o di un responsabile del trattamento che non è stabilito nell'Unione[7], riguardino l'offerta di beni o la prestazione di servizi agli interessati o il monitoraggio del loro comportamento all'interno dell'UE. Ciò risponde all'esigenza di far fronte all'accresciuta incidenza dei flussi transfrontalieri dei dati personali, garantendo misure di sicurezza[8] affinché "*le persone fisiche abbiano il controllo dei dati personali che li riguardano e la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le Autorità pubbliche*"[9].

Ampliando conseguentemente l'ambito di applicazione della normativa europea, il Regolamento trova applicazione anche nei confronti del titolare e del responsabile del trattamento non stabilito nell'Unione, nell'eventualità in cui tali attività del trattamento riguardino l'offerta di beni o servizi[10]; così come nell'ipotesi dei contratti di *cloud computing*[11].

---

5 Il Regolamento dispone che le norme in esso contenute si applicano a tutti i trattamenti di dati personali, automatizzati o meno, contenuti in un archivio o destinati a figurarvi, purché non rientrino in uno dei casi eccettuati, nello specifico effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico5, e quindi senza una connessione con un'attività commerciale o professionale.

6 Cfr. art. 3 del Regolamento

7 Il legislatore europeo, recependo la nozione di stabilimento, afferma che la disciplina europea si applica a qualsiasi trattamento dei dati effettuato nell'ambito delle attività di uno stabilimento di un titolare o responsabile del trattamento, all'infuori dell'ipotesi che questo avvenga all'interno o all'esterno del territorio dell'Unione Europea.

8 Si veda a riguardo L. Bolognini, "*Il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali*", in L. Bolognini, C. Bistolfi (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016, p. 462, ove afferma che il nuovo Regolamento ha creato un sistema di garanzie e responsabilità a più livelli, mediante un regime di tutele definito come "*sticky regulation*", regime che resta "appiccicato" ai dati e non si esaurisce a seguito del primo trasferimento.

9 Cfr. considerando 7 del Regolamento

10 Cfr. considerando 23 del Regolamento

11 Per *cloud computing*, o nuvola informatica, così come precisato dal Working Party Art. 29 nella Opinion 5/2012 del 1 luglio 2012, WP n. 196, si intende: "*a set of technol-*

Il Regolamento, al fine di garantire uniformità alla normativa in materia di trattamento di dati personali, recepisce la nozione di "stabilimento" già precedentemente elaborata dalla Corte di Giustizia e dal *Data Protection Working Party* ex. Art 29 (di seguito anche "WP29") affermando che, ai sensi dell'art. 3, "il Regolamento si applica a qualsiasi trattamento di dati personali effettuato nell'ambito delle attività dello stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione" .

Il Regolamento consente dunque l'estensione della protezione dei dati personali a tutti coloro che si trovano nell'Unione Europea, indipendentemente dal luogo in cui è effettuato il trattamento dei dati personali, garantendo al contempo la tutela anche ai trattamenti effettuati da Titolari non stabiliti nell'Unione Europea se avrà ad oggetto dati personali di interessati che si trovano, anche "virtualmente", nell'Unione.

3.1 Il trattamento dei dati personali sulle piattaforme *cloud*

Il *cloud computing* rappresenta oggi una delle innovazioni tecnologiche più rilevanti in materia di conservazione, elaborazione e memorizzazione delle informazioni, contribuendo alla produzione sempre maggiore di dati personali che viaggiano nel ciberspazio[12].

L'utilizzo del *cloud computing* e i servizi da esso erogati, come ad esempio lo *storage*, che consente una memorizzazione di informazioni e l'accesso ai propri dati da postazioni potenzialmente indefinite, comporta inevitabilmente un trattamento di dati, il più delle volte di carattere personale.

In ambito nazionale l'Autorità Garante per la Protezione dei Dati Personali (di seguito anche "Garante Privacy") ha analizzato le problematiche e gli aspetti relativi alla protezione e al trattamento dei dati personali in un si-

---

ogies and service models that focus in the internet-based use and delivery of IT appilcations, processing capability, storage and memory space". *WP Opinion 05/2012 on Cloud Computing*, reperibile qui: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[12] Per una panoramica dei servizi sul cloud nella loro dimensione tecnica, economica e regolamentare si veda M. Franzosi, O. Pollicino e G. Campus (a cura di), "*Il digital single market e i cloud services*", Aracne, Roma, 2018

stema *cloud*, dettando accurate informazioni al fine di favorirne un consapevole utilizzo e affermando che "l'importante patrimonio informativo di dati personali necessita di una doverosa opera di informazione, con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi"[13].

In particolar modo deve essere garantito all'utente *cloud* il rispetto del principio di trasparenza, specificazione e limitazione delle finalità del trattamento e la cancellazione dei dati personali al termine del rapporto contrattuale.

Il principio di trasparenza[14] si traduce nel diritto del titolare a ricevere informazioni comprensibili, facilmente accessibili, chiare e trasparenti circa il suo rapporto con il fornitore, caratteristica dunque necessaria in un legittimo trattamento di dati personali.

Ma non solo, tale principio trova applicazione anche nella fase antecedente al trattamento dei dati personali, ovvero a quella dell'acquisizione del

---

[13] Così l'Autorità Garante per la protezione dei dati nella premessa della Scheda di documentazione del 23/06/2011 *"Cloud computing: indicazione per l'utilizzo consapevole dei servizi"*. In particolare, in riferimento a un utilizzo consapevole dei servizi afferma che l'utente *cloud* deve: *"*Ponderare prioritariamente rischi e benefici dei servizi offerti, effettuare una verifica in ordine all'affidabilità del fornitore, privilegiare i servizi che favoriscono la portabilità dei dati, assicurarsi la disponibilità dei dati in caso di necessità, selezionare i dati da inserire nella *cloud*, non perdere di vista i dati, informarsi su dove risiederanno, concretamente, i dati porre attenzione alle clausole contrattuali, verificare le politiche di persistenza dei dati legate alla loro conservazione, esigere e adottare opportune cautele per tutelare la confidenzialità dei dati e formare adeguatamente il personale".

[14] Il principio di trasparenza è stato ampliamente discusso dalla dottrina. Il principio di trasparenza, con riguardo all'accessibilità di documenti, dati e informazioni in possesso della pubblica amministrazione, ha conosciuto nel nostro ordinamento un'evoluzione del tutto peculiare, passando dal "*need to know*" dell'accesso documentale di cui alla legge n. 241/1990, al "*right to know*" dell'accesso civico di cui al decreto legislativo n. 33/2013, recante "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni". Si è assistito negli anni ad un ampliamento delle sue finalità, passando da una esclusiva tutela di situazioni giuridiche soggettive, alla più estesa funzione di garantire il controllo diffuso sul perseguimento dei compiti istituzionali e sull'utilizzo delle risorse pubbliche, al fine di tutelare i cittadini e promuovere la partecipazione democratica all'attività amministrativa. Si veda a riguardo G. Arena, "*Trasparenza amministrativa*", in S. Cassese (diretto da), *Dizionario di diritto pubblico*, Giuffrè, Milano, 2006; F. Pizzetti, "*Trasparenza e riservatezza nella pubblica amministrazione*", in F. Pizzetti - A. Rughetti (a cura di), *La riforma del lavoro pubblico*, Edk, Firenze, 2010 pp. 29 e ss.; E. Carloni, "*La 'casa di vetro' e le riforme. Modelli e paradossi della trasparenza amministrativa*", in *Diritto pubblico*, Il Mulino, Bologna, 2009, pp. 779 e ss.;

consenso[15]. L'utente *cloud* deve essere consapevole delle operazioni di trattamento che saranno effettuate sui propri dati e, in virtù di ciò, deve essere libero di prestare il proprio consenso.

Il principio di trasparenza deve essere inoltre garantito anche nel rapporto intercorrente tra cliente *cloud*, fornitore *cloud* ed eventuali subcontraenti, dovendo essere al cliente *cloud* specificata la presenza di eventuali parti che contribuiscono all'erogazione del servizio, nonché di tutti i *data center* ove viene effettuato il trattamento dei suoi dati personali.

Dall'analisi delle predette disposizioni emerge come anche nei servizi di *cloud computing*, in relazione alle attività svolte dal titolare del trattamento, di carattere personale o professionale, sono diversi gli oneri gravanti sui medesimi.

Mediante l'affidamento in *outsourcing* dei dati personali o aziendali, il *cloud provider* sarà infatti coinvolto in attività riguardanti il trattamento di dati[16].

Nelle ipotesi di utenti *cloud* professionali, una delle maggiori criticità riscontrabile nei contratti di *outsourcing* riguarda l'obbligo di controllo e di sorveglianza gravante in capo al titolare, il cui espletamento risulta complesso in virtù del processo di esternalizzazione delle attività di trattamento. Tale difficoltà risulta maggiormente evidenziata dallo squilibrio contrattuale esistente tra l'utente *cloud* e il fornitore del servizio. Il principio di responsabilizzazione, quale elemento fondante il Regolamento, prescrive in capo al titolare l'obbligo di effettuare delle valutazioni preventive sul livello di protezione e i servizi offerti dal *cloud*.

Preminente è, da parte del titolare, un'analisi delle risorse informatiche impiegate e l'eventuale possesso, da parte del *cloud*, di eventuali certificazioni idonee ad assicurarne l'affidabilità. Inoltre, è necessaria la conoscenza dell'ubicazione territoriale delle infrastrutture fornite dal *cloud*. A riguardo infatti, potrebbero sorgere rilevanti implicazioni giuridiche in relazione alla protezione dei dati personali.

Nell'ipotesi in cui i server del *cloud* si trovino in Paesi terzi, è necessario che il titolare del trattamento effettui una valutazione di adeguatezza del livello di tutela equivalente alla normativa comunitaria. Inoltre, i servizi *cloud*

[15] Per il principio di trasparenza si veda il considerando n. 39 del Regolamento

[16] Sul punto E. Belisario, *"Diritto sulle nuvole – profili giuridici del cloud computing"*, in *Altalex eBook "Informatica Giuridica"*, 2011, p. 21

possono coinvolgere un'ulteriore serie di parti contraenti che ricoprono il ruolo di responsabili del trattamento, mediante un atto di disegnazione che prende il nome di contratto di esternalizzazione, il cui contenuto è delineato all'art. 28 del Regolamento, un contratto atipico in cui il titolare affida in capo a un terzo la gestione di alcuni servizi della sua impresa o attività, pur mantenendo autonomia nella determinazione dei mezzi e delle finalità[17].

