Rivista Semestrale

Luglio - Dicembre 2019

N. 2/2019

Data Protection Law

Diritto delle nuove tecnologie, privacy e protezione dati personali

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it

Diretta da Elio Errichiello

www.dataprotectionlaw.it

DATA PROTECTION LAW – RIVISTA GIURIDICA

Rivista online non soggetta ad obbligo di registrazione ai sensi dell'art. 3-bis del Decreto Legge 103/2012

Sito web: www.dataprotectionlaw.it

Contatti: info@dataprotectionlaw.it

"Data Protection Law" è una rivista elettronica di diritto Open access pubblicata dall'associazione Data Protection Law. La rivista pubblica con cadenza semestrale numeri costituiti da articoli scientifici inediti, saggi, traduzioni di estratti da opere scientifiche significative e di recente pubblicazione o articoli rilevanti per la comunità scientifica, recensioni di libri ed eventi culturali.
I numeri della rivista ospitano contributi scientifici prodotti e sottoposti su invito diretto della redazione.
Tutti i contributi sono sottoposti a doppia blind peer review.

Indice.

IL TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI.

di Monica Mandico

SOMMARIO. 1. Premessa - 2. Dalla Direttiva 95/46/CE al Regolamento 679/16 - 3. La nozione di «stabilimento» e il principio di territorialità - 4. La sentenza Privacy Shield per il trasferimento dei dati negli Stati Uniti - 5. Il trasferimento dei dati trasfrontalieri come da Regolamento 679/16. Un nuovo modello.

The case of data transfer to a third country or an international organization is subject to careful regulation by the legislator of the EU Regulation 2016/679, which was also achieved following the development of technological evolution and datafication processes in progress, in addition to the concerns and criticalities that the phenomenon infuses, given the massive and continuous use of cloud computing technologies, which through the principle of "redundancy" of data to placed servers, very often not only outside from Italy, but also from Europe, they stimulate questions about the levels of protection that such a technology can offer to information placed on platforms, which offer users such a service.

1. Premessa

La fattispecie del trasferimento dei dati verso un paese terzo o un'organizzazione internazionale[1], è oggetto di attenta disciplina da parte del legislatore del Regolamento UE 2016/679, a cui si è pervenuti anche a seguito del divenire dell'evoluzione tecnologica e dei processi di *datafication* in progresso, oltre alle preoccupazioni e criticità che il fenomeno infonde, stante il massiccio e continuativo uso delle tecnologie di *cloud computing*[2], che attraverso il principio di "ridondanza" dei dati verso *server*

[1] Con "organizzazione internazionale" deve intendersi un soggetto giuridico costituito e formato da enti pubblici (e.g., gli Stati) che persegue finalità pubblicistiche, restando escluse quelle organizzazioni che, pur perseguendo finalità di pubblico interesse, non sono costituite da soggetti di diritto pubblico

[2] M. MANDICO, *"Privacy le prime applicazioni settoriali della nuova disciplina",* Santarcangelo di Romagna, 2019: "*Il cloud computing (letteralmente "nuvola informatica") è un complesso di sistemi di archiviazione, elaborazione e trasmissione di dati che permette all'utente di accedere agli stessi in qualsiasi momento e da qualsiasi dispositivo, purché dotato di una connessione ad Internet. Il Garante Privacy ha predisposto una guida per imprese e pubblica amministrazione (in allegato). "Il mondo delle imprese e della P.a. sta attraversando un periodo di intensa innovazione guidata da un nuovo tipo di tecnologie e di modalità di fruizione dei servizi: il cloud computing. Questo termine è diventato talmente diffuso da essere utilizzato, a volte anche in modo inappropriato, per qualunque tipo di prodotto o servizio ICT. Le cosiddette "nuvole informatiche" offrono una serie di opportunità in*

collocati, spessissimo fuori non solo dall'Italia, ma anche dall'Europa, stimolano interrogativi sui livelli di protezione che una tale tecnologia può offrire alle informazioni collocate sulle piattaforme, che offrono agli utenti un tale servizio.

Al trasferimento dei dati verso paesi extra UE, il nuovo Regolamento europeo dedica un apposito capo – il *V* – intitolato ai «*trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*». La preoccupazione del legislatore del *GDPR*, e` che la tutela garantita dalla disciplina europea, non sia elusa o superata a causa del trasferimento dei dati all'estero fuori dall'Europa.

La normativa, nasce sia dall'esigenza di armonizzare le diverse disposizioni dei paesi europei, mirando, dunque, a garantire, nel caso di un trasferimento di dati extra-UE, che i medesimi non vengano trattati in modo da ledere i diritti e le libertà degli interessati, - cioè da costituire un punto debole rispetto ai diritti delle persone fisiche - ; sia per essere al passo con il progresso tecnologico, sul punto l'intento è ben espresso nel considerando 101che si riporta per quanto di specifico interesse:

"*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. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese*

termini di efficienza e risparmio, ma possono comportare criticità e costi aggiuntivi di cui è bene tener conto. Il Garante per la protezione dei dati personali, per facilitare l´attività di aggiornamento e innovazione di imprenditori e amministratori pubblici, ha deciso di realizzare una "mini guida" intitolata "CLOUD COMPUTING - Proteggere i dati per non cadere dalle nuvole", pensata non solo per gli esperti del settore, ma anche per coloro che sono interessati alla comprensione e alla potenziale adozione di queste nuove tecnologie. Prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è infatti necessario porsi alcune domande, scegliendo con cura la soluzione più sicura per le attività istituzionali o per il proprio business. Il vademecum predisposto dall´Autorità è corredato da esempi concreti e da un decalogo con spunti operativi e di riflessione. Imprese e P.a. potranno utilizzare questo strumento per cominciare ad approfondire i potenziali rischi del cloud, decidere quali tipi di dati – anche personali o addirittura sensibili – trasferire e per quali scopi. Una scelta consapevole consentirà di "avvicinarsi alle nuvole" senza rischiare di cadere. La mini guida è suddivisa in cinque capitoli: "Cos´è il cloud computing"; "Nuvole diverse per esigenze diverse"; "Il quadro giuridico"; "Valutazione dei rischi, dei costi e dei benefici"; "Il decalogo per una scelta consapevole". Nei primi due capitoli si approfondiscono i principali tipi di "nuvole" e le modalità di utilizzo. Il terzo offre una panoramica dei principali riferimenti normativi del settore, con particolare riguardo alla protezione dei dati. Gli ultimi due capitoli propongono i principali criteri per valutare costi e benefici dell´adozione del cloud e una serie di consigli concreti per effettuare le scelte più opportune".

terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. (...)".[3]

2. Dalla Direttiva 95/46/CE al Regolamento 679/16

In passato a soddisfare l'esigenza di *data protection*, sia a livello internazionale, sia europeo era intervenuta l'OCSE, ben prima che fosse approvata la *Direttiva Madre* 95/46/CE, che con l'articolo 25, par. 1) stabiliva il concetto di adeguatezza nel " *trasferimento*[4] *verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento* ." Proprio dalla Direttiva ritroviamo i fondamenti applicati ai trattamenti nel nostro ordinamento giuridico, con il Codice della *privacy* (D. Lgs. 196/2003), fino alla effettiva applicazione del nuovo regolamento 679/16.

Nell'ambito della c.d. "*Direttiva madre*" in materia di *privacy*, infatti, venne introdotto il principio fondamentale secondo cui la libera trasferibilità, da uno Stato all'altro, di dati personali, fosse subordinata alla garanzia di un livello di protezione adeguato. Il concetto di "*adeguatezza*", anche se non esplicitato come nozione, divenne indispensabile per consentire il trasferimento dei dati. Tuttavia fu previsto e

[3] A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di internet,* in *Europa e Diritto Privato*,.4, 2017, pag. 1179: "*Sono responsabili del fenomeno del trattamento transnazionale dei dati personali e del trasferimento dei dati verso Paesi terzi, in particolare, le imprese che gestiscono motori di ricerca, social network, siti commerciali dalla portata transfrontaliera, gli operatori dei servizi di cloud computing. Il trattamento transnazionale ed il trasferimento dei dati accompagnano gli sviluppi tecnologici informatici del prossimo futuro tra i quali, oltre al cloud computing, i c.d. big data e la Internet of Things (IoT). Il trasferimento dei dati personali all'estero è anzi all'atto pratico coessenziale allo svolgimento di servizi come quelli di cloud computing oggi di ampio utilizzo e in via di sempre maggiore diffusione nel prossimo futuro. Il fenomeno del trattamento transnazionale dei dati si allarga, ancora, ad abbracciare la grande maggioranza dei siti Internet se si riflette sulla circostanza che i cookie impiegati dai siti raccolgono dati personali degli utenti, che si prestano spesso nel concreto ad essere trattati secondo leggi di Paesi terzi o ad essere trasferiti all'estero"*.

[4] *Ibidem*: relativamente alla nozione di trasferimento dei dati, la Corte di Giustizia ha precisato con la sentenza Lindqvist (Corte Giust. Ue, 3 novembre 2003, C-101/01) che non si configura un trasferimento di dati in un Paese terzo quando una persona che si trova in uno Stato membro inserisce in una pagina Internet dati personali, rendendoli così accessibili a chiunque si colleghi a Internet, compresi coloro che si trovano in Paesi terzi. Sentenza che sembra fondarsi sul timore di un'interpretazione estensiva della nozione di trasferimento, secondo cui si avrebbe un trasferimento verso un Paese terzo (vietato in principio dalla direttiva, se tale Paese non garantisce un livello di protezione adeguato) ogni qualvolta il dato sia caricato su Internet e sia quindi accessibile a chiunque in rete, anche se non trasferito direttamente da chi lo carica a chi vi accede. Focarelli, op. cit., pp. 35 ss.

riconosciuto, un potere per la Commissione *UE*, di stabilire se sussistesse siffatta adeguatezza, mediante una specifica decisione che tenesse conto degli aspetti di cui al comma 6 del medesimo articolo 25.