Il responsabile deve garantire al titolare di poter esercitare tempestivamente l'obbligo di segnalazione di *data breach*. Il termine di settantadue ore si verifica nel momento in cui il titolare viene a conoscenza della perdita o alterazione dei dati, dovendo però essere sempre in grado di controllare costantemente gli strumenti per la conservazione dei dati, così da poter individuare la loro eventuale perdita o modificazione.

Il Regolamento tuttavia prevede che, a loro volta, i responsabili del trattamento possono designare dei sub-responsabili, i quali avranno accesso ai dati archiviati sulla "*nuvola*". In tale caso si riversa sui responsabili del trattamento l'onere di informare il titolare circa l'eventuale sub-appalto, descrivendo analiticamente il servizio subappaltato, le specifiche caratteristiche dei subcontraenti attuali o potenziali e le garanzie offerte da quest'ultime al *provider*[18].

È facile comprendere come la necessità di conoscere dove, come e a quali condizioni viene offerta la gestione dei propri dati, sia di importanza preminente, al fine di contenere i rischi e mantenere il controllo sui propri dati.

La legittimità al trattamento dei dati in un sistema *cloud* è dunque soggetto al rispetto della normativa in materia di trattamento di dati personali conformemente al Regolamento.

Relativamente al principio di specificazione e limitazione delle finalità, la disciplina europea afferma che i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità, nonché conservati limitatamente al perse-

[17] Si veda a riguardo L. Greco, "*I ruoli: titolari e responsabili*", in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati*, op. cit., p. 274

[18] Analisi effettuata dal *Working Party* ex. art. 29 nel Parere 05/2012 sul *Cloud Computing*, n. 196
http://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

guimento delle finalità per le quali sono trattati, anche previa fissazione di un termine per la definitiva eliminazione o eventuale modifica[19].

La nuova normativa europea a riguardo specifica che il fornitore del servizio *cloud*, qualora determini finalità e mezzi del trattamento[20], deve fornire all'interessato, le informazioni ai sensi degli artt. 13 e 14, e specificatamente: "*la sua identità, i suoi dati di contatto e di quelli del responsabile della protezione dei dati, nelle ipotesi in cui tale figura risulti necessaria, le finalità e la base giuridica del trattamento e, qualora il trattamento trovi il suo fondamento nel legittimo interesse, devono essere specificati i legittimi interessi perseguiti dal titolare del trattamento o da terzi, gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma[21], il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili*"[22].

Inoltre, sempre secondo le disposizioni dell'art. 13, qualora nel tempo si modifichino o vengano ad aggiungersi ulteriori finalità del trattamento, sarà onere del titolare informarne prontamente l'interessato e chiederne il consenso. Dunque, nel caso in cui debba essere effettuato un trattamento cd. secondario, in assenza del consenso dell'interessato o di un atto legislativo che disponga la liceità del trattamento, il titolare è tenuto a valutare la sussistenza dei principi di proporzionalità e necessità ai sensi dell'art. 23 del Regolamento[23], in relazione agli scopi del trattamento principale.

---

[19] In riferimento si rinvia ulteriormente al considerando n. 39 del Regolamento

[20] Art. 28 par. 10 del Regolamento: "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".

[21] Gli articoli ad oggetto indicano ipotesi in cui il trasferimento è soggetto ad adeguate garanzie, sono presenti norme vincolanti d'impresa o vi è la presenza di deroghe in specifiche situazioni e in particolare: il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato.

[22] Cosi l'art. 13 del Regolamento

[23] Sul punto si veda il considerando n. 50 del Regolamento

Per ciò che concerne la liceità del trattamento dei dati, ai sensi dell'art. 6 del Regolamento, il trattamento è lecito oltre nell'ipotesi in cui l'interessato abbia prestato il proprio consenso, anche quando ricorra una delle seguenti condizioni: l'esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su richiesta dello stesso, l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento, la salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che questo non prevalga sugli interessi, sui diritti o sulle libertà fondamentali dell'interessato che richiedano la protezione dei dati personali.

Qualora i dati non siano ottenuti presso l'interessato ma presso terzi, ai sensi dell'art. 14 rubricato "*Informazioni da fornire qualora i dati non siano ottenuti presso l'interessato*", il titolare deve fornire all'interessato le informazioni precedentemente specificate.

Nell'ipotesi di memorizzazione dei dati su piattaforme *cloud* diviene inoltre difficile assicurare la riservatezza di tali dati in virtù della loro libera circolazione su Internet. Incombe dunque sull'utente *cloud* l'onere di assicurarsi l'effettiva collocazione del *server* del fornitore, prestando particolare attenzione a quelle clausole contrattuali che eventualmente permettano un trasferimento, anche transfrontaliero, di determinati dati personali.

Può avvenire infatti che, specie nel caso di fornitori di servizi *cloud* di grandi dimensioni, la nuvola si estenda geograficamente su vasti territori e che i dati siano conservati in più siti.

3.2 La protezione dei dati personali sulle nuvole informatiche

Il Regolamento pone alla base del trattamento e della protezione dei dati personali l'estensione del principio di prevenzione e di precauzione[24].

[24] Sulla differenza tra le nozioni di prevenzione e precauzione si rinvia a M.G. Stanzione, "*Principio di precauzione, responsabilità civile e diritto alla salute. Profili di diritto comparato*", in *Comparazione e diritto civile*, 2010, pp. 1-3

La tutela preventiva intesa come la possibilità di vagliare i rischi sottesi al trattamento dei dati personali prevede, come già analizzato precedentemente, l'analisi e la valutazione d'impatto quale tecnica a tutela della protezione dei dati, nonché l'obbligo di protezione dei dati per impostazione fin dalla progettazione cd. *privacy by design*, e la protezione dei dati per impostazione predefinita, cd. *privacy by default*[25]. Inoltre, il principio di minimizzazione dei dati riflette l'intento del legislatore di rendere più rigorosa la tutela, richiedendo che essi siano pertinenti adeguati e limitati alle finalità per i quali sono stati raccolti.

L'impostazione preventiva risultante dall'analisi della normativa ad oggetto, risponde così all'esigenza precauzionale di limitazione dei rischi per i diritti e le libertà delle persone interessate.

Tuttavia la prospettiva internazionale della nozione di dato destinato alla libera circolazione[26] trova un'ineluttabile riferimento anche all'interno del Regolamento, all'interno del quale permane sempre vivo il binomio circolazione-protezione dei dati[27]. È infatti proprio in relazione a tale contesto che sorgono le limitazioni nel trattamento dei dati personali.

La normativa europea infatti ha perseguito lo scopo di rafforzare l'effettiva tutela dei dati delle persone fisiche presenti nel territorio dell'Unione, riproponendo il principio di extraterritorialità in relazione al trattamento dei dati effettuato nell'attività di uno stabilimento del titolare o del responsabile del trattamento operante nel territorio europeo.

Necessaria è tuttavia una maggior adeguatezza e l'innalzamento dei livelli di tutela che devono essere garantiti in un eventuale trasferimento di dati verso paesi terzi, perseguendo nel contempo un equilibrio tra i diversi approcci normativi verso il diritto alla privacy[28].

---

[25] Si veda a riguardo A. Principato, "*Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*", in *Contratto e impresa,* Europa (1), 2015, pp. 197-229.

[26] In riferimento alla libera circolazione dei dati personali si voglia leggere il considerando n. 8 del Regolamento

[27] Sull'analisi della funzione protettiva e circolativa del binomio circolazione-protezione si veda J. Litman, "*Information Privacy/Information Property*, in *Stan. L. Rev*., 52, 2000, p.1283; S. Rodotà, *Tecnopolitica*, op. cit., pp. 155 e ss.

[28] Il problema di sovranità e di regolamentazione del trattamento dei dati in diversi approcci regolatori è stato analizzato da V. Zeno-Zencovich, "*Intorno alla decisione nel caso Schrems: La sovranità digitale e il governo internazionale delle reti di telecomuni-*

L'enorme produzione di dati e la loro memorizzazione sulle nuvole informatiche in relazione alle potenzialità delle nuove tecnologie, presuppone l'accertamento di determinati livelli di sicurezza da parte del titolare.

I dati personali o aziendali, all'interno di sistemi di *cloud computing*, non sempre godono di quella tutela minima volta a limitare le conseguenze derivanti da possibili perdite o distruzioni dei dati allocati sui vari server. Il *cloud* service provider infatti non sempre è in grado di garantire le misure tecniche e organizzative a tutela della riservatezza, sicurezza, integrità e disponibilità dei dati, molto speso affidati a data center esterni.

L'utilizzo di sistemi di *cloud computing* necessita così l'esame di alcune peculiarità proprie delle "nuvole informatiche". In particolar modo tra i maggior rischi relativi alla protezione dei dati vi è la diminuzione del controllo del titolare sui propri dati, un aumento di condivisione dei propri dati, in virtù delle caratteristiche strutturali tipiche del *cloud*, ed un esponenziale utilizzo delle reti pubbliche per l'accesso alle risorse remote .

Individuato il tipo di relazione intercorrente tra utente *cloud* e *provider*, i quali ricoprono soventemente la figura di titolare e responsabile del trattamento, palesemente ricade sull'utente *cloud*, in qualità di titolare del trattamento, l'onere di analizzare gli aspetti e le misure minime di sicurezza offerte dal *cloud service provider*.

In particolar modo ricade sull'utente *cloud* l'obbligo di assicurarsi, mediante una verifica preventiva, di possedere un effettivo controllo sui dati e di assicurarsi il rispetto delle misure minime tecniche e di sicurezza offerte dal provider.

La verifica preliminare ovviamente può consistere in un'analisi e in una comparazione delle varie offerte proposte dai vari *cloud providers*, ma senz'altro da considerare nel corso della verifica preliminare è il rispetto, da parte di quest'ultimo, del possesso di idonei standard relativi alla sicurezza e

---

cazione, in *Diritto dell'informazione e dell'informatica,* 4/5, 2015, p. 683; F. Bignami - G. Resta, "*Transatlantic Privacy Regulation: Conflict and Cooperation*", in *Law &Contemp. Probs*., 78, 2015, p. 231

alla gestione dei dati e delle informazioni mediante certificazioni, in particolare la c.d. ISO/IEC 27001[29] e ISO/IEC 27002[30] .

Il possesso di tali certificazioni tuttavia, qualora non venga espressamente menzionato all'interno del contratto stipulato dalle parti, non può essere considerato un parametro di adempimento o non adempimento del *cloud provider* in relazione alle misure minime di integrità e sicurezza. Conseguenza è dunque che l'utente *cloud*, al momento della stipula, dovrà attenersi al parametro di diligenza professionale offerto dagli operatori del settore. In tal caso solamente il mancato rispetto degli standard previamente pattuiti potrà assumere rilevanza giuridica.

4. I presupposti di legittimità al trasferimento dei dati personali

Il capo V del Regolamento, rubricato come "*Trasferimento dei dati personali verso Paesi Terzi e Organizzazioni Internazionali*", è dedicato interamente alla disciplina dei flussi transfrontalieri dei dati personali e, conseguentemente, anche all'utilizzo dei servizi di *cloud computing*.

Sebbene manchi a livello giuridico una definizione precisa di trasferimento dei dati, non rinvenibile neanche nella Direttiva madre 95/46/CE, fondamentale è stata la giurisprudenza della Corte di Giustizia dell'Unione europea, la quale ha affermato che: "*Non si configura un trasferimento verso un paese terzo di dati ai sensi dell'art. 25 della direttiva 95/46 allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet -*

[29] Per un'analisi sui rischi relativi ai sistemi di *cloud computing* si rinvia a G. Troiano, *"La conservazione dei documenti in cloud computing", in Ciberspazio e diritto*, 2013, Vol. 14, n. 48, pp. 269 e ss.

[30] Lo standard ISO/IEC 27001 è una norma internazionale emanata dall' International Organization for Standardization (ISO) in cooperazione con l'*International Electrotechnical Commission* (IEC), che definisce i requisiti per un SGSI (Sistema di Gestione della Sicurezza delle Informazioni), con l'obiettivo principale di stabilire un sistema per la gestione del rischio e protezione delle informazioni e degli *asset* ICT. In particolar modo la ISO/IEC 27001 "specifica i requisiti per impostare, mettere in opera, utilizzare, monitorare, rivedere, manutenere e migliorare un sistema documentato all'interno di un contesto di rischi legati alle attività centrali dell'organizzazione". https://www.iso.org/isoiec-27001-information-security.html

caricata presso una persona fisica o giuridica che ospita (web hosting provider) il sito Internet nel quale la pagina può essere consultata e che è stabilita nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi"[31].

L'art. 44 del Regolamento definisce il trasferimento dei dati personali chiarendo che non è necessario che i dati soggetti a trasferimento siano sottoposti immediatamente a un trattamento, bensì è sufficiente che siano "*destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale* "[32].

La necessità di regolamentazione dei flussi transfrontalieri dei dati risponde tuttavia al principio di libera circolazione dei dati, nonché al costante supporto allo sviluppo dell'economia e del mercato.

In tal senso il considerando n. 101 del Regolamento afferma che: "*I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale*".

---

[31] Pronuncia della Corte di Giustizia nel procedimento penale a carico di *Bodil Lindqvist*, 6 novembre 2003, consultabile qui: https://eurlex.europa.eu/legalcontent/IT/ALL/?uri= CELEX%3A62001CJ0101; la soluzione a tale pronuncia consisterebbe nell'esonero di responsabilità per i responsabili del trattamento. Infatti, se la pubblicazione su una pagina web dovesse essere considerata come trasferimento, si dovrebbe applicare la normativa europea a tutti i Paesi dai quali è possibile accedere a quella pagina web. Sul punto P. Piroddi - Y. Poullet, "*Transborder Data Flows and Extraterritoriality: The European Position*", in *Journ. Intern. Comm. Law &Techn*., 2007; D. Pittella, "*Trasferimento verso paesi terzi*", in *La nuova disciplina europea della privacy*, op. cit. pp. 259-261

[32] Tale definizione nasce dalla consapevolezza del legislatore europeo di sottolineare la differenza tra "*comunicazione*" e "*trasferimento*", così come affermato in dottrina, ove viene enunciato che: "*Il trasferimento non è sinonimo di 'comunicazione' anche se le sue operazioni distinte possono, in taluni casi, sovrapporsi*". R. Imperiali - R. Imperiali, *Il trasferimento all'estero dei dati personali*, Il Sole 24 Ore, Milano, 2003, p. 8; M. Bellabarba, "*Trasferimento all'estero dei dati personali*", in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, p. 1755

La progressiva diffusione del fenomeno delle *Information and Communications Technology* ha permesso una maggiore produzione di dati[33], da cui ne è derivato un scambio sempre maggiore non solo dovuto alla delocalizzazione dei sistemi informatici utilizzati, ma anche per evidenti ragioni di sicurezza, come ad esempio per la duplicazione dei dati al fine di arginare i problemi derivanti da una possibile perdita o distruzione degli stessi, così come accade nei servizi di *cloud computing*, servizi che notevolmente influenzano la produttività dei lavoratori e delle aziende.

Da ciò ne deriva che lo scambio dei dati transfrontaliero non può essere evitato.

La delocalizzazione transfrontaliera dei dati personali e aziendali è una delle problematiche di maggior rilievo nell'utilizzo di servizi *cloud* da parte di titolari del trattamento soggetti al Regolamento. I servizi di *cloud computing* si caratterizzano infatti per la loro naturale erogazione dei propri servizi a prescindere dal territorio in cui è ubicato il *provider*, così da trasformarsi in un fenomeno di dimensioni globali. È noto che molti *cloud service provider* si avvalgono dell'utilizzo di *providers* esterni collocati in diversi paesi al fine di contenere i costi.

Il flusso di tali dati personali viaggia da Paesi più industrializzati a Paesi meno industrializzati, così da introdurre aspetti di internazionalità nel rapporto tra *cloud provider* e utente utilizzatore del *cloud,* nonché da offrire di conseguenza diversi livelli di sicurezza nel trattamento dei dati.

La possibilità di operare in mercati transnazionali necessita tuttavia della definizione di regole giuridiche comuni, applicabili a tutti gli utenti *cloud*, non essendo ipotizzabile che i *providers* capitalizzino ulteriori costi per sostenere le differenti condizioni derivanti dalle diverse nazionalità degli utenti[34].

La necessità dunque di definire un quadro normativo utile a regolamentare il trattamento dei dati mediante i servizi di *cloud computing* esula dalle regole civilistiche, rientrando invece in quei diritti propri della persona, ove

[33] Cfr. considerando n. 5 del Regolamento

[34] Sul punto D. Mula, "*Il trattamento dei dati nel territorio dell'Unione e il meccanismo "*one stop shop*",* in *La nuova disciplina europea della Privacy*, op. cit., p. 274

la forza contrattuale delle parti risulta inidonea a garantirne la tutela, specie in riferimento alla privacy.

Accade frequentemente infatti che il fornitore del servizio *cloud*, ad esempio nelle ipotesi di mancanza di capacità di *storage*, si avvalga della memoria di altri *providers* terzi, creando una frammentazione di dati che viaggiano da un *provider* ad un altro, senza tenere conto che, nelle ipotesi di memorizzazione di dati aziendali, è necessario effettuare il *back-up* delle informazioni e delle copie, con la conseguenza che esistono più copie di ogni singolo dato potenzialmente collocabili in diversi paesi o *data center*[35].

L'utilizzo di servizi *cloud* che comportano così lo svolgimento di attività al di fuori dei confini dello Stato pone una serie di problematiche.

Il Regolamento, a tutela dei dati personali delle persone fisiche, subordina alla presenza di determinate condizioni, il trasferimento verso Paesi Terzi o Organizzazioni Internazionali.

Tra gli strumenti giuridici validi per il trasferimento transfrontaliero dei dati vi sono le "*Model contract clauses*" e le "*Binding Corporate Rules*"[36].

Le *Model contract clauses*[37], ovvero le clausole contrattuali standard, sono "clausole-tipo" adottate dalla Commissione europea a seguito di quattro

[35] Si tenga in considerazione anche l'ipotesi in cui, nel caso di *SaaS*, venga offerto da una società ICT un software in modalità *cloud* ad un'azienda, tale da creare un'aggregazione di servizi acquisiti dalla prima ma comunemente offerti, creando una pluralità di relazioni contrattuali con conseguente trasferimento dei dati fra più soggetti. A riguardo A. Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, op. cit., pp. 687-688

[36] Sul punto G.M. Riccio Giovanni Maria, ***"Model contract clauses" e "corporate binding rules": valide alternative al "Safe Harbor Agreement"?*** *Nota a CGUE Grande sezione 6 ottobre 2015 (causa C-362/14)*, in *Il Diritto dell'informazione e dell'informatica,* **2015**, fasc. 4-5, pp. 865-885.

[37] La previsione di clausole contrattuali standard da parte della Commissione Europea, in un'ottica comparatistica, appare contrapporsi alla metodologia contrattuale dei sistemi giuridici appartenenti all'area di *civil law*, ove l'elemento volontaristico si manifesta predominante e la sostituzione della volontà privata è concessa solo in via meramente eccezionale. Pertanto, sebbene vi sia questo discostamento tra ordinamenti di *common law* e di *civil law*, l'influenza di pratiche e di esperienze appartenenti all'area del diritto angloamericano ha permesso al legislatore di fissare i termini del regolamento contrattuale. Si veda a riguardo G. Mirabelli, "*Dei contratti in generale*", in *Comm. Cod. civ*., IV, tomo II, Torino, 1958, p. 87; per un'analisi sugli ordinamenti di *common law* e *civil law* cfr. P. Durand, *La Tendence à la Stabilitè du Rapport Contractuel*, Parigi, 1960, pp.

diverse decisioni in conformità all'art. 26 della Direttiva 95/46/CE, il cui inserimento all'interno di un contratto assicura che il trattamento dei dati nel Paese terzo avvenga in conformità dei principi della Direttiva[38].