"La Commissione può constatare (...) che un Paese terzo garantisce un livello di protezione adeguato ai sensi del par. 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (...) ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona". L'adeguatezza del livello di protezione garantito da un Paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati, ed in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il Paese d'origine e il Paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel Paese di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate (art. 25, 2° co. dir. 95/46). Come conseguenza della valutazione di adeguatezza risultava possibile trasferire i dati personali in tale Paese terzo. Nello specifico l'art. 44 lett. b del cod. privacy prevedeva che il trasferimento dei dati all'estero è autorizzato dal Garante del Paese da cui i dati provengono, sulla base delle decisioni di adeguatezza del livello di protezione garantito dal Paese destinatario assunte dalla Commissione europea secondo la previsione di cui all'art. 25, 6° co. della direttiva. Erano, tuttavia previste, all'articolo 26, delle deroghe al vaglio della Commissione, che giustificavano il trasferimento di dati personali verso un Paese terzo non "*adeguato*" nei seguenti casi:

- la presenza del consenso dell'interessato;

- per l'esecuzione di un contratto tra il titolare e la persona interessata o per l'esecuzione di misure precontrattuali;

- per la conclusione o l'esecuzione di un contratto da concludere, concluso nell'interesse della persona interessata, del responsabile del trattamento o di un terzo;

- per la salvaguardia di un interesse pubblico rilevante, oppure per constatare, esercitare o difendere un diritto per via giudiziaria;

- per la salvaguardia di un interesse vitale dell'interessato;

- qualora il trasferimento avvenisse da un registro pubblico, in forza di disposizioni legislative o regolamentari.

All'art. 26, comma 2 della Direttiva, inoltre, si prevedeva un'ulteriore fattispecie, data dall'autorizzazione da parte dello Stato dell'Unione europea su richiesta del

titolare del trattamento, accompagnata da un corredo documentale dimostrativo di garanzie "*adeguate"* di livello contrattuale per la tutela dei dati personali dell'interessato oggetto di trasferimento. In Italia, la materia fu trasposta e regolata nel Codice *privacy* d. lgs. 196/2003, al Titolo VII.

Segnatamente, la presenza di discipline diverse nei diversi paesi europei, e la frammentazione normativa, che produceva effetti negativi al mercato digitale europeo, ha spinto l'UE all'emanazione del Regolamento (UE) 2016/679, che ne ha dettato la definitiva stabilizzazione su tutto il territorio dell'Unione europea e ha così costituito, congiuntamente alla Convenzione 108/1981 del Consiglio d'Europa, l'unico strumento, per il tema, vincolante a livello internazionale.

Su questo impianto di partenza si è perciò sovrapposta, l'abrogazione della Direttiva 95/46/CE con sostituzione delle norme del Codice italiano non più compatibili, la disciplina del Regolamento europeo, che contiene alcuni elementi di novità.[5]

Il trasferimento dei dati personali all'interno dell'Unione europea, è dunque libero (art. 1, par. 3, Reg. 2016/679), vigendo tra gli stati membri il principio della libera circolazione dei dati. Sul punto il considerando n. 10 stabilisce "*al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati dovrebbe essere equivalente in tutti gli Stati membri"*. L'art. 1, par. 3 prevede che "*la libera circolazione dei dati personali nell'Unione non puo` essere limitata ne´ vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*," in vista dell'obiettivo della realizzazione del mercato unico digitale europeo.

[5] M. MANDICO, *Numero monografico sul Regolamento Europeo UE 2016/679*, in *Diritto ed Economia dei mezzi di Comunicazione*, 2/3. 2017-2018 "*Il legislatore europeo, in primo luogo, ha voluto adeguare alle innovazioni tecnologiche, i principi di protezione dei dati personali, anche alla luce dello stato di consapevolezza raggiunto da parte delle istituzioni europee, sulla necessità di tutelare i dati personali in una dimensione complessiva e globale. In secondo luogo il Regolamento, parte dal presupposto che la protezione dei dati personali degli utenti è necessaria ed indispensabile, proprio per il medesimo sviluppo del commercio elettronico, affinché gli utenti possano farvi ricorso con la fiducia che i propri dati personali saranno trattati nel rispetto dei loro diritti. I punti cruciali della nuova disciplina, riguardano dunque: una tutela rafforzata dei diritti della persona; una più rigida ed effettiva applicazione delle norme; una regolamentazione razionalizzata dei trasferimenti internazionali di dati personali e l'istituzione di norme di protezione dei dati a livello generale. La disciplina prevista dal GDPR, nasce dalla prospettiva di garantire che i dati personali degli utenti europei siano protetti, a prescindere dal luogo in cui sono inviati, trattati o conservati, anche al di fuori dall'UE, come di sovente succede nel mondo informatico e digitale".*

Si rileva, che a seguito dell'uscita della Gran Bretagna dall'Unione europea, ad oggi prevista per il 31 ottobre 2019, il trasferimento di dati personali verso la Gran Bretagna sara` considerato trasferimento verso uno stato terzo. La Gran Bretagna ha adottato il

Data Protection Act 2018 di adattamento al *GDPR*, essendo essa obbligata ad osservare la disciplina europea fino al compimento del processo di *Brexit*[6].

3. La nozione di «stabilimento» e il principio di territorialità

Di rilievo è di certo il dibattito sulle questioni interpretative che si pongono in relazione alle disposizioni della dir. 95/46, che si riferiscono al "*principio di territorialità*" in materia di trattamento dei dati personali. Esso è, infatti, enunciato in relazione alla competenza delle autorità di controllo all'art. 28, co. 6, dir. 95/46. Lo stesso principio affiora dalle disposizioni sull'individuazione della legge applicabile in base al luogo ove si trova lo stabilimento del responsabile del trattamento o alla sussistenza di strumenti finalizzati al trattamento dei dati (arg. dall'art. 4 dir. 95/46). Segnatamente, sul punto si rileva che i giudici europei si sono dimostrati aperti ad un'interpretazione ampia ed estensiva dei criteri territoriali, ampliando i confini della nozione di stabilimento, al fine di osteggiare probabili comportamenti opportunistici da parte degli operatori di servizi *Internet*. Difatti sono diverse le decisioni della Corte di Giustizia dell'Unione europea, che si sono pronunciate sulle problematiche del trattamento transnazionale dei dati in via interpretativa dell'art. 4, 1° co., lett. a della dir. 95/46. In via di principio esse affermano di volersi attenere ad una forte tutela del diritto sui dati personali secondo la protezione ad esso data a livello fondamentale negli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che vengono adottati quale base interpretativa della dir. 95/46. Il ragionamento seguito dai giudici, segna l'evoluzione dei tempi seguendo la realtà attuale dei rapporti economici come si svolgono su

[6] L. VALLE, B. RUSSO, G. BONZAGNI, D. LOCATELLO, *Struttura dei contratti e tutela dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE,* in *Contratto e impresa/Europa, 2018, pp. 344-406. Contratto e impresa/Europa*, 2018 "*Il flusso di dati verso e dalla Gran Bretagna è di primario rilievo considerato che circa il 43% delle società high tech europee hanno sede lı`, e che il 75% dei trasferimenti di dati del Regno Unito avviene tra Paesi dell'Unione europea, ragione per cui il governo del Regno Unito manifesta la volontà di mante-nere tali flussi di dati. Non si può prevedere al momento se, successivamente alla realizzazione dell'uscita della Gran Bretagna dall'Unione europea, l'adesione alla disciplina contenuta nel Reg. 2016/679 verrà in-debolita. Guardando a tale futura prospettiva va in ogni caso tenuto presente che la Gran Bretagna è parte del Consiglio d'Europa, che ha recentemente adottato un Protocollo aggiuntivo della Convenzione n.108, di cui si dirà` oltre in questo par., che ha per obiettivo la libera circolazione dei dati personali tra i Paesi aderenti alla Convenzione"*

Internet, che richiede l'allontanamento da rigorosi riferimenti territoriali per la determinazione della legge applicabile altrattamento dei dati personali. Invero non ha rilievo la cittadinanza degli interessati al trattamento , ovvero il luogo di residenza abituale degli stessi interessati, né l'ubicazione fisica dei dati personali . Viceversa, si punta sulla competenza dell'autorità di controllo in materia di "supervisione" del trattamento dei dati nel territorio dello Stato membro di appartenenza, a cui viene riconosciuta un'estensione territoriale più estesa rispetto a quella definita dall'art. 4 dir. 95/46, valorizzando, al di là dello stabilimento del responsabile del trattamento, ogni elemento in grado di riferire il trattamento dei dati considerato al territorio dello Stato membro di appartenenza.[7] La portata applicativa espansiva alla disciplina europea della tutela dei dati personali, viene espressa nella sentenza Google Spain che tanto risulta in particolare dai considerando da 18 a 20 e dall'art. 4 della dir. 95/46, attraverso i quali il legislatore dell'Unione ha inteso evitare che una persona venga esclusa dalla protezione garantita da tale direttiva e che tale protezione venga elusa (punto 54). La Corte di Giustizia Europea, nella medesima sentenza, afferma che non si può ammettere che il trattamento dei dati personali effettuato per le esigenze del funzionamento del motore di ricerca in questione venga sottratto agli obblighi e alle garanzie previsti dalla dir. 95/46, ciò che pregiudicherebbe l'effetto utile di quest'ultima e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone che detta direttiva mira a garantire (punto 58) . Sta nei fatti che nel caso *Google Spain*, deciso nel 2014, era giunta al vaglio della Corte, l'attività della società *Google Spain*, avente sede in Spagna, ove essa realizzava la promozione e la vendita di spazi pubblicitari che la Corte riconosceva come parte essenziale dell'attività commerciale del gruppo Google. La suddetta attività era individuata come strettamente connessa a quella di Google Search, gestita e amministrata da Google Inc., avente sede negli Stati Uniti. In proposito la Corte rilevava che non fosse contestato che *Google Spain* si dedicava all'esercizio effettivo di un'attività mediante un'organizzazione stabile in Spagna e, essendo dotata di personalità giuridica propria, tale società costituiva una filiale di *Google* Inc. nel territorio spagnolo; e di conseguenza uno «*stabilimento*» ai sensi dell'art. 4, 1° co., lett. a della dir. 95/46. Inoltre riteneva "*che il trattamento dei dati personali realizzato per esigenze di servizio di un motore come Google Search, gestito da un'impresa con sede in uno Stato terzo, ma avente uno stabilimento in uno Stato membro, si possa dire*