I rapporti tra il titolare e il responsabile nella figura di *cloud provider* sono regolati da un contratto di servizio, volto a disciplinare non solo le relazioni economiche ma, *in primis*, la disciplina legata al trattamento dei dati. In relazione alla struttura tipica dei *server cloud*, la cui infrastruttura è talvolta distribuita in diverse aree geografiche, necessita una valutazione preventiva del titolare circa l'effettiva localizzazione dei servizi richiesti. Pertanto, uno degli strumenti maggiormente utilizzati nei servizi di *cloud computing,* sono le clausole contrattuali standard[39], inserite nei contratti tra titolare e *cloud server* come base legale per legittimare il trasferimento dei dati.

Le clausole contrattuali standard rappresentano uno strumento giuridico di integrazione[40] e "*sicuro*", in quanto il loro inserimento all'interno di un contratto legittima il trasferimento dei dati verso Paesi terzi che non godono di accordi di adeguatezza, determinando però di conseguenza l'aumento di

---

10 e ss., e D. Harris – D. Tallon, *Contract Law Today: Anglo-French Comparisons*, Clarendon Press, Oxford, 1989, *passim*, e ancora J. Gordley, *The Philosophical Origins of Modern Contract*, Clarendon Press, Oxford, 1991, pp. 1 e ss.

[38] Si tratta della cd. Decisione Commissione, Clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95/46/CE del 5 febbraio 2010; della Decisione della Commissione per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi del 27 dicembre 2004; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE del 5 giugno 2001; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati personali a incaricati del trattamento residenti in paesi terzi, dir. 95/46/CE del 27 dicembre 2001.

[39] Le clausole contrattuali standard rappresentano uno strumento negoziale sottoscritto dalle parti contraenti tra cui avviene il flusso dei dati mediante il quale le parti si impegnano a rispettare un determinato livello di protezione.

[40] Le clausole contrattuali standard sono un forte esempio di integrazione contrattuale, operanti non solo in caso di lacune normative ma agiscono quali forme di integrazione alla volontà contrattuale infatti, come osserva Stefano Rodotà: "*Il problema dell'integrazione non è strettamente condizionato dall'esistenza di lacune. In altri termini, non è soltanto nei casi di oggettiva inidoneità ad operare del regolamento predisposto dalle parti che può aver luogo il ricorso agli strumenti integrativi*". Per un'analisi sul tema si rinvia a S. Rodotà, *Le fonti di integrazione del contratto*, Giuffrè, Milano, 2004, p.8

costi transattivi, dovuti alla vasta gamma di obblighi e responsabilità gravanti sull'importatore[41].

Le *Binding Corporate Rules* rappresentano le cd. "*norme vincolanti d'impresa*", le quali consentono il trasferimento dei dati nell'ambito del medesimo gruppo imprenditoriale o il medesimo gruppo di imprese. Sono dunque il complesso di tutte le norme tecniche nonché delle *policy* aziendali, adottate dalle società dello stesso gruppo per il trattamento dei dati personali[42].

Le norme vincolanti d'impresa necessitano tuttavia dell'approvazione dell'autorità di controllo competente che, in assenza del consenso del soggetto interessato, deve legittimare il trasferimento, ma è necessario che siano vincolanti per tutto il gruppo imprenditoriale, compresi i dipendenti; e che sia consentito ai soggetti interessati di azionare i propri diritti e, infine, applicare i principi del Regolamento conformemente all'art. 47 par. 2[43]. Il Regolamento inoltre pre-

---

[41] Sul punto si veda F. Piraino, "*Il codice della privacy e la tecnica del bilanciamento di interessi*", in R. Panetta (a cura di) *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, 709 e ss.

[42] Il *Working Party* art. 29 ha pubblicato copiosi documenti per fissare le linee guida da seguire nella redazione delle norme vincolanti al fine di aiutare e sensibilizzare le imprese. I documenti sono i seguenti: WP 107: *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules*"; WP 108: *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*; WP 133: *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*; WP 153: *Working Document setting a table with the elements and principles to be found in Binding Corporate Rules*; WP 154: *Working Document Setting up a framework for the structure of Binding Corporate Rule*s; WP 155: *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rule*s.

[43] Nello specifico le norme vincolanti d'impresa devono integrare i seguenti requisiti: "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; i 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; la loro natura giuridicamente vincolante; l'applicazione dei principi generali di protezione dei dati; i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli; 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; le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa; i compiti di qualunque responsabile della protezione dei dati; le procedure di reclamo; i meccanismi all' interno del gruppo im-

dispone ulteriori alternative che operano nel momento in cui non è possibile legittimare il trasferimento dei dati sulla base di una decisione di adeguatezza. La prima garanzia indicata dal Regolamento, prevista al secondo comma dell'art. 46, consiste in "*uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici*"[44]. Per essere validi questi accordi non devono però incidere sulle disposizioni in materia di trattamento dei dati risultanti dal Regolamento o qualsiasi altro diritto dell'Unione Europea, e devono includere un adeguato livello di protezione dei diritti fondamentali dei soggetti interessati[45]. Un'ulteriore ipotesi di garanzia in ipotesi di trasferimento di dati tra autorità pubbliche, che necessita però dell'autorizzazione da parte di un'Autorità di controllo, sono le "*disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati*", basando così il trasferimento su disposizioni *ad hoc* inserite in accordi amministrativi.

In ultimo, ai sensi del secondo comma dell'art. 47 può essere considerata una garanzia adeguata, senza la necessità di autorizzazione dell'Autorità di controllo, "*un codice di condotta approvato a norma dell'art. 40*", purché "integrato da un "*impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate*, così come può essere considerata una garanzia adeguata "*un meccanismo di certificazione approvato a norma dell'art. 42*".

4.1 Il trasferimento dei dati verso gli Stati Uniti

Il modello statunitense in materia di trattamento dei dati infatti, significativamente diverso da quello europeo, si caratterizza per l'assenza di una regola-

---

prenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa; i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo; il meccanismo di cooperazione con l'autorità di controllo; i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale; l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali".

[44] Cfr. considerando n. 108 del Regolamento

[45] Cfr. considerando n. 102 del Regolamento

mentazione unitaria in materia di *data protection,* a causa della presenza di copiosi interventi settoriali di matrice federale, statale e autoregolamentare[46] e a fronte dell'indiscusso riconoscimento giurisprudenziale del diritto alla privacy.

Il primo importante intervento legislativo in materia di trasferimento e circolazione dei dati transfrontaliero fu definito nel 1980 dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), con la raccomandazione del Consiglio d'Europa, la quale forniva, mediante linee-guida, una regolamentazione in materia di "*Protection of Privacy and Transborder Flows of Personal Data*"[47], nella quale si invitavano gli Stati membri ad adottare tutte le misure di sicurezza adeguate volte a garantire un corretto e lecito flusso transfrontaliero dei dati, conformemente alle normative nazionali in vigore.

Successivamente all'adozione della raccomandazione, a livello europeo il Consiglio d'Europa approvò nel 1981 la più volte citata Convenzione n. 108, o di Strasburgo, sulla protezione degli individui con riguardo al trattamento automatico di dati personali[48].

I sopraesposti interventi normativi hanno costruito così il terreno all'interno del quale è maturato tutto il sistema di principi che ha dato poi origine alla Direttiva 95/46/CE la quale, con riguardo ai trattamenti tran-

[46] Si veda a riguardo S. Sica – V. D'Antonio, "*Verso il Privacy Shield: il tramonto dei Safe Harbor Privacy Principles*", in G. Resta – V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali: Dai Safe Harbor Principles al Privacy Shield*, op. cit., pp. 137 e ss.

[47] Con lo sviluppo delle tecnologie informatiche in vaste arie della vita economica e sociale, nel 1980, l'OECD ha adottato le linee guida, "Linee guida del 1980", con l'obiettivo di regolamentare il copioso flusso di dati personali e tutelare al contempo la riservatezza, per affrontare i problemi derivanti dal sempre maggiore uso di dati personali ed evitare rischi per le economie globali risultanti da eventuali restrizioni al trasferimento di informazioni oltre i confini. Le linee guida del 1980, contenenti il primo insieme di principi generali sulla privacy, hanno così influenzato la legislazione e la politica degli stati membri dell'OECD e a livello internazionale. Nel 2013 il documento è stato oggetto di revisione, la quale ha comportato l'introduzione di nuovi concetti quali: strategie nazionali sulla privacy, programmi di gestione della privacy e la notificazione delle violazioni dei dati. OECD *Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) as amended on 11 July 2013* https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[48] *Council of Europe, Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, 28 gennaio 1981, *European Treaty Series* - No. 108. https://rm.coe.int/1680078b37

sfrontalieri di dati, detta il principio generale per il quale è consentito il trasferimento solamente se il Paese terzo garantisce un "*adeguato livello di protezione*"[49].

In tal senso, se un Paese terzo presenta un grado di protezione adeguato "*ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona*"[50], la Commissione può adottare una decisione volta a "*certificare*" l'adeguatezza della tutela dei dati personali fornita da quell'ordinamento extraeuropeo[51].

Al contrario, qualora i paesi extraeuropei non siano in grado di fornire adeguati livelli di tutela, la Commissione avvia trattative con il Paese terzo in questione all'esito delle quali valutarne il livello di tutela offerto, sulla base degli impegni assunti, della legislazione nazionale o degli impegni internazionali del Paese extraeuropeo così da emettere, in caso favorevole, una decisione favorevole o meno alla circolazione transfrontaliera.

A seguito di numerosi negoziati tra *US Department of Commerce* e la Commissione Europea, la necessità di definire un quadro normativo di principi ha portato poi all'adozione, il 26 luglio del 2000, dell'accordo tra Europa e Stati Uniti denominato "*Safe Harbor*"[52], cd. "*porto sicuro*", con l'obiettivo di garantire un'equivalente livello protezione nel trattamento dei dati oltreoceano.

---

[49] Così l'art. 25 e il considerando n. 75 della Direttiva 95/46/CE

[50] Così l'art. 25 paragrafo 6 della Direttiva 95/46/CE

[51] Nello specifico il parametro di adeguatezza, così come stabilito dai giudici della Grande sezione della Corte di Giustizia dell'Unione Europea nella Sentenza 6 ottobre 2015 – *Causa C-362/14 Schrems*: "Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione del livello di protezione ad essi accordato in ciascuno di tali paesi, l'articolo 25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata […], vuoi dagli Stati membri vuoi dalla Commissione". https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN
Sul punto si veda anche S. Sica – V. D'Antonio, *Verso il Privacy Shield: il tramonto dei Safe Harbor Privacy Principles*, op. cit. p 141-142

[52] L'accordo *Safe Harbor* trova il suo fondamento giuridico nella Direttiva 95/46/CE la quale, all'art. 25 par. 1 impone che il paese terzo verso il quale avvenga il trasferimento dei dati fornisca un adeguato livello di protezione. La scelta dell'Unione europea è stata quella di imporre a chiunque esportasse dati di origine comunitaria di conformarsi al dettato normativo europeo, garantendo così che i dati in transito godessero di specifici livelli di tutela, modellati sulla base della Direttiva 95/46/CE. Sul punto. A. Mantelero, "*Data*

Con l'adozione del *Safe Harbor*[53] venne così creato uno strumento volto a favorire lo scambio delle informazioni nonché le relazioni commerciali tra l'Europa e le organizzazioni americane. Successivamente all'adozione del *Safe Harbor* la Commissione Europea, in data 1 novembre 2000, ha formalmente approvato i "*Safe Harbor Privacy Principles*"[54].

L'adesione dunque ai Principi del *Safe Harbor* permetteva alle organizzazioni statunitensi di omologarsi alla decisione di adeguatezza della Commissione Europea, così da non veder bloccato il proprio trasferimento di dati oltreoceano, creando un "*ponte*" di contatto fra le diverse normative[55].

Protection ed attività di impresa. Verso dove guardano gli USA?", in *Diritto dell'informazione e dell'informatica*, 2011, pp. 457 e ss., ove sottolinea come il modello comunitario "*grazie ad un'acuta scelta di strategia normativa, sia stato esportato al di fuori dei confini dell'Unione, adottato o usato come esempio per legislazioni di diverse nazioni, ed è divenuto in ogni caso parametro necessario di confronto*".

[53] L'accordo *Safe Harbor* è costituito dai "*Safe Harbor Privacy Principles"* formalmente approvati dalla Commissione Europea il 1 novembre 2000, e dalle "*Frequently Asked Questions*" o "FAQ", contenenti commenti elaborati dall'*US Department of Commerce,* con l'obiettivo di fornire maggiori informazioni circa il significato dei Principi, riassumendo inoltre gli impegni assunti dalle imprese aderenti all'accordo ed un memorandum sulle azioni risarcitorie messe a disposizione degli individui.

[54] I *Safe Harbor Privacy Principles* contengono una serie di Principi ispirati alla Direttiva 95/46/CE. I principi contenuti nell'accordo sono sette: a) *Principle of Notice*: Gli interessati devono essere informati dall'impresa circa gli scopi per i quali i loro dati verranno raccolti e le modalità del trattamento. Inoltre l'impresa deve fornire in "*a clear and conspicious language*" tutte le informazioni necessarie per presentare un ricorso e i soggetti terzi ai quali i dati potranno essere comunicati; b) *Principle of Choice*: Gli individui devono avere la possibilità di rifiutare la raccolta e inoltrare il trasferimento dei dati a terzi; c) *Principle of Onward Transfer*: I trasferimenti di dati a terzi possono avvenire solo ad altre organizzazioni che seguono adeguati principi di protezione dei dati; d) *Principle of Security*: l'impresa deve porre in essere il massimo impegno al fine di prevenire eventuali perdite di informazioni raccolte; e) *Principle of Data Integrity*: i dati devono essere pertinenti e affidabili per lo scopo in cui sono stati raccolti; f) *Principle of Access*: Gli individui devono essere in grado di accedere alle informazioni detenute su di loro e, se inaccurati, correggerli o eliminarli; g) *Principle of Enforcment*: L'impresa deve possedere mezzi idonei atti a far rispettare tali regole. Così *European Court of Justice Commission Decision 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*,25/08/2000 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

[55] Si veda a riguardo S. J. Kobrin, "*Safe harbors are Hard to Find: the Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*", in *Review of International Studies*, Volume 30, Issue 1, January 2004, pp. 111-131

Tuttavia, il ponte di contatto creato con l'accordo *Safe Harbor* tra Europa e Stati Uniti venne ben presto a scontrarsi con diverse problematiche applicative. Infatti, la portata normativa dei *Safe Harbor Principles* era soggetta a determinati limiti di natura oggettiva. La partecipazione al sistema di principi, fondato anzitutto su base volontaria e sul principio di "*self certification scheme*"[56], non si estendeva a specifici settori economici che trattano una vasta quantità di dati personali, quali ad esempio, il settore delle assicurazioni, istituzioni finanziarie o delle telecomunicazioni[57], ma solamente a quelle imprese americane operanti nei settori sottoposti al controllo dell'autorità del

[56] Il meccanismo di autocertificazione prevede che gli operatori statunitensi presentino al *Department of Commerce* l'adesione ai Principi *Safe Harbor*, godendo così di una presunzione di adeguatezza di tutela per poter procedere all'importazione dei dati nel territorio europeo. Così FAQ 6 – *Self Certification* del *Safe Harbor*, per cui: "*Safe Harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below. To self-certify for the safe harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the safe harbor, that contains at least the following information: 1. name of organization, mailing address, e-mail address, telephone and fax numbers; 2. description of the activities of the organization with respect to personal information received from the EU; and3. description of the organization's privacy policy for such personal information, including: (a) where the privacy policy is available for viewing by the public, (b) its effective date of implementation, (c) a contact office for the handling of complaints, access requ*
ests, and any other issues arising under the safe harbor, (d) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), (e) name of any privacy programs in which the organization is a member, (f) method of verification (e.g. in-house, third party)(1), and (g) the independent recourse mechanism that is available to investigate unresolved complaints". Così2000/520/EC: *Commission Decision 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 Commerc*e, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX %3A32000D0520

[57] Per un'analisi sul tema cfr. W. J. Long – M. Pang Quek, "*Personal Data Privacy Protection in an Age of Globalization: the US-EU Safe Harbor Compromise*", in *Journal of European Public Policy*, 3 June 2003, pp. 325-344; I. M. Azmi, "*E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill*", in *Journal of European Public Policy*, 21 July 2010, pp. 317-330, e anche V. Shaffer, "*Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting of U.S. Privacy Standards*", in *25 Yale J. Int. L. I*, 87, 2000

Department of Transportation (per le compagnie aeree e l'emissione dei biglietti), e *della Federal Trade Commission* (FTC)[58].

In ambito europeo, un'eventuale violazione dei *Safe Harbor Privacy Principles* poteva portare, a seguito del potere di controllo esercitato dai singoli Garanti privacy nazionali dei singoli Stati membri, alla sospensione del flusso transfrontaliero dei dati, indipendentemente dalla valutazione e dall'accertamento operato dalla *Federal Trade Commission*[59].

L'accordo *Safe Harbor* ha dunque, senza ombra di dubbio, apportato notevoli vantaggi ai settori economici dell'Unione Europea e degli Stati Uniti consentendo a milioni di organismi americani di ricevere dati personali provenienti dall'UE.

---

[58] La *Federal Trade Commission*, in materia di protezione dei *Safe Harbor*, gode di specifici poteri, dettati dalla sezione 5. Nello specifico dichiara l'illiceità di "*unfair or deceptive acts or practices in or affecting commerce"* ordina l'adozione di idonee misure *"to prevent such acts and practices"*, e pronunciare *"cease and desistorders"* con lo scopo di far cessare violazioni già in atto. Inoltre può ordinare, per motivi di pubblico interesse, la pronuncia da parte di una *District Court* di un *"temporary restraining order"* oppure di una *"temporary or permanentinjunction"* e, nell'ipotesi di pratiche sleali o ingannevoli può promulgare *"an administrative rule prescribing the acts or practices involved"*. Chiunque non rispetti o infranga le ordinanze della FTC è soggetto a una sanzione civile fino a un massimo di $ 10.000. Così *Section 5 of Federal Trade Commission Act,* disponibile al seguente link: https://www.ftc.gov/sites/default/files/documents/ statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf

[59] Così art. 3 della decisione 2000/520, per cui: "le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:

a) gli enti governativi degli Stati Uniti […] abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ; b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare. La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE".

Tuttavia, il 6 ottobre 2015, con la sentenza *Schrems c. Data Protection Commissioner*[60], la corte di Giustizia Europea ha dichiarato invalido l'accordo *SafeHarbor*, pronunciandosi così sull'inadeguato livello di prote-