[7] Antonino Barletta, cit., *in Europa e Diritto Privato*, 4, 1 dicembre 2017, pag. 1179.

effettuato « nel contesto delle attività » di tale stabilimento, qualora quest'ultimo sia destinato a garantire in tale Stato membro la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo" (punto 55). "*Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio, essendo tale motore al tempo stesso lo strumento che consente lo svolgimento delle attività in questione (punto 56). Concludendo che l'art. 4, 1° co., lett. a non esige che il trattamento di dati personali in questione venga effettuato «dallo » stesso stabilimento interessato, bensì soltanto che venga effettuato, appunto, « nel contesto delle attività » di quest'ultimo, dirigendosi tra l'altro verso gli abitanti di detto Stato membro*"(punto 60). La Corte, ha poi rilevato *che l'attività del motore di ricerca — consistente nella raccolta di dati attraverso l'esplorazione di Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni qui pubblicate che esso « estrae », « registra » e « organizza » successivamente nell'ambito dei suoi programmi di indicizzazione, « conserva » nei suoi server e eventualmente « comunica » e « mette a disposizione » dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche — realizza un « trattamento » dei dati secondo la disposizione dell'art. 2, lett. b della dir. 95/46 che contempla un tale genere di operazioni . E che il motore di ricerca deve essere considerato il titolare di tale trattamento ai sensi dell'art. 2, lett. d della dir. (punto 33). È pacifico — osserva la Corte — che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati in quanto li rende accessibili a qualsiasi utente di Internet che esegua una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina web su cui questi dati sono pubblicati (punto 36). Inoltre, l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet da parte dei motori di ricerca al fine di facilitare ai loro utenti l'accesso a tali informazioni possono avere come effetto che tali utenti, quando la loro ricerca viene eseguita a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente di stabilire un profilo più o meno dettagliato di quest'ultima (punto 37). Pertanto l'attività di un motore di ricerca può incidere in modo significativo sui diritti fondamentali alla vita privata e alla protezione dei dati*

personali, in aggiunta all'attività degli editori dei siti web, e per questo il gestore del motore di ricerca deve assicurare che detta attività soddisfi le prescrizioni della dir. 95/46 affinché possa essere realizzata una tutela efficace e completa delle persone interessate, in particolare del diritto al rispetto della loro vita privata". Infine, la Corte si esprime nel senso che la « visualizzazione stessa di dati personali su una pagina di risultati di una ricerca costituisce un trattamento di dati personali » (punto 57).[8] Anche con il caso Weltimmo deciso nel 2015, la Corte ripropone la questione dello "stabilimento" e afferma che l'art. 4, 1° co., lett. a consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il titolare del trattamento di tali dati è registrato purché quest'ultimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale realizza tale trattamento. La fattispecie riguardava una società "Weltimmo", registrata in Slovenia, che gestiva siti Internet aventi ad oggetto annunci immobiliari relativi ad immobili situati in Ungheria e redatti nella lingua di quest'ultimo Paese, e per la raccolta dei dati personali degli inserzionisti le era stata indirizzata una sanzione dalla Autorità Garante ungherese .In tale caso la Corte sottolinea di nuovo, come già in *Google Spain* che l'art. 4, 1° co., lett. a dir. 95/46 " *non esige che il trattamento di dati personali in questione venga effettuato "dallo" stesso stabilimento interessato, bensì soltanto che venga effettuato "nel contesto delle attività" di quest'ultimo », ciò che conduce al« l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile (n.d.a. leggasi: titolare) del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge il trattamento . Ne consegue, come aveva rilevato l'Avvocato generale nelle sue conclusioni (ai punti 28 e 32-34), una concezione flessibile della nozione di stabilimento che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata."*. Il considerando n. 19 della dir. 2000/31/CE sul commercio elettronico afferma infatti che il luogo di stabilimento per le società che forniscono servizi tramite siti Internet non è là dove si trova la tecnologia di supporto del sito, né dove esso è accessibile, bensì il luogo in cui dette società svolgono la loro attività economica . Nella successiva sentenza Amazon del 2016, il già

[8] Antonino Barletta, cit, in *Europa e Diritto Privato*, 4, 2017, pag. 1179.

citato principio del luogo verso cui è diretta l'attività dell'operatore per la definizione della legge applicabile, (oggetto delle pronunce Google Spain, Weltimmo) la Corte di Giustizia afferma che l'art. 4, 1° co., lett. a della dir. 95/46 dev'essere inteso nel senso che il trattamento dei dati personali eseguito da un'impresa del commercio elettronico sia regolamento dal diritto dello Stato membro verso il quale, la suddetta impresa rivolge le proprie attività, nel caso che sia constatato che tale impresa eserciti il trattamento dei dati in esame, nell'ambito delle attività di uno stabilimento situato in detto Stato membro. "*Il caso si pronuncia sullo schema di contratto per il commercio elettronico della società Amazon EU (con sede in Lussemburgo ed appartenente ad un gruppo internazionale) rispetto alle attività svolte attraverso il sito Internet con dominio amazon.de, e rivolte anche a consumatori residenti in Austria, con riguardo ai profili inerenti alla privacy, alle clausole del trattamento dei dati al fine del recupero crediti e ad altri fini, ed alla determinazione della legge applicabile, definita come quella lussemburghese."* [9]

[9] *Ibidem*: "*A proposito della nozione di « stabilimento » la Corte ripete, in linea con le conclusioni dell'Avvocato generale (par. 119) e come già affermato nel caso Weltimmo, che, sebbene l'impresa titolare del trattamento non possieda né filiali né succursali in uno Stato membro, ciò non esclude che essa possa ivi possedere uno stabilimento ai sensi dell'articolo sopra detto (punto 79), e che la nozione di stabilimento si estenda a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile (punto 75, richiamando la decisione Weltimmo, punto 31). Mentre, d'altra parte, uno stabilimento non può esistere per il semplice fatto che ivi sia accessibile il sito Internet dell'impresa in questione (punto 76), e che occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività nello Stato membro interessato (punto 77, che richiama la decisione Weltimmo, punto 29). Allo stesso tempo, come già affermato in precedenza, la Corte ripete che non occorre che il trattamento dei dati personali in questione venga effettuato «dallo » stabilimento interessato stesso, bensì soltanto « nel contesto delle attività » di quest'ultimo. Allo stesso modo che nella decisione Weltimmo, e prima ancora nella decisione Google Spain, la Corte — come detto sopra — mette l'accento sul luogo verso il quale è diretta l'attività dell'operatore per farne derivare la determinazione del diritto applicabile. Con ciò si apre la possibilità di associare alla tutela dei dati personali del consumatore parte di un contratto di fornitura di beni e servizi secondo la disciplina di tutela dei dati personali del suo Paese di residenza (se ed in quanto in tale Paese l'operatore esegua il trattamento dei dati nel contesto delle sue attività) la disciplina del contratto secondo le norme imperative di regolazione del contratto del consumatore del suo Paese di residenza, così come prevede il Regolamento Roma I al suo art. 6, 2° co., se il consumatore venga qui "raggiunto" dall'operatore commerciale attraverso lo svolgimento delle sue attività .In conclusione, dalle decisioni della Corte di Giustizia emergono diverse linee interpretative dell'art. 4, 1° co., lett. a della dir. 95/46 che si concentrano sia sulla nozione di stabilimento che sulla nozione di trattamento dei dati, con i seguenti profili di rilevanza applicativa. Quanto alla nozione di « stabilimento », una sua nozione svincolata dal contesto territoriale della registrazione dell'operatore in un determinato Stato membro, e legata al luogo dello svolgimento effettivo delle attività dell'operatore o alla presenza di un rappresentante; e una sua nozione che ricomprende non soltanto le operazioni svolte direttamente dall'operatore, ma anche le operazioni che si svolgono « nel contesto » delle attività dell'operatore; che tiene conto anche della loro natura di attività che vengono realizzate tramite Internet; che tiene conto anche del luogo verso il quale si indirizzano le attività, se sia quello di uno Stato membro e di quale Stato membro, e in quest'ottica della lingua nella quale si svolgono. Quanto alla nozione di « trattamento » dei dati, una sua nozione che considera trattamento dei dati l'attività del motore di ricerca consistente nella raccolta di dati attraverso l'esplorazione di Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni qui pubblicate, e la « visualizzazione stessa di dati personali su una pagina di risultati di una ricerca ». Ne*

4. La sentenza Privacy Shield per il trasferimento dei dati negli Stati Uniti

Particolarmente importante riveste il trasferimento transnazionale dei dati nei rapporti Europa-USA per ragioni legate all'importanza degli operatori online aventi sede negli Stati Uniti. In argomento con una decisione di adeguatezza del 2000, la Commissione europea aveva "*ratificato*" il c.d. accordo politico ed economico denominato " *Safe Harbour",* che disciplinava i rapporti tra Europa e Stati Uniti, nell'ambito del trattamento dei dati personali, riconoscendo come legittimi e consentendo liberamente i trasferimenti di dati tra Paesi membri dell'Unione europea e gli USA. Si ricorda che tale patto, fu il frutto di un negoziato tra la Commissione Europea e e il Department of Commerce statunitense condotto tra la fine del 1998 e il 2000, ed è di fatto l'accettazione, ad opera dell'Unione europea di un indebolimento della propria posizione sul principio di adeguatezza, attraverso un approccio del tutto eccezionale in favore delle imprese statunitensi che non ha pari nei rapporti con gli altri Paesi terzi. L'adesione delle imprese ai principi di Safe Harbour avveniva su base volontaria e attraverso una forma di autocertificazione, prevedendosi appropriati meccanismi di controllo e di enforcement a garanzia del rispetto di una protezione « adeguata ».