[60] Nel 2013 il cittadino austriaco, utente di *Facebook*, *Maximillian Schrems* ha proposto reclamo all'Autorità garante irlandese per la protezione dei dati personali contro *Facebook Ireland* Ltd. Nel ricorso *Schrems* affermava che la società in questione, filiale europea di quella americana *Facebook* Inc., fosse responsabile del trattamento dei dati personali degli utenti utilizzatori di *social network* residenti o
domiciliati in Irlanda. I dati raccolti da *Facebook Ireland* nell'Unione Europea erano infatti trasmessi alla società madre statunitense per un ulteriore trattamento, precedentemente all'archiviazione che avveniva sempre in territorio americano. Il trasferimento dei dati dall'UE agli Stati Uniti avveniva sulla base dell'accordo *Safe Harbor*. Il ricorso proposto da *Schrems* aveva come oggetto non la legittimità del trasferimento transfrontaliero, bensì il giudizio della Commissione in relazione al livello di adeguatezza offerto dagli Stati Uniti nel programma *Safe Harbor*, a seguito delle dichiarazioni di *Edward Snowden* e lo scandalo *Datagate*, ove si denunciava l'attività della sorveglianza elettronica di massa da parte dei servizi pubblici di sicurezza statunitensi. In primo grado l'Autorità garante irlandese ha rigettato il ricorso affermando che l'accorso *Safe Harbor* costituisse un atto vincolante conformemente all'art. 288 TFUE. La decisione della Commissione fu dunque oggetto del ricorso proposto dinanzi all'*High Court* Irlandese, la quale osservò che non risultava che *Facebook* avesse violato gli obblighi del *Safe Harbor* e dunque di non poter interrompere il trasferimento dei dati in quanto mancasse uno specifico comportamento illegittimo, quale requisito necessario. Ciononostante, la *High Court* irlandese palesava i suoi dubbi sulla compatibilità del trasferimento verso gli USA con la Direttiva europea. Secondo la Corte irlandese infatti, sebbene la sorveglianza di massa potesse rispondere ad esigenze di pubblico interesse, la sorveglianza su larga scala operata dagli Stati Uniti sembrava aver ecceduto i limiti consentiti in relazione alla proporzionalità, senza garantire ai cittadini nessuna tutela amministrativa o giurisdizionale. L'*High Cour*t ha dunque operato un rinvio pregiudiziale di interpretazione alla Corte di Giustizia Europea, chiedendo di esaminare se, in presenza di una decisione di adeguatezza della Commissione, le Autorità Garanti nazionali potessero operare una valutazione a posteriori sull'adeguatezza del Paese terzo per la presenza di elementi sopravvenuti volti a dichiarare un'inadeguatezza. Per un'analisi sul tema cfr. M. Mann, "*The Maximillian Schrems Litigation: a Personal Account*", in E. Fahey (a cura di), *Institutionalisation beyond the Nation State: Transatlantic Relations. Data, Privacy and Trade Law*, *Studies in European Economic Law and Regulation*, 10, Springer, London, 2018, pp. 75-89; M. Tzanou, *The Foundamental Right to Data Protection: Normative Value in the context of Counter-Terrorism Surveillance*, Hart Publishing, Portland, 2017, pp. 221 e ss; G. Scarchillo, "*Dal Safe Harbor al Privacy Shield: il trasferimento dei dati personali vs Stati Uniti dopo la sentenza Schrems"*, in 30 *Diritto commercio internazionale*, 2016; D. Pittella, "*Trasferimento verso paesi terzi*", in *La nuova disciplina europea della privacy*, op. cit. pp. 264-266; P. Piroddi, "*I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*", op. cit. pp. 180 e ss.

zione dei dati offerto dagli Stati Uniti[61], a seguito anche delle rivelazioni emerse dal caso *Snowden* e dallo scandalo "*Datagate*".

All'indomani della sentenza *Schrems*, la necessità di concludere negoziati con gli Stati Uniti, già iniziati al momento della proposizione del rinvio pregiudiziale alla Corte di Giustizia Europea, si è mostrata sempre più necessaria. Il WP29 e la Corte di Giustizia premevano infatti sulle trattative per la sostituzione del *Safe Harbor*, invitando la Commissione a trovare una soluzione con il gli Stati Uniti per sopperire al vuoto normativo lasciato dall'invalido accordo[62]. La Commissione, accelerando le trattative per la so-

[61] La Corte esamina la decisione della Commissione osservando che il *Safe Harbor* in primo luogo non certifica l'adeguatezza del livello di protezione offerto dagli Stati Uniti: Esso è infatti applicabile solamente alle imprese e organizzazioni che vi abbiano specificatamente aderito, non vincolando autorità e istituzioni pubbliche. In secondo luogo afferma che il *Safe Harbor* non presenta misure di sorveglianza necessarie a un sistema del genere e, infine, legittimando l'accesso ai dati per esigenze di sicurezza o in presenza di atti legislativi o giurisprudenziali che li autorizzino, non predispone al contempo controlli giuridici per limitare questa ingerenza, nè rimedi giurisprudenziali volte a tutelare i diritti degli interessati nelle ipotesi di accesso illegittimo. Tali carenze sono state anche oggetto dell'analisi del Gruppo art. 29, nel quale si evince come il *Safe Harbor* non abbia salvaguardato i cittadini europei dagli accessi illegittimi da parte delle autorità americane. L'ingerenza delle istituzioni americane viola l'art. 7, 8 e 47 della Carta dei diritti fondamentali. Su tali considerazione la Corte ha dichiarato invalido l'art. 1 della decisione della Commissione sul *Safe Harbor*. La Corte ha altresì dichiarato invalido l'art. 3 della decisione, il quale consente alle autorità nazionali di sospendere i trasferimenti transfrontalieri qualora vi sia un ragionevole dubbio che i principi di legittimità del *Safe Harbor* siano violati. Le condizioni richieste per l'applicabilità di tale articolo sono tuttavia, secondo l'orientamento della Corte, troppo restrittive da limitare il potere delle autorità di controllo. In considerazione dell'inseparabilità dell'art. 1 e 3, la Corte ha così dichiarato invalida tutta la decisione relativa al *Safe Harbor*. Si veda Article 29 Data Protection Working Party Opinion 4/2000 *on the level of protection provided by the "Safe Harbor Principles*", http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf

[62] Cfr. WP29 "*Statement 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*", per cui: "*the Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights. Such solutions could be found through the negotiations of an intergovernmental agreement providing stronger guarantees to EU data subjects. The current negotiations around a new Safe Harbor could be a part of the solution. In any case, these solutions should always be assisted by clear and binding mechanisms and include at least obligations on the necessary oversight of access by*

stituzione del *Safe Harbor*, il 29 febbraio 2016 ha annunciato di aver trovato un'intesa con il governo americano, con la presentazione della proposta della decisione di adeguatezza *dell'EU-US Privacy Shield*[63], cd. "*Scudo per la riservatezza*".

Il *Privacy Shield* persegue l'obiettivo, come nel caso del *Safe Harbor*, di istituire un sistema di protezione dei dati per il trasferimento dei dati al di fuori del territorio europeo, comprendendo una serie di principi che le organizzazioni aderenti sono tenute a rispettare, nonché l'istituzione di organismi di vigilanza con potere di infliggere sanzioni per il mancato rispetto di tali principi, e con la previsione, nell'ipotesi di violazione dell'accordo, di mezzi di ricorso individuali.

La novità maggiore è il rilascio, da parte del governo americano, di dichiarazioni scritte a conferma della vincolatività dell'accordo e pubblicati *nell'U.S. Federal Register*.

Le organizzazioni che intendono aderire al sistema del *Privacy Shield* devono ottenere una certificazione presso il *Department of Commerce* degli Stati Uniti, che avrà l'onere di sottoporre a verifiche periodiche la *compliance* delle stesse alla nuova regolamentazione. Le organizzazioni saranno poi responsabili di eventuali cd. "trasferimenti successivi" di dati personali di cittadini europei a soggetti terzi, esterni all'accordo contrattuale.

L'accordo prevede inoltre l'istituzione di un mediatore indipendente, il cui scopo sarà quello di trattare i ricorsi dei cittadini dell'Unione per gli accessi effettuati dalle autorità pubbliche americane per i motivi di pubblico interesse.

In ultimo, l'accordo *Privacy Shield* istituisce il meccanismo di riesame congiunto, volto a monitorare il corretto funzionamento dell'accordo, congiuntamente al *Department of Commerce* degli Stati Uniti[64].

---

public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights". http://ec.europa.eu/justice/article-29/pressmaterial/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

[63] L'accordo politico denominato *Privacy Shield* è stato adottato dalla Commissione, il 12 luglio 2016, successivamente all'analisi del *Working Party* Art. 29 e alla risoluzione del Parlamento europeo.

[64] Cfr. Commissione europea – Comunicato stampa del 29 febbraio 2016: "*Ripristinare la fiducia nei trasferimenti transatlantici di dati mediante forti misure di salvaguardia:*

Il nuovo accordo sembra così offrire maggiori garanzie a tutela della protezione dei dati più elevate del precedente *Safe Harbor*. L'approccio incentrato sul rischio, l'innalzamento del livello di responsabilità dei soggetti interessati al trattamento dei dati, la definizione di specifiche procedure per i reclami concernenti illeciti trattamenti dei dati e l'adozione di un sistema di monitoraggio costante oltreoceano, fa da sfondo al nuovo Regolamento, perseguendo dunque l'obiettivo comune di preservare e creare un equilibrio regolatorio tra i due differenti approcci al diritto alla privacy[65].

Lo standard della norma in esame ben si sposa con le caratteristiche e le novità introdotte dal Regolamento n. 679/2016 che infatti, in linea con il principio di *privacy by design,* ha elaborato una serie di regole volte a minimizzare il rischio valutandone *ex ante* le possibili conseguenze, con la previsione di misure e di livelli di sicurezza da garantire all'utente *cloud.*

4.2 La questione Brexit e il suo impatto sul trasferimento transfrontaliero dei dati

Tramite il referendum del 23 giugno 2016, il Regno Unito ha dimostrato di voler lasciare l'Unione Europea[66]. Il voto favorevole per il divorzio da Bruxelles ha comportato notevoli conseguenze sul piano non solo economico e politico, ma anche in relazione a taluni aspetti di natura giuridica.

Nonostante i numerosi tentativi volti alla definizione di un accordo tra il Regno Unito e l'UE al fine di evitare la cd. "*Hard Brexit*"[67], le possibilità di

---

la Commissione europea presenta lo scudo UE-USA per la privacy", Bruxelles, disponibile al seguente link: http://europa.eu/rapid/press-release_IP-16-433_it.htm

[65] Si veda a riguardo S. Sica, "*Verso l'unificazione del diritto europeo alla tutela dei dati personali?*", in *La nuova disciplina europea della privacy*, op. cit., p.12

[66] L'articolo 50 del Trattato di Lisbona dispone che "Ogni Stato membro può decidere, conformemente alle proprie norme costituzionali, di recedere dall'Unione". Gazzetta ufficiale dell'Unione Europea: Trattato di Lisbona, 2007: https://www.ecb.europa.eu/ecb/legal/pdf/it_lisbon_treaty.pdf

[67] Tra i vari tentativi per la definizione di un accordo, il 17 ottobre 2019, due settimane prima della data prevista dall'uscita del Regno Unito dall'UE, il governo britannico e la Commissione europea hanno annunciato di aver raggiunto un accordo sui termini dell'uscita del Regno Unito dall'Europa. Tuttavia, tale accordo non è stato approvato dal Parlamento britannico che ha invece approvato un Emendamento che sposta il voto sull'accordo Brexit ad un momento successivo, richiedendo prima l'approvazione di tut-

uscita del Regno Unito dal territorio dell'Unione con *no-deal,* ovvero senza un accordo, sembra manifestarsi come una delle possibili conseguenze.