Tale accordo rappresentava, dunque una posizione di compromesso con l'impostazione della tutela della privacy nella disciplina normativa degli USA, meno protettiva rispetto al modello europeo, che trovava nei fatti le sue ragioni negli interessi commerciali, grazie ai quali si erano fatte speciali concessioni alle imprese statunitensi.

Tuttavia la predetta decisione della Commissione di riconoscimento dell'accordo di *Safe Harbour* sul flusso transfrontaliero dei dati tra Unione europea e Stati Uniti, ritenendolo « adeguato » alla luce dell'art. 25 della dir. 96/45, quale livello di prote-

consegue in definitiva un rafforzamento della portata protettiva del diritto sui propri dati personali della disciplina europea di cui alla dir. 95/46 ed un ampliamento della sua portata applicativa."

zione garantito dalla disciplina degli USA, è stata, poi invalidata dalla Corte di Giustizia dell'Unione europea con la decisione *Schrems*[10] dell'ottobre del 2015.[11] Con tale decisione, è stato confermato che il trattamento posto in essere dalle autorità statunitensi per i fini di sicurezza nazionale, invero violava i principi di necessità e proporzionalità cui è soggetto il trattamento dei dati nella disciplina europea, e che gli interessati dal trattamento dei dati non godevano di un'effettiva tutela amministrativa o giudiziaria quanto ai diritti inerenti al trattamento dei loro dati. Questo ha comportato come conseguenza, che non sussistevano più i presupposti legali idonei a legittimare il trasferimento dei dati verso gli USA. Va da sé che è stato così elaborato il *Privacy Shield*, ossia un accordo frutto del negoziato tra la Commissione europea e il Governo USA, formalmente adottato dalla Commissione Ue il 12 luglio 2016, designato a succedere all'accordo di Safe Harbour per disciplinare la tutela della privacy nei rapporti Europa — USA . Per l'effetto, a partire dal 1° agosto 2016, le imprese possono certificarsi come aderenti al Privacy Shield, presso il Dipartimento del commercio degli Stati Uniti .

Il Privacy Shield impone obblighi severi per le imprese statunitensi che importano dati personali dall'Europa quanto al trattamento dei dati e alla protezione dei dati personali. Difatti, le imprese sono anche sottoposte ad un rigido controllo, proprio per

---

[10] M. MANDICO, *Numero monografico sul Regolamento Europeo UE 2016/679*, in Diritto ed Economia dei mezzi di Comunicazione – numero 2/3. 2017-2018 *"La sentenza Schrems, ha segnato il momento del cambiamento nel contesto del trasferimento di dati verso gli Stati Uniti. Sta nei fatti che i giudici di Lussemburgo hanno sconquassato l'inattività delle contrattazioni tra Unione europea e Stati Uniti, dando, in tal modo, la spintafondamentale per cambiare l'impiantoSafe Harbor. Il successivo sistema denominato Privacy Shield è stato, innanzitutto, predisposto per decifrare e risolvere le criticità che sono appunto emerse dalla decisione Schrems, sebbenepresenti comunquesvariati elementi di fragilità e debolezza. Le speranze e ibisogni degli europei sono accresciuti in conseguenza dello scandalo delle confessioni sui piani dell'intelligence statunitense e sull'impronta della decisione della Corte di Giustizia. Resta comunque, sempre vivo ed attuale il problema di come poter bilanciare, da un lato laprotezione dei dati e dall'atro laavanzamento della circolazione dei dati personali e il mercato digitale e non.Segnatamente ad oggi, non sono numerosi i paesi e le organizzazioni che, hanno ricevuto dalla Commissione europea, la valutazione positiva di adeguatezza ai canoni di protezione posti a tutela delle persone fisiche interessate .Di seguito sono riportate le decisioni della Commissione sinora pubblicate in materia di adeguatezza di Paesi terzi: - Andorra; Argentina; Australia – PNR; Canada; FaerOer; Guernsey; Isola di Man; Israele; Jersey; Nuova Zelanda; Svizzera; Uruguay ".*

[11] Antonino Barletta, cit., *in Europa e Diritto Privato*, 4, 1 dicembre 2017, pag. 1179.: "*Corte Giust. Ue, 6 ottobre 2015, causa C-362/15, Schrems c. Data Protection Commissioner, Digital Rights Ireland Ltd. Il caso aveva avuto origine dalricorso di un cittadino austriaco, Max Schrems, contro Facebook in Irlanda — dove la società ha la sua sede europea — che lamentava la mancanza di un adeguato livello di protezione dei dati personali inviati da Facebook negli USA in ragione dell'accesso indiscriminato che la National Security Agency (NSA) statunitense aveva sui dati inviati da Facebook verso i server situati in territorio statunitense. La High Court of Ireland, presso la quale era stato portato il ricorso contro la decisione dell'Autorità per la protezione dei dati personali irlandese che si era basata sull'accordo di Safe Harbour, aveva rilevato i dubbi sull'adeguatezza del sistema di protezione offerto dagli USA e sollevato la questione pregiudiziale di fronte alla Corte di Giustizia Ue".*

rendere effettivi gli obblighi. Inoltre il Dipartimento del Commercio statunitense, sottopone a verifiche ed aggiornamenti periodici, le imprese aderenti allo "scudo," al fine di monitorare ed accertare che essi rispettino nella pratica le regole che hanno volontariamente accettato . Pertanto, in caso di inadempimenti o di violazioni degli obblighi in questione, l'impresa si espone a sanzioni e alla cancellazione dall'elenco degli aderenti. Ulteriore profilo del Privacy Shield, riguarda la protezione effettiva dei diritti dei cittadini europei attraverso maggiori possibilità di ricorso a rimedi. Segnatamente sono infatti previsti diversi meccanismi di composizione delle controversie alternativi di risoluzione, per garantire una tutela effettiva dei diritti individuali, al fine di assicurare a chiunque ritenga di aver subito un abuso sui dati che lo riguardano che ricada nel contesto del Privacy Shield di avere a disposizione diversi meccanismi di composizione delle controversie, di agevole accesso e dal costo contenuto. Va poi rilevato che lo strumento del Privacy Shield viene poi sottoposto, per il buon funzionamento dello stesso, ad un continuo monitoraggio attraverso un riesame annuale.

5. Il trasferimento dei dati transfrontalieri come da Regolamento 679/16. Un nuovo modello.

In materia di trasferimento dei dati personali all'estero fuori dall'Unione europea, in confronto alla precedente direttiva, per quanto riguarda i principi, continuano a permeare lo spirito alla base dell'impianto normativo del *GDPR*, che però è molto più dettagliato nella regolamentazione del trasferimento dei dati, difatti si pensi che la direttiva 96/45, riservava a tale tema solo due norme, gli artt. 25-26, mentre il nuovo codice *privacy* 679/16, vi dedica un'approfondita attenzione con l'intero Capo V e gli artt. 44-50**.** Proprio l'art. 44 rappresenta l'esempio lampante dei vincoli imposti dal Regolamento in termini di tutela dei dati personali.

Il Regolamento è nato dalla necessità di assicurare un'armonizzazione completa a livello europeo in materia di protezione dei dati personali, con l'intento del legislatore di avere una disciplina effettivamente comune a tutti i Paesi membri dell'Unione europea, salvo che per quei profili che il Regolamento lascia all'iniziativa dei singoli Stati membri disciplinare diversamente.[12] Quanto ai profili di rafforzamento dei diritti

[12] *La discrezionalità concessa agli Stati membri ha un rilievo tale da impedire di « procedere ad un commento strutturato ed esaustivo della nuova regolazione, che illustri adeguatamente agli utenti il quadro normativo complessivo, anche tenendo conto, caso per caso, delle diverse regolazioni nazionali » fino a quando non saranno adottate le norme statali attuative e i provvedimenti di organizzazione delle Autorità nazionali, ciò che è obbligatorio fare entro il 25 maggio 2018*, Pizzetti, Privacy e il diritto europeo alla protezione dei dati personali, II, Torino, Giappichelli, 2016, p. X. *Volendo assicurare «un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano*

della persona, il Regolamento attribuisce al soggetto interessata una maggiore consapevolezza rispetto al trattamento dei dati che la riguardano, offrendo vari strumenti di rivelazione della trasparenza più elevati rispetto alla dir. 95/46, dato che agli interessati devono essere forniti nuovi elementi di conoscenza, relativi al trattamento, al fine di garantire che questi siano posti nelle condizioni di essere realmente consapevoli di quale sia la logica utilizzata nel trattamento dei propri dati. Sul punto si osserva che la definizione di dato personale si estende fino ad includere i dati sulla ubicazione e gli identificativi online (art. 4 n. 1); inoltre tra le "categorie particolari di dati personali" sono ricompresi i dati genetici e biometrici (art. 9). La tutela dell'interessato si evince anche dalle condizioni per il consenso previste dal Regolamento: il consenso al trattamento dei dati deve essere dato attraverso un atto positivo inequivocabile che può consistere ad esempio in una dichiarazione scritta, anche attraverso mezzi elettronici, o orale (mentre il silenzio o le caselle preselezionate non sono più sufficienti a rappresentare il consenso) (art. 7).

"*Nella recente comunicazione della Commissione europea del gennaio 2017 "Building a European Data Economy" il nuovo Regolamento fa da base alla disciplina del trattamento dei dati personali, che è concepita dalle istituzioni europee come in piena evoluzione. Al fine della costruzione di una data economy (che inerisce all'impatto complessivo del mercato dei dati sull'economia nel suo insieme; essa concerne la generazione, la raccolta, la conservazione, la distribuzione, l'analisi, l'elaborazione, la consegna e l'utilizzazione dei dati consentita dalle tecnologie digitali), la*

ostacolare la libera circolazione dei dati personali nel mercato interno » e garantire certezza del diritto e una tutela dei dati personali uniforme in tutti gli Stati dell'Unione (considerando 13) il Regolamento è costretto a fare i conti anche con le differenze economiche e culturali che caratterizzano i diversi Paesi e i loro ordinamenti (p. 18). In alcuni casi esso rimette agli Stati di regolare soltanto profili "interstiziali" di norme specifiche relative alla tutela di aspetti circoscritti degli istituti disciplinati. A volte la normativa statale è essenziale per l'attuazione del Regolamento, altre volte il potere regolatorio statale è essenzialmente facoltativo ma, se esercitato, integra le disposizioni del Regolamento con norme stabilite dalla legislazione nazionale (p. 17). È infatti lasciata agli Stati membri la libertà, ad esempio, di stabilire le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito (considerando n. 10); o ancora, gli Stati membri possono altresì prevedere ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei dati genetici, biometrici o quelli relativi alla salute (art. 9, 4° co.). Ancora, in via esemplificativa, è concesso agli Stati membri di prescrivere che i titolari del trattamento consultino l'autorità di controllo e ne ottengano l'autorizzazione preliminare in relazione al trattamento per l'esecuzione di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (art. 36, 5° co.).In quest'ottica, vi sono molte disposizioni del Regolamento che richiedono agli Stati membri e alle Autorità di protezione dei dati chiarimenti ed integrazioni prima di poter essere attuate, ciò che consente il costante aggiornamento in linea con lo sviluppo della tecnologia e della realtà. V. Intervento di Giuseppe Busia, Segretario generale del Garante per la protezione dei dati personali, pp. 1-2, cit., infra, nota 95.

Commissione pone l'attenzione sulla necessità di un quadro di policy che consenta l'uso dei dati su tutta la catena del valore per scopi scientifici, sociali e industriali ed in particolare sulla necessità che il flusso dei dati all'interno dell'Unione europea sia consentito e protetto, dato che un flusso dei dati libero, sicuro e affidabile è strumentale alla protezione delle quattro libertà fondamentali del mercato unico europeo previste dai Trattati (COM(2017) 9 final, 10 gennaio 2017, aprendo ad una pubblica consultazione sulla materia). Contestualmente viene proposta la revisione della dir. 2002/58 sul trattamento dei dati personali e sulla tutela della vita privata nelle comunicazioni elettroniche attraverso un nuovo Regolamento al fine di assicurare un elevato livello di protezione in coerenza con il Reg. 2016/679 (COM(2017) 10 final, 10 gennaio 2017, che contiene appunto una proposta di Regolamento)".[13]

Con il nuovo modello di regolamentazione del trattamento dei dati personali, il legislatore europeo ha provveduto a modificare l'ambito di applicazione territoriale della normativa,[14] recependo integralmente gli orientamenti delineatisi nella giurisprudenza della Corte di Giustizia Ue (soprattutto a partire dalla sentenza Google Spain), che mirano ad applicare la disciplina europea di tutela dei dati personali anche nei confronti di titolari non europei e, per i cittadini europei.[15] Infatti, il Regolamento cambia il tradizionale principio di stabilimento, sancendo al suo art. 3 l'applicabilità della disciplina da questo dettata "*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione "* e prevedendo l'applicazione della normativa anche a titolari e responsabili non stabiliti nell'Unione europea, quando l'attività di trattamento riguardi:

[13] Antonino Barletta, cit., *in Europa e Diritto Privato*, 4, 1 dicembre 2017, pag. 1179.

[14] Per approfondimenti: KOTSCHY, *The proposal for a new General Data Protection Regulation — problems solved?,* in *International Data Privacy Law*, IV/2014, pp. 274-281.

[15]A. BARLETTA cit: "*Si è quindi fatta strada nel tempo una volontà riformatoria del criterio di applicazione territoriale della normativa europea i cui primi segnali si possono rintracciare nel Parere espresso dal Gruppo Art. 29 nel dicembre del 2010, ove per la prima volta viene esaminata la nozione di "contesto delle attività" e vengono suggerite alcune possibili soluzioni al trattamento effettuato da titolari situati al di fuori dei confini europei. In realtà già tempo prima, nel gennaio 2010, con lo "Studio comparativo dei diversi approcci alle nuove sfide della privacy, in particolare alla luce degli sviluppi tecnologici" la stessa Commissione europea aveva palesato delle remore circa l'ambiguità e la contrastante attuazione delle disposizioni della direttiva sul diritto applicabile, raccomandando «regole migliori, più chiare e univoche sul diritto applicabile» . A tale studio aveva fatto poi seguito una comunicazione del novembre 2010, ove la Commissione evidenziava la necessità di « rivedere e chiarire le disposizioni vigenti in materia di diritto applicabile, compresi gli attuali criteri determinanti, al fine di migliorare la certezza giuridica, di chiarire le competenze degli Stati membri nell'applicare le norme di protezione dei dati e di garantire lo stesso livello di protezione alle persone residenti nell'UE, a prescindere dalla localizzazione geografica dal responsabile del trattamento».*

a) l'offerta di beni o la prestazione di servizi a soggetti interessati che si trovano nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure,

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione (art. 3, 1° e 2° co. del Regolamento). In proposito il considerando n. 23 recita che " *onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione ".* Il nuovo Regolamento a tutela dei dati personali, sarà applicato, inoltre non solo ai trattamenti effettuati nell'ambito delle attività di uno stabilimento del titolare situato nell'Unione, ma anche nel caso in cui si tratti di uno stabilimento del responsabile. Sul punto secondo quanto statuito dal 3° co. dell'art. 3 del Regolamento, la disciplina europea si applica tra l'altro anche ai titolari non stabiliti nell'Unione ma sottoposti alla legge nazionale di uno Stato membro in virtù del diritto pubblico internazionale. Tale disposizione non ha carattere innovativo in quanto riproduce la clausola già presente nella dir. 95/46 all'art. 4, lett. b.

A differenza della Direttiva 46/95/CE, il GPDR non contiene una definizione di "*trasferimento*". Deve, comunque, ritenersi che esso sussista ogniqualvolta un dato personale sia materialmente trasferito al di fuori dello spazio economico europeo. La

dottrina, inoltre, pare unanime nel considerare che, il mero transito di dati personali su strumenti non fisicamente presenti nel territorio dell'Unione, non integri un'ipotesi di trasferimento, anche alla luce del dato letterale dell'art. 44 del *GDPR*.

Il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è dunque vietato, in linea di principio (articolo 25, comma 1, della Direttiva 95/46/CE), a meno che il paese in questione garantisca un livello di protezione "*adeguato*"; la Commissione ha il potere di stabilire tale adeguatezza attraverso una specifica decisione (articolo 25, comma 6, della Direttiva 95/46/CE).

In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall´articolo 26, comma 1, della Direttiva 95/46 :

- consenso della persona interessata;
- necessità del trasferimento ai fini di misure contrattuali/precontrattuali;
- interesse pubblico preminente, ecc.;
- nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46).

La novità più rilevante in materia, rispetto alla direttiva, concerne proprio la specificazione delle c.d. "garanzie adeguate " (di cui già all'art. 26, 2° co. dir. 95/46 come " garanzie sufficienti "), sulla base delle quali un titolare o un responsabile può trasferire dati personali verso un Paese terzo od un'organizzazione internazionale in assenza di una decisione di adeguatezza (art. 46).

Ciò detto, è evidente che il regolamento prosegue nell'approccio attualmente vigente per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo[16], stabilendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

i) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

[16] Si veda la Scheda informativa Mercato unico digitale – Comunicazione sullo scambio e la protezione dei dati personali in un mondo globalizzato Domande e risposte della Commissione Europea del 10 gennaio 2017.

ii) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);

iii) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

In tali ipotesi, la Commissione UE, si pronuncia positivamente circa il fatto che un *"paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o un'organizzazione internazionale*" garantiscono un livello di protezione adeguato dei dati trasferiti con l'effetto che, solo in casi del genere, non siano necessarie specifiche autorizzazioni (art. 45.1 GDPR). Sinora la Commissione UE ha pubblicato le decisioni in materia di adeguatezza nei confronti dei seguenti paesi: Andorra, Argentina, Australia – PNR, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay.

Ognuna di queste diverse fattispecie serve per regolare i trasferimenti internazionali di dati verso paesi terzi che avvengono però in circostanze diverse. Soprattutto nei contesti dei trasferimenti non basati su decisioni di adeguatezza, dunque per trasferimenti che devono essere soggetti a garanzie adeguate o che avvengono sulla base delle BCR, sono di fondamentale importanza le clausole che gli operatori dei dati (titolari e responsabili) utilizzino nei contratti con i quali si definiscono i termini dei loro rapporti e, soprattutto, i termini che definiscono la "allocazione" delle rispettive responsabilità. Sul trasferimento dei dati personali va anche ad incidere il principio dell'*accountability* introdotto dal Reg. 2016/679 in quanto titolare e responsabile del trattamento hanno la responsabilità di provare che il trasferimento sia avvenuto in conformità alle disposizioni del Regolamento. L'art. 30 prevede che le attività di trasferimento dei dati personali sono incluse tra le informazioni che titolare e responsabile devono inserire.

"L'art. 44 del GDPR statuisce che i trasferimenti di dati personali al di fuori del SEE sono ammessi solo in determinate circostanze: "Articolo 44 - Principio generale per il trasferimento (C101, C102). Qualunque trasferimento di dati personali oggetto di un trattamento o 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, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di

cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato." Il regolamento individua due categorie di destinatari in relazione a tale disciplina: gli altri paesi e le organizzazioni internazionali (si pensi all'ONU, l'Unesco, a titolo esemplificativo ma non esaustivo). Il trasferimento di dati personali al di fuori dello Spazio SEE è lecito:

1) se il destinatario garantisce un livello di protezione dei dati adeguato a quello europeo. Il requisito dell'adeguatezza, che si basa sulla "decisione di adeguatezza", permette l'utilizzo di disparatedirezioni per assicurare la protezione dei dati;

2) quando il trasferimento è soggetto a garanzie adeguate;

3) altri casi di legittimo trasferimento dati all'estero.

- Decisioni di adeguatezza: una prima ipotesi in cui è ammesso ed è legittimo il trasferimento di dati all'estero, si verifica quando, il paese terzo, il territorio, uno o più settori specifici all'interno del paese extra UE,o l'organizzazione internazionale del caso, riescono ad ottenere il benestare della Commissione Europea, che con una pronuncia positiva, "una decisione di adeguatezza", riconosce le garanzie per un livello di protezione dei dati adeguato a quello europeo. Il Gruppo di lavoro articolo 29 con Parere 01/2012 aveva osservato che "il regolamento agevola i responsabili del trattamento mediante la previsione di varie zone di sicurezza (Safe Harbour) nella forma di decisioni di adeguatezza, di un sistema semplificato di norme vincolanti d'impresa per le multinazionali, di clausole contrattuali approvate e di approvazioni individuali da parte dell'autorità di protezione dei dati". Invero la Commissione europea, esaminato l'impianto normativo, del paese terzo o dell'organizzazione internazionale, può decidere, che lo stesso possa fornire un'adeguata tutela ai dati che vi sono trasferiti, in tal caso verrà presa una decisione di adeguatezza (art. 45 GDPR), o eventualmente potrà indicare le necessarie modifiche alla legislazione, per giungere ad un accordo. La Commissione per potersi pronunciare, deve preventivamente valutare ed accertare che il paese terzo, o l'organizzazione internazionale del caso, garantiscano un livello di protezione appropriato e conforme agli standard del Reg. 679/16. Il Regolamento indica i parametri per valutare l'adeguatezza del paese terzo. Innanzitutto occorre esaminare diversi aspetti del trattamento: la natura dei dati, la finalità del trattamento, la possibilità che tali dati transitino in altri paesi prima di giungere alla destinazione, le norme di diritto anche settoriali, le misure di sicurezza osservate.

L'European Data Protection Board, ha il compito di fornire un parere alla Commissione. Le decisioni di adeguatezza, sono strumenti vincolanti per i paesi dell'Unione, e in base ad esse è ammesso il trasferimento di dati verso il paese indicato. La decisione viene adottata sulla base dei parametri che sono esplicitati all'art. 45 II comma:

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

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

c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali."

Va rilevato che in tali casi la Commissione potrà adottare atti di esecuzione che disciplinano il trasferimento dei dati verso il paese terzo, o lo specifico territorio o più settori specifici all'interno di un paese o di un'organizzazione internazionale, senza la necessità di ulteriori autorizzazioni; per cui il trasferimento sarà più semplice e i soggetti coinvolti saranno esonerati da ulteriori adempimenti, stante il preventivo controllo della Commissione, è ovvio che i paesi terzi o organizzazioni internazionali, dovranno aderire e adeguarsi alle procedure stabilite. Il nuovo regolamento, stabilisce che anche quando vi sono stati atti di esecuzione, la Commissione è tenuta a controllare in modo costante e ripetuto la sicurezza accordata ai dati dei cittadini, pertanto gli sviluppi e le evoluzioni dei paesi terzi o delle organizzazioni internazionali

vanno verificati dalla Commissione, che dovrà monitorare lo stato di adeguatezza degli strumenti di protezione dei dati, aggiornando di volta in volta il giudizio valutativo. Difatti lo stesso articolo 45 al comma III, stabilisce che "La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2. " Sulla medesima scia prosegue il comma 4 dell'art. 45, che attribuisce alla Commissione, il compito di controllare, in modo continuativo, gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate fino ad arrivare ad una loro modifica o revisione. Difatti questo aspetto viene ancor meglio precisato nel successivo quinto comma, che appunto dispone che nel caso in cui si verifichino le indicate circostanze, la Commissione potrà decidere di revocare, modificare o sospendere, la precedente decisione, il tutto mediante atti di esecuzione senza effetto retroattivo; in ogni caso sono anche possibili le rinegoziazioni di accordi che sono venuti a cadere. Si ricorda la sentenza del 6 ottobre 2015,(già citata in precedenza) con cui la Corte di Giustizia europea ha invalidato la decisione di adeguatezza relativa al trasferimento di dati negli Usa (cosiddetto Safe Harbour), tuttavia, come sopra detto, da agosto 2016 è operativo il Privacy Shield, recepito in Italia con provvedimento dell'Autorità per la protezione dei dati personali e utilizzato dalla Commissione europea in sostituzione."[17] Va rilevato che mentre l'art. 26, 2° co. della dir. 95/46 menzionava nello specifico le sole "clausole contrattuali appropriate", ora il Regolamento inserisce tra gli strumenti di garanzia adeguata anche le *Binding Corporate Rules*, o norme vincolanti d'impresa, i codici di condotta, i meccanismi di certificazione, le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il

[17] Cit M. MANDICO, *Numero monografico sul Regolamento Europeo UE 2016/679,* in *Diritto ed Economia dei mezzi di Comunicazione*, 2/3. 2017-2018.

titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale, e le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati . Sul punto, si ricorda che ai sensi dell'art. 46, 2° e 3° co. del Regolamento, solo le norme vincolanti d'impresa, le clausole tipo (sia quelle adottate dalla Commissione sia quelle dell'Autorità di supervisione), i codici di condotta e i meccanismi di certificazione, rappresentano garanzie adeguate, senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo. Le restanti "garanzie" devono invece essere sottoposte alla valutazione dell'autorità di controllo. Tra i requisiti minimi previsti per le *Binding Corporate Rules*, si indicano l'indicazione della struttura organizzativa del gruppo imprenditoriale, i trasferimenti di dati previsti, le regole che l'organizzazione ritiene giuridicamente vincolanti, la dichiarazione di come l'organizzazione intende applicare i principi base di protezione dei dati personali, i diritti dei soggetti interessati, il riconoscimento di potenziali responsabilità per qualunque violazione delle norme vincolanti d'impresa, il monitoraggio interno rispetto alla *compliance*, la comunicazione con i soggetti interessati e la cooperazione con i regolatori (art. 47). All'art. 48, viene inoltre prevista l'ipotesi che un trasferimento di dati possa avvenire sulla base delle sentenze di un'autorità giurisdizionale e delle decisioni di un'autorità amministrativa di un Paese terzo, purché basate su un accordo internazionale in vigore tra il Paese terzo richiedente e l'Unione o un suo Stato membro, e fatti salvi gli altri presupposti di trasferimento. Il successivo articolo 49 del Regolamento, prevede invece le fattispecie che riguardano le deroghe in virtù delle quali è legittimo il trasferimento dei dati, anche in mancanza dei presupposti sinora menzionati, disposizione che riproduce pressoché fedelmente le deroghe già previste dalla dir. 95/46 all'art. 26 (secondo quanto si è visto sopra al par. 3). In proposito, va detto che in assenza dei presupposti di legittimità e delle deroghe per il trasferimento dei dati, questo possa ugualmente avvenire " *se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali "* (1° co., ult. par.). Il Capo V del Regolamento dedicato ai trasferimenti di dati personali all'estero si conclude con una disposizione di grande rilevanza, in quanto prevede una serie di

misure volte ad incoraggiare la collaborazione internazionale per la protezione dei dati personali, e cioè dirette a incrementare meccanismi di collaborazione internazionale, prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, coinvolgere le parti interessate in discussioni ed attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali, promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali (art. 50).

DAL REGISTRO PUBBLICO DELLE OPPOSIZIONI ALLA LEGGE 11 GENNAIO 2018 N. 5.

Di Francesco Lo Chiatto

SOMMARIO. 1. Premessa: che cosa è il telemarketing. 2. Il Registro delle Opposizioni. 3. La legge 5/2018. 4. Conclusioni: dalla teoria alla pratica.

Law 178/2010 estabilishes the Public Register of Oppositions for the protection of consumer privacy and indicates its functioning by outlining the main figures of reference, engaged in marketing activities such as: subscriber, operator, manager. Changes to the D.P.R.178/2010 occurred with Law 149/2018, which extends the consultation of the Registry also to paper mail. Law 5 of 2018 sets new provisions regarding the registration and functioning of the RPO, and establishes a national prefix for telephone calls and extends the obligations for operators to consult registers monthly and before each promotional campaign.

1. Premessa: che cosa è il telemarketing

Il telemarketing o televendita è una pubblicizzazione telefonica di beni e servizi commerciali, da parte di una o più aziende consociate, che si svolge nell'ambito di un Call Center, mediante le specifiche modalità di outbound e inbound. Nel primo caso il contatto telefonico avviene fra cliente e operatore, che contatta, uno o più utenti, mediante una serie di liste di numeri telefonici, usualmente forniti dall'azienda; nel secondo caso, invece, le telefonate, giungono al Call Center direttamente dal cliente, mediante la composizione di un numero verde.

Diversi sono gli strumenti di lavoro, degli operatori telefonici, di particolare importanza è lo script, che determina il testo della telefonata, mediante una serie di domande rivolte al cliente, tale da favorire l'interesse potenziale dello stesso, per la campagna di marketing, con la fase conclusiva che dà luogo al consenso esplicito dello stesso.

La normativa in tal senso non sempre è stata chiara, perché è passata da una fase restrittiva, quando si potevano contattare solo i soggetti che avevano fornito il loro esplicito assenso, a una fase di liberalizzazione, tramite l'autorizzazione alle chiamate

pubblicitarie, anche senza il consenso dell'utente, in deroga alle norme sulla privacy fino al 31 dicembre 2009, introdotto dal Decreto mille proroghe. [18]

Questa situazione ha dato luogo per tutti coloro come consumatori, persone giuridiche enti o associazioni, che non gradivano ricevere telefonate per scopi commerciali o di ricerche di mercato di usufruire del servizio pubblico di iscrizione nel Registro dell'Opposizioni istituito con il D.P.R. 178/2010, gestito su delega del Ministero dello Sviluppo Economico, dalla Fondazione Ugo Bordoni, (FUB) che rappresenta un ente terzo indipendente e impegnato in attività di pubblico interesse.

Gli abbonati o "contraenti", secondo una nuova dicitura legislativa i nominativi e numeri dei quali si trovano in elenco, che non desiderano ricevere telefonate pubblicitarie possono iscriversi in maniera gratuita al Registro Pubblico dell'Opposizioni, e richiedere l'aggiornamento dei dati e la revoca dello stesso, in qualsiasi momento. Vi sono quattro modi per opporsi alle telefonate pubblicitarie rivolgendosi al Gestore del Registro Pubblico delle Opposizioni che si attuano mediante utilizzo del web o compilazione di un modulo elettronico; del telefono con la chiamata al numero verde; oppure per posta elettronica; o nel modo più classico di una specifica raccomandata.

L'operatore di telemarketing, che utilizza i dati presenti negli elenchi telefonici pubblici è tenuto, pertanto, a verificare con l'RPO, le liste dei potenziali contatti, tramite una serie di servizi disponibili sul sito, per non incorrere nelle sanzioni per la violazione del diritto di opposizione degli utenti, per la mancata osservanza del R.P.O., come all'art.83 par.5, del Regolamento Generale sulla Protezione dei dati dell'UE 2016/679. In particolare, viene previsto in tal caso l'applicazione di sanzioni amministrative pecuniarie, fino a 20.000.000 di euro o per le imprese al 4% del fatturato mondiale totale annuo dell'esercizio precedente, come da recenti casi internazionali e transnazionali.[19]

2. Registro pubblico delle opposizioni.

Il Registro Pubblico delle Opposizioni istituito con il D.P.R. 178/2010 e aggiornato con il D.P.R. 149/2018 è un servizio gratuito per l'utente che permette di opporsi all'utilizzo per finalità pubblicitarie dei numeri di telefono di cui si è intestatari e dei corrispondenti indirizzi postali associati, presenti negli elenchi pubblici da parte degli operatori che svolgono attività di marketing. L'opposizione, tuttavia, non annulla la

[18] Cfr. *https://it.wikipedia.org/wiki/Telemarketing.*

[19] Cfr. *http://www.registrodelleopposizioni.it/.*

validità dei consensi per contatti con finalità commerciali rilasciati direttamente dagli utenti alle singole società, fermo restando il diritto di opposizione di cui all'art.21 del regolamento UE 679/2016. Nel panorama della tutela del consumatore risulta di fondamentale importanza la legge 178/2010 perché istituisce Registro Pubblico delle Opposizioni, ne indica il funzionamento e delinea le principali figure di riferimento impegnate in attività di marketing quali: abbonato, operatore, gestore. Evidenzia inoltre, all'art.11 l'importanza di specifiche campagne informative atte a favorire la piena conoscenza delle modalità di opposizione al trattamento di dati per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale. Importanti modifiche al D.P.R. 178/2010 si sono avute con la legge 149/2018 prevedendo nuove regole riguardo all'impiego della posta cartacea. Per tale motivo, ogni operatore che intenda effettuare il trattamento dei dati di contatto dei consumatori per fini di invio di materiale pubblicitario di vendita diretta per il compimento di ricerca di mercato sia mediante l'impiego del telefono che della posta cartacea sarà obbligata alla preventiva consultazione del Registro delle Opposizioni, al fine di verificare se è stato espresso un dissenso da parte degli intestatari dei dati di contatto alla recezione di pubblicità, vendite o sondaggi.

A seguito della modifica dell'art.7 del D.P.R. 178/2010, ciascun abbonato può chiedere gratuitamente al gestore che la propria numerazione sia scritta nel registro delle opposizioni, dal 4 febbraio 2019 anche l'iscrizione del corrispondente indirizzo postale di cui risulta intestatario sempre secondo le consuete modalità. Su di una linea di continuità con la tutela dei propri dati si pone la legge 5/2018 che riguarda l'ambito di applicazione del RPO a tutti i numeri riservati inclusi i cellulari.

3. La Legge 5/2018.

Il 4 febbraio 2018 è entrata in vigore la legge n. 5 contenente sia le nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni, sia l'istituzione di un prefisso nazionale per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato.

Il predetto testo di legge non solo estende in maniera considerevole l'operatività del registro pubblico delle opposizioni,di cui all'art.3 del D.P.R. n. 7 2010, n.178, ma amplia gli obblighi per gli operatori che svolgono attività di call center verso numerazioni nazionali fisse o mobili.

L'art.1 dopo aver disposto il rinvio alle norme contenute nell'art.4 del D.lgs. 30 giugno 2003, n. 196 (c.d. Codice Privacy) stabilisce che possono iscriversi al registro

pubblico delle opposizioni tutti gli interessati che vogliano opporsi al trattamento delle proprie numerazioni telefoniche per finalità di marketing vendita diretta o compimento di ricerche di mercato, mediante l'impiego del telefono. In tale registro saranno inoltre inserite tutte le numerazioni fisse non pubblicate negli elenchi degli abbonati di cui all'art.129 del Codice Privacy e che gli operatori sono comunque tenuti a fornire al gestore del registro con la stessa periodicità di aggiornamento prevista per la base di dati unica. Gli interessati iscritti al registro delle pubbliche opposizioni (comma 3) le cui numerazioni siano o meno riportate negli elenchi degli abbonati, potranno revocare anche solo per periodi di tempo definiti la propria opposizione in qualunque momento anche per via telematica o telefonica. Il comma 5 indica poi quali sono gli effetti connessi all'iscrizione nel registro pubblico delle opposizioni, che danno luogo a una revoca di tutti i consensi espressi in precedenza con qualsiasi forma o mezzo finalizzati ad autorizzare il trattamento delle proprie numerazioni, mediante l'utilizzo del telefono. Pertanto, è preclusa ogni attività promozionale di marketing, statistica o finalizzate ad effettuare ricerche di mercato, così come allo stesso tempo è vietato l'uso di numerazioni cedute a terzi direttamente dal titolare del trattamento, anche se interesserà solo il contatto telefonico, non interessando modalità diverse dallo stesso, per cui l'interessato abbia espresso il proprio consenso. Rispetto a quanto detto sono fatti salvi i consensi effettuati nell'ambito di specifici rapporti contrattuali in essere oppure cessati da non più di 30 giorni, per i quali è assicurata in maniera semplificata la facoltà di revoca. Il comma 6 prevede, comunque, che l'interessato iscritto presso il registro avrà la possibilità di prestare nuovi e ulteriori consensi a titolari del trattamento indicato dallo stesso. Ai sensi del comma 7, a seguito dell'iscrizione nel registro delle opposizioni sono vietati con qualsiasi forma o mezzo la comunicazione a terzi, il trasferimento dei dati personali degli iscritti al registro per finalità commerciali o di vendita. Di particolare importanza risulta il comma 8, ai sensi della quale in caso di cessione a terzi dei dati relativi alle comunicazione telefoniche, il titolare deve comunicare agli interessati gli estremi identificativi del soggetto a cui dati medesimi sono trasferiti.

Al fine di rendere effettivo il sistema alla base del registro pubblico delle opposizioni è stato previsto al comma 12, l'obbligo per gli operatori di consultare i registri con cadenza almeno mensile e prima dell'inizio di ogni campagna promozionale. Per rendere più agevole e meno costosa la consultazione del registro, il comma 13 rinvia a un decreto del Ministero dello Sviluppo Economico la definizione dei criteri

generali per l'aggiornamento periodico delle tariffe. Il comma 11 dispone, altresì, che il titolare del trattamento è responsabile in solido anche nel caso di affidamento a terzi di attività call center, per l'effettuazione di chiamate telefoniche dell'operatore in violazione della legge. Merita una particolare attenzione il comma 14 ai sensi del quale è vietato l'utilizzo di compositori telefonici per la ricerca automatica di numeri, anche non inseriti nell'elenco degli abbonati. Ai sensi dell'art. 2 della legge in oggetto tutti gli operatori che svolgono attività di call center rivolte a numerazioni nazionali fisse o mobile hanno l'obbligo di presentazione dell'identificazione della linea chiamante. A tal fine entro novanta giorni dalla data entrata in vigore della presente legge l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) individuerà due codici o prefissi specifici atti a identificare e distinguere in modo univoco le chiamate telefoniche finalizzate ad attività statistiche, da quelle finalizzate al compimento alle ricerche di mercato ed attività di marketing.

I suddetti operatori provvederanno ad adeguare tutte le numerazioni telefoniche utilizzate per i servizi di call center, anche delocalizzati facendo richiesta di assegnazione della relativa numerazione entro 60 giorni dalla data di entrata in vigore del provvedimento AGCOM, oppure presentando l'identità della linea a cui possono essere contattati. L'attività di vigilanza riguardanti gli obblighi citati darà luogo da parte della stessa AGCOM, che in caso di violazione applicherà le sanzioni all'art.1 commi 29,30,31,32 della legge 31 luglio 1997 n.249.

4. Conclusioni: dalla teoria alla pratica.

La tutela dei dati personali viene ampliata dal nuovo regolamento del Ministero dello sviluppo economico, che si concentra sul Registro pubblico delle opposizioni, al quale si possono iscrivere gli utenti che non intendono ricevere alcun tipo di offerta promozionale, né sul telefono fisso, né sul cellulare, né in forma cartacea. Tale possibilità viene estesa oggi anche a numeri di telefonia mobile e a numeri riservati, o non presenti negli elenchi telefonici pubblici.

Il garante, tuttavia, dopo aver premesso che il regolamento ha già recepito precedenti indicazioni, aggiunge ulteriori condizioni per renderlo pienamente conforme alla tutela dei dati personali. A tal fine, richiede che le nuove norme devono chiarire ulteriormente che l'iscrizione nel registro determina automaticamente l'opposizione a qualsiasi trattamento di dati personali per fini promozionali**,** effettuate da chiunque, compresa anche la revoca dei consensi precedentemente espressi, con qualsiasi riferimento alle categorie merceologiche. Pertanto, valuta la possibilità di far confluire nel

Registro delle opposizioni tutti gli indirizzi postali dei contraenti, anche quelli che non sono presenti negli elenchi telefonici. La revoca selettiva al trattamento dei dati potrebbe essere sostituita dal consenso espresso ai singoli operatori. Altrettanto macchinosa potrebbe essere la gestione delle categorie merceologiche, perché lo stesso operatore può svolgere attività promozionali relative alle stesse, per cui bisognerebbe consentire all'utente di revocare non solo l'intera attività dell'operatore, ma anche ogni singola campagna. Nei casi illeciti, inoltre, il garante propone sanzioni e una responsabilità, non derogabile tramite contratto, tra la società e il call center che ha effettuato la chiamata per una responsabilità in concorso o in solido,come è avvenuto nel caso Green Power che affida a VinCall il compito di procacciare nuovi clienti per conto di Edison Energia. VinCall affida al Call Center albanese il raggiungimento dell'obiettivo tramite l'attività di telemarketing. Una volta manifestato agli operatori di Tel it la volontà di concludere il contratto, l'utente viene ricontattato da VinCall. L'irregolarità si sostanzia nel fatto che la società, nel caso specifico, VinCall, oltre a non aver reso alcuna informativa alle persone contattate, non aveva richiesto come previsto il consenso al trattamento dei dati personali per finalità di marketing. Consenso che la società, peraltro, avrebbe dovuto annotare per iscritto. Tali adempimenti spettavano, infatti, alla società che operava in qualità di autonomo titolare del trattamento, non essendo mai stata designata responsabile. Si rileva, a tale proposito, che Tele It contattava telefonicamente i potenziali clienti usando numeri di telefono raccolti dallo stesso call center, senza che la lista fosse stata fornita o validata da VinCall, Edison e GreenPower. [20]. Lo schema in cui si colloca l'operato di VinCall coinvolge anche altri soggetti nello specifico: Edison Energia S.p.A e il suo agente di vendita Green Power s.r.l Tele It, call center albanese con sede a Valona.In attesa dell'approvazione delle nuove regole sul Registro delle Opposizioni, il Garante passa dalla teoria alla pratica infliggendo una multa da 2 milioni di euro a carico di VinCall per telemarketing indesiderato**.**

[20] https://www.hdblog.it/2019/05/30/telemarketing-garante-privacy-riforma-registro/

LA TUTELA DELLA CONCORRENZA E DEI CONSUMATORI: LE LINEE GUIDA EDPB SUI SERVIZI ONLINE.

di Cristian Telese

SOMMARIO: 1. Premessa; - 2. Le Linee guida 2/2019: delucidazioni e prospettive di applicazione; - 3. Impatto del trattamento dei dati personali nei servizi online sulla tutela della concorrenza e del consumatore

"…The contract, whose execution necessarily requires the processing of personal data of the interested party, is a negotiation in which two necessities cross sinallagmatically…

…Online service supply contracts, in addition to complying with the general principles of lawful processing of personal data, must aim at effectively limiting the purpose of the processing, as well as minimizing the data to be processed…."

1. Premessa

Con l'introduzione del GDPR[21] che ha abrogato la direttiva 95/46/CE, molteplici sono state le novità apportate alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Tra queste, particolare rilevanza assume anche la trasformazione di un organismo consultivo di primaria importanza, il cd. "Working Party 29" (spesso indicato con l'abbreviazione "WP29") nell'attuale "European Data Protection Board"[22] o Comitato europeo per la protezione dei dati (di seguito indicato EDPB o "Comitato") i cui compiti sono analiticamente descritti dagli artt. 68 e ss. del GDPR.

In particolare, è ora compito precipuo dell'EDPB di garantire l'applicazione coerente del Regolamento tramite un'attività di consulenza prestata direttamente alla Commissione europea o anche con esame di propria iniziativa di qualsiasi questione relativa all'applicazione del Regolamento, generalmente tramite la pubblicazione di

[21] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

[22] Cfr. https://edpb.europa.eu/edpb_en

"linee guida, raccomandazioni e buone prassi in materia" (art. 70, par. 1, lett. e) GDPR)[23].

2. Le Linee guida 2/2019: delucidazioni e prospettive di applicazione

Di assoluta attualità sono oggi senza dubbio le "Linee guida 2/2019"[24] sul trattamento dei dati personali ai sensi dell'art. 6, par. 1, lett. b) del GDPR[25] nel contesto della fornitura di servizi online, adottate il 9 aprile 2019 per la consultazione pubblica.

L'elaborato interviene in materia di servizi online con particolare riguardo alla base giuridica del trattamento dei dati personali (acquisiti per la fornitura di prestazioni inerenti a tali servizi) prevista dall'art. 6, par. 1, lett. b) GDPR.

Secondo tale norma è considerato lecito il trattamento dei dati personali se e nella misura in cui *"il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso"*.

I servizi online, punto cardine della società moderna (spesso, non a caso, definita "società dell'informazione"), si declinano in molteplici prestazioni quali i social-media, l'e-commerce, internet come fonte di ricerca, mezzo di comunicazione etc.

L'utente di tali servizi è pressoché sempre anche il soggetto interessato che fornisce i propri dati personali e che, in quanto tale, deve essere tutelato dalla minaccia di un loro utilizzo indiscriminato.

Secondo la norma contenuta nell'art. 6, par. 1, lett. b) del GDPR, pertanto, il fornitore di tali servizi (titolare del trattamento) può lecitamente utilizzare i dati personali appresi dall'utente qualora ciò sia necessario o "all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso".

L'EDPB sottolinea la differenza che intercorre tra i casi previsti dalla norma appena citata che, infatti, si distinguono sia per finalità che per impulso.

---

[23] Regolamento (UE) 2016/679, art. 70 par. 1, lett. e): *"esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento"*

[24] *Guidelines 2/2019 on the processing of personal data under article 6(1)(b) GDPR in the context of the provision of online services to data subjects* in *https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en*

[25] Regolamento (UE) 2016/679, art. 6, par. 1, lett. b): *"1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: ... b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso"*

Il contratto, la cui esecuzione presuppone necessariamente il trattamento di dati personali dell'interessato, è un atto negoziale in cui si incrociano in maniera sinallagmatica due necessità: quella del titolare/fornitore del servizio di trattare i dati personali per lo svolgimento della prestazione richiesta e quella dell'interessato/utente di ricevere detta prestazione.

La seconda parte dell'art. 6, par. 1, lett. b) del GDPR, invece, dichiara lecito il trattamento dei dati personali anche quando essi debbano essere necessariamente trattati per l'esecuzione di misure precontrattuali adottate su richiesta dell'interessato: com'è evidente, in quest'ipotesi l'impulso che giustifica l'adozione di questa base giuridica a fondamento del trattamento dei dati personali promana unilateralmente dall'interessato/utente.

Uno dei rischi evidenziati nelle linee guida è che l'interessato veda trattati i propri dati personali senza aver "scelto", né in virtù di uno strumento contrattuale negoziato e concluso con il fornitore/titolare né dietro un'esplicita richiesta di adozione di misure precontrattuali, quali dati personali fornire per il trattamento e, soprattutto, per quali finalità.

A tal proposito l'EDPB tenta di individuare alcuni elementi imprescindibili che devono essere considerati prima dell'adozione da parte del titolare della base giuridica ex art. 6, par. 1, lett. b) del GDPR a fondamento di liceità del trattamento che si appresta ad effettuare.

Innanzitutto, si pone estrema rilevanza al carattere della necessità che il trattamento deve avere, affinché si possa consentire l'esecuzione del contratto o la concreta adozione delle misure precontrattuali richieste dallo stesso.

Se la prima accezione della base giuridica di liceità introdotta dalla norma sopra richiamata è di intelligibile comprensione e non necessita di alcuna spiegazione, più ostico è capire cosa il legislatore europeo abbia voluto intendere con l'espressione "esecuzione di misure precontrattuali adottate su richiesta dello stesso (ndr interessato)".

Ebbene è proprio l'EDPB a chiarire la portata di tale espressione nelle linee guida 2/2019 con il seguente esempio: una persona interessata fornisce il proprio codice postale per verificare se un determinato fornitore di servizi opera nella propria area.

Anche questo, quindi, può essere considerato come un trattamento necessario per elaborare dati personali su richiesta dell'interessato stesso e prima di stipulare un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b)

La presenza dell'elemento della "necessità" (oggetto di un paragrafo specifico delle linee guida 2/2019) deve essere verificata, in concreto, caso per caso, non rilevando all'uopo un riferimento generico nelle clausole contrattuali di un eventuale accordo titolare/interessato che potrebbe aprire al titolare spazi non ben definiti di attività di trattamento e, soprattutto, pericolosamente non presidiati dalla consapevolezza dell'interessato.

Non a caso l'EDPB, trattando del delicatissimo ambito della pubblicità comportamentale, puntualizza che i dati personali non possono essere considerati come beni commerciabili, in quanto elevati (dal GDPR e, ancor prima, dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea[26]) al rango di diritti fondamentali e, perciò, incommerciabili.

Partendo da quest'ottica, va da sé che tutti i trattamenti che non vedano o un consapevole consenso da parte dell'interessato oppure il supporto di una base giuridica espressamente prevista dal Regolamento, sono illeciti.

Il trattamento dei dati personali giustificato dalla base giuridica di cui all'art. 6, par. 1, lett. b) è necessario solo quando rispetti anche tutti gli altri limiti imposti dal GDPR ad ogni trattamento lecito, essenzialmente corrispondenti a quelli descritti dall'art. 5 GDPR: liceità, correttezza e trasparenza del trattamento, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza dei dati trattati.

3. Impatto del trattamento dei dati personali nei servizi online sulla tutela della concorrenza e del consumatore.

L'adozione della base giuridica prevista dall'art. 6, par. 1, lett. b) come fondamento di liceità di un trattamento di dati