Naturalmente, in assenza di un accordo tra il Regno Unito e l'UE (*no-deal Brexit*), saranno notevoli le conseguenze applicative e normative, specialmente in riferimento alla privacy e alla protezione dei dati, poiché in caso di mancato accordo, il Regno Unito diventerà un paese terzo ai sensi del Regolamento.

In caso di *no-deal Brexit*, il trasferimento transfrontaliero dei dati personali potrà avvenire esclusivamente in presenza dei presupposti richiesti per i paesi terzi.

La qualificazione di un paese terzo, ai sensi del Regolamento, comporta difatti l'esclusione di detto paese dall'area di libera circolazione dei dati tra gli stati membri dell'UE, risultando per i Titolari del trattamento obbligatoria l'individuazione e l'applicazione di una base giuridica per il trasferimento dei dati verso i paesi terzi[68].

Nell'ottica dunque di una possibile *no-deal Brexit*, il Comitato Europeo per la Protezione dei Dati ("**EDPB"**) ha emanato e adottato una nota informativa con il fine di illustrare a tutti i titolari e responsabili del trattamento le modalità per il corretto trasferimento dei dati al di fuori dell'UE[69].

---

te le leggi collegate all'uscita del Regno Unito dall'UE (cd. "*Withdrawal Agreement Bill*"). Senza il voto del Parlamento, il governo è costretto a chiedere una nuova proroga per l'uscita del Regno Unito dall'EU, spostando la Brexit dal 31 ottobre 2019 al 31 gennaio 2020. Il primo ministro Boris Johnson ha inviato alla Commissione europea due lettere, a mezzanotte, una con la quale chiedeva lo slittamento della Brexit, non firmata; e un'altra (firmata) con la quale chiedeva di ignorare la precedente missiva. La Commissione ha tuttavia affermato di decidere nel merito solamente dopo la discussione parlamentare britannica. E' poi pervenuta all'attenzione della Commissione europea una terza lettera della Rappresentanza diplomatica britannica la quale chiariva la natura delle precedenti due missive, in particolare emergeva che la lettera priva di firma era l'assolvimento di un obbligo del primo Ministro a seguito della votazione parlamentare inglese, li dove invece il contenuto della lettera firmata rappresentava la reale intenzione del primo Ministro. https://www.dailymail.co.uk/news/article-7592073/Boris-Johnson-sends-THREE-letters-EU-one-urge-Brussels-NOT-grant-delay.html

[68] Cfr. art. 1, par. 3 Regolamento

[69] EDPB - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit-october_en.pdf - 4 ottobre 2019

In caso di *no-deal Brexit* infatti, il trasferimento dei dati personali verso il Regno Unito potrà avvenire solo in presenza dei presupposti richiesti al paese terzo e, in linea generale, il trasferimento non è ammesso salvo che tale paese assicuri un livello di protezione dei dati adeguato, il cd. "*livello di adeguatezza*"[70].

Ne consegue che, qualora non venga raggiunto un accordo sulla Brexit tra il Regno Unito e l'UE relativo alla protezione dei dati nonché alle ipotesi di trasferimento transfrontaliero, la Commissione dovrà sottoporsi ad un processo di valutazione per poter garantire l'adeguatezza del Regno Unito.

In mancanza di una decisione di adeguatezza, così come illustrato dall'EPDB, il trasferimento dei dati dall'UE al Regno Unito dovrà trovare fondamento nelle seguenti basi giuridiche:

- clausole tipo di protezione dei dati personali (*standard contractual clauses*)[71];
- norme vincolanti d'impresa (*Binding corporate rules*);
- codici di condotta e meccanismi di certificazione;
- deroghe ai sensi dell'art. 49 del Regolamento[72].

[70] Cfr. art. 45 Regolamento

[71] Nello specifico, per il trasferimento dei dati personali da Titolari siti nell'area dell'UE a Titolari situati in paesi terzi si veda la Decisione della Commissione 2001/497/CE relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE e la Decisione 2004/915/CE, 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. Inoltre per i trasferimenti da Titolari in UE a responsabili in paesi terzi si veda la decisione della Commissione 2010/87/CE, 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.

[72] Ai sensi dell'art. 49 del Regolamento, le deroghe al trasferimento transfrontaliero dei dati personali sono: a) il consenso espresso dell'interessato, b) la necessità del trasferimento ai fini dell'esecuzione o della conclusione di un contratto stipulato fra l'interessato e il titolare, ovvero di un contratto stipulato nell'interesse della persona interessata; c) la necessità del trasferimento per importanti motivi di interesse pubblico; d) la necessità del trasferimento per il perseguimento degli interessi legittimi e cogenti del titolare o del responsabile.

Secondo la nota informativa adottata dall'EPDB le aziende dovranno impegnarsi attivamente per adottare le seguenti azioni pratiche:

1. Individuare i trattamenti che implicano un trasferimento di dati personali verso il Regno Unito.
2. Individuare uno strumento giuridico appropriato per il trasferimento di dati personali.
3. Implementare, entro il 31 ottobre 2019, lo strumento giuridico scelto per il trasferimento.
4. Indicare nella documentazione interna che verrà effettuato un trasferimento dei dati personali verso il Regno Unito.
5. Aggiornare le informative sulla protezione dei dati[73].

Resta inteso che, per il trasferimento dei dati personali dal Regno Unito all'UE, anche in caso di "*hard Brexit*" continuerà a vigere la libera circolazione dei dati personali[74].

5. Conclusioni: verso l'avvicinamento del modello europeo e statunitense

Sebbene il diritto alla privacy sia "nato" negli Stati Uniti, inteso come quel labile confine che intercorre tra riservatezza e informazione, è a livello europeo che si sviluppa e si qualifica come un diritto inviolabile dell'uomo.

È infatti il crescente sviluppo tecnologico e la nascita della Comunità Economica Europea che ha contribuito all'affermazione di un concetto di privacy legato alla tutela della libertà personale e alla sua individualità, quale diritto inscindibilmente connesso ai diritti di libertà tanto individuale quanto collettivo. Lo stesso concetto di privacy risulta evidentemente inefficace nel ricomprendere le diverse accezioni che lo stesso ha nel tempo assunto.

[73] EDPB, *Information note on BCRs for companies which have ICO as BCR Lead Supervisory Authority* – 12 febbraio 2019.
[74] Si veda il provvedimento del Garante per la protezione dei dati personali – "*Trasferimento in caso di "hard Brexit"*, 27 febbraio 2019 https://www.garanteprivacy.it/ regolamentoue/brexit#allegato

Per tale ragione si è affiancato al modello nordamericano, incentrato esclusivamente sulla tutela della privacy, il modello europeo che valorizza *a contrario* anche la dimensione del trattamento dei dati personali.

Il modello statunitense, infatti, si caratterizza per una più diffusa tutela in sede giurisdizionale del diritto alla privacy, inteso come l'ampio diritto a limitare le intrusioni nella propria vita privata, e l'assenza di una legislazione di riferimento in materia di *data protection*, mentre il quello europeo si caratterizza per la presenza di una normativa di dettaglio in materia di protezione dei dati e la tutela giurisdizionale, relegata a poche ipotesi residuali, del diritto alla riservatezza.

Tali modelli si sono nel tempo influenzati attraverso i vari accordi internazionali in materia – dapprima la Convenzione di Strasburgo del 1981[75], poi, sotto la direttiva 95/46/CE, il *Safe Harbour*[76] e il *Privacy Shield*[77] – che

[75] Con lo sviluppo delle tecnologie informatiche in vaste arie della vita economica e sociale, nel 1980, l'OECD ha adottato le linee guida, "Linee guida del 1980", con l'obiettivo di regolamentare il copioso flusso di dati personali e tutelare al contempo la riservatezza, per affrontare i problemi derivanti dal sempre maggiore uso di dati personali ed evitare rischi per le economie globali risultanti da eventuali restrizioni al trasferimento di informazioni oltre i confini. Le linee guida del 1980, contenenti il primo insieme di principi generali sulla privacy, hanno così influenzato la legislazione e la politica degli stati membri dell'OECD e a livello internazionale. Nel 2013 il documento è stato oggetto di revisione, la quale ha comportato l'introduzione di nuovi concetti quali: strategie nazionali sulla privacy, programmi di gestione della privacy e la notificazione delle violazioni dei dati. *OECD Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) as amended on 11 July 2013* https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[76] L'accordo *Safe Harbor* trova il suo fondamento giuridico nella Direttiva 95/46/CE la quale, all'art. 25 par. 1 impone che il paese terzo verso il quale avvenga il trasferimento dei dati fornisca un adeguato livello di protezione. La scelta dell'Unione europea è stata quella di imporre a chiunque esportasse dati di origine comunitaria di conformarsi al dettato normativo europeo, garantendo così che i dati in transito godessero di specifici livelli di tutela, modellati sulla base della Direttiva 95/46/CE. Sul punto. A. Mantelero, "*Data Protection ed attività di impresa. Verso dove guardano gli USA?*", in *Diritto dell'informazione e dell'informatica*, 2011, pp. 457 e ss., ove sottolinea come il modello comunitario "*grazie ad un'acuta scelta di strategia normativa, sia stato esportato al di fuori dei confini dell'Unione, adottato o usato come esempio per legislazioni di diverse nazioni, ed è divenuto in ogni caso parametro necessario di confronto*".

hanno permesso lo scambio dei dati senza tuttavia incidere sull'approccio interno dei rispettivi legislatori.

L'approccio incentrato sul rischio, l'innalzamento del livello di responsabilità dei soggetti interessati al trattamento dei dati, la definizione di specifiche procedure per i reclami concernenti illeciti trattamenti dei dati e l'adozione di un sistema di monitoraggio costante oltreoceano, fa da sfondo al nuovo Regolamento, perseguendo dunque l'obiettivo comune di preservare e creare un equilibrio regolatorio tra i due differenti approcci al diritto alla privacy[78].

La crescente diffusione delle tecnologie di comunicazione e, in particolare, delle piattaforme di *cloud computing* impiegate nel trattamento dei dati personali ha imposto che le parti, *cloud provider* prevalentemente statunitensi e utenti *cloud* professionali europei, regolassero contrattualmente più nel dettaglio gli aspetti legati al trattamento dei dati.

In tal senso si richiamano le Linee-guida della Commissione Europea in materia di standardizzazione delle clausole nei contratti di servizi *cloud* che, appunto, evidenziano l'opportunità che nei contratti sottoscritti per lo svolgimento di servizi impiegati professionalmente nei livelli di servizi sia riportato il diritto di verificare la reale corrispondenza di quanto dichiarato dal *cloud provider*. Ciò, si potrebbe aggiungere all'indomani dell'adozione del Regolamento (UE) n. 2916/679 che ha riscritto il quadro normativo europeo in materia di *data protection*, anche e soprattutto in ragione del principio di *accountability* che grava sui titolari del trattamento ai quali spetta l'onere di designare responsabili esterni nel trattamento, quali sarebbero i *cloud provider*, solo dopo averne verificato il possesso di misure di sicurezza tecniche ed organizzative adeguate ai rischi correlati al trattamento affidato.

---

[77] L'accordo politico denominato *Privacy Shield* è stato adottato dalla Commissione, il 12 luglio 2016, successivamente all'analisi del Working Party Art. 29 e alla risoluzione del Parlamento europeo, a seguito della sentenza *Schrems c. Data Protection Commissioner*, con la quale la corte di Giustizia Europea ha dichiarato invalido l'accordo *Safe Harbor*.

[78] Si veda a riguardo S. Sica, "*Verso l'unificazione del diritto europeo alla tutela dei dati personali?*", in S. Sica, V. D'Antonio, G.M. Riccio *(*a cura di), *La nuova disciplina europea della privacy,* Cedam, Padova, 2016, p.12

A quanto detto si aggiunga che il citato Regolamento ha altresì ampliato il proprio ambito territoriale di applicazione estendendosi a tutti i servizi che vengono offerti a individui che si trovano nel territorio dell'Unione[79].

Ed ecco che allora pare emergere come da un lato i fornitori di servizi statunitensi debbano assumere maggiori obblighi in materia di trattamento dei dati personali verso quei titolari del trattamento stabiliti in Europa che si

[79] E' bene tuttavia sottolineare taluni problemi derivanti dall'implementazione del "*Clarifying Lawful Overseas Use of Data (CLOUD) Act*" cd. US CLOUD Act, adottato dal Governo federale degli Stati Uniti lo scorso 23 marzo 2018, il quale consente alle autorità statunitensi, forze dell'ordine e agenzie di intelligence, al fine di accelerare e rendere più efficienti le loro indagini, di richiedere e acquisire dati ed informazioni contenuti in documenti elettronici dagli operatori di servizi di *cloud computing* a prescindere dal posto ove questi dati si trovano, e dunque anche se collocati su server al di fuori dagli Stai Uniti. La sola condizione è che questi operatori siano sottoposti alla giurisdizione degli Stati Uniti, che siano le stesse società europee ad avere una filiale negli Stati Uniti o che siano società che operano nel mercato americano. Secondo l'EPDB sono molteplici e di varia natura i dubbi emersi in relazione alla legittimità di suddetta previsione normativa, così come emerso durante la dodicesima riunione plenaria dello scorso luglio 2019. Nello specifico, la possibilità che le autorità USA possano "ordinare" la produzione di dati personali a soggetti cui si applica il Regolamento, pare poter essere inteso come il tentativo di bypassare, con il pur fine legittimo di accelerare e rendere efficaci le indagini, le attuali previsioni in materia di cooperazione internazionale. La richiesta di produzione di documenti elettronici, di per sé sola non costituisce una base legale sufficiente ad autorizzare il trasferimento dei dati, entrando in conflitto con le disposizioni dell'art. 48 del Regolamento, il quale contiene le disposizioni volte a disciplinare "trasferimenti o comunicazioni non autorizzati dal diritto dell'Unione", costituendo un elemento importante dell'attuale insieme di norme che inquadra la divulgazione e il trasferimento di dati personali dall'UE verso paesi terzi. E dunque, siffatta procedura, sembra essere priva di tutte le garanzie procedurali e sostanziali che possono essere garantite esclusivamente mediante l'approvazione di accordi internazionali. Pertanto, l'EPDS ha affermato che a meno che il suddetto US CLOUD Act sia riconosciuto o sia reso esecutivo sulla base di un accordo internazionale, la liceità di tali trasferimenti di dati personali non può essere sempre riconosciuta, fatte salve circostanze eccezionali in cui il trattamento è necessario al fine di proteggere gli interessi vitali dell'interessato. In particolare, si è sottolineata l'esigenza di procedere ad una rapida modifica dell'attuale "Mutual Legal Assistance Treaty (MLAT) in vigore tra UE e Usa dal 19 luglio 2003, con il fine di garantire un maggiore livello di protezione dei dati mediante la previsione di determinate garanzie basate, ad esempio, sul principio di proporzionalità e minimizzazione dei dati. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf . Per un'analisi sulle implicazioni giuridiche del US CLOUD ACT in rapporto con il Regolamento UE si veda R. Milch and S. Benthall (eds), "*Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?"*, in *Cybersecurity and Privacy in a Globalized World - Building Common Approaches*, New York University School of Law, NY, 2019

avvalgono dei loro servizi *cloud* e, dall'altro, che gli operatori economici che intendono anche solo offrire dei servizi in Europa devono adeguarsi alla disciplina ora vigente[80].

Tale evoluzione tecnico-normativa pare che stia portando ad un progressivo avvicinamento tra i due modelli di tutela della riservatezza e dei relativi dati personali. Pare che una elemento indiziario a sostegno dell'anzidetto avvicinamento tra i modelli possa essere rinvenuto nel *California Consumer privacy Act*[81] (di seguito anche "CCPA") del 28 giugno 2018, che fa proprio il modello europeo.

Il CCPA, in vigore dal 1° gennaio 2020, è una legge che protegge i consumatori residenti in California[82] che acquistano, a titolo personale, beni o servizi da imprese che operano nel settore business in California ed effettuano operazioni di trattamento sui dati medesimi[83].

Il senatore statale Bill Dodd, co-promotore del disegno di legge, ha affermato che il CCPA porta la California in "*the lead in protecting consumers and holding bad actors accountable. My hope is other states will follow, ensuring privacy and safeguarding personal information in a way the federal government has so far been unwilling to do",* aggiungendo che *"lot of time and effort was put into the original bills and the initiative. This is a great example of people working together and getting something done for consumers"*[84].

---

[80] Si rammenta a mero titolo esemplificativo come all'indomani del 25 maggio 2018, data di diretta applicazione del Regolamento (UE) n. 2016/679, molti quotidiani statunitensi abbiano impedito l'accesso ai rispettivi siti internet agli utenti europei dichiarandosi non conformi con il Regolamento e, per tanto, in ragione del perimetro di applicazione dello stesso, impossibilitati ad erogare il servizio.

[81] California Consumer Privacy Act https://leginfo.legislature.ca.gov/faces/ billCompareClient.xhtml?bill_id=201720180AB375

[82] Il *California Civil Code* §1798.140 (g) definisce come consumatore *"[a] natural person who is a California resident*".

[83] In particolare ai consumatori che*"(a) have annual gross revenues of $25 million or more; (b) buy, receive, sell, or share the personal information of 50,000 or more consumers (defined in the CCPA as California residents), households or devices on an annual basis; or (c) have 50% or more of its annual revenues coming from the sale of personal information of California residents*". Cal. Civ. C. §1798.140(c)(1)(a), (b) and (c).

[84] https://sd03.senate.ca.gov/news/20180814-california-consumer-privacy-act-2018

Tra le principali somiglianze rinvenibili tra il CCPA e il Regolamento, emerge anzitutto la tutela dei diritti che entrambi i regolamenti forniscono ai consumatori, quali il diritto di conoscere le informazioni personali che una società possiede, il diritto di ottenere informazioni sulla fonte di raccolta, la natura delle informazioni raccolte, eventuali divulgazioni di dati personali, trasferimenti o vendite a terzi e le finalità che giustificano la conservazione dei dati[85]. Sono presenti anche alcune similitudini tra le basi giuridiche del trattamento, distinguendo tra il "legittimo interesse" unionale, e l'"*internal use*" californiano.[86]

Rileva, in particolare, l'obbligo per le imprese di dichiarare ai consumatori quali dati collezionano e se vengono condivisi con terze parti, così come previsto nell'obbligo di informativa di cui all'art. 13 del Regolamento. Inoltre, viene garantita ai consumatori la possibilità di chiedere che i dati registrati siano cancellati, così come prevede l'art. 17 del Regolamento, e di non vedere le proprie informazioni personali cedute, in analogia a quanto disposto dall'art. 18 del Regolamento.

Ciò che differenzia il CCPA dal Regolamento è forse l'impronta economica che permane nella nuova legge californiana, in quanto autorizza espressamente le società a fornire incentivi finanziari agli utenti per incoraggiare la divulgazione dei dati. Pertanto, una società può effettuare pagamenti ai consumatori come compenso per la raccolta dei propri dati, oppure offrire prezzi, livelli tariffari, qualità di beni o servizi diversi, specificando che gli incentivi devono essere "*directly related to the value provided to the consumer by the consumer's data"*[87]*,* e non *"unjust, unreasonable, coercive, or usurious in nature"*[88].

Così, da un approccio fattuale di protezione dei dati, con il *California Consumer Privacy Act*, gli Stati Uniti hanno adottato la prima normativa vicina ai sistemi di *data protection* europei, prevedendo sistemi di protezione

[85] Cfr. Cal. Civ. C. §1798.110(a)(1) e artt. 13-14 Regolamento.
[86] Sul punto si veda il commento di L. Bolognini, *Le differenze tra GDPR e CCPA*, https://www.lucabolognini.it/2018/07/02/2-luglio-2018-luca-bolognini-espone-le-differenze-tra-gdpr-e-ccpa/
[87] Cfr. Cal. Civ. C. §1798.125(b)(1)
[88] Cfr. Cal. Civ. C. §1798.125(b)(4)

dei dati improntati sul diritto, di ogni consumatore, di controllare l'insieme delle informazioni a lui riferibili, eliminando la residuale protezione dei dati.

Pare dunque che il CCPA rappresenti un importante elemento di avvicinamento tra il modello statunitense e quello europeo cui si è giunti in ragione del combinarsi di molteplici fattori e che potrebbe, presto, essere seguito da analoghe iniziative legislative di altri stati federali, i quali potrebbero dare un'ulteriore spinta a tale percorso.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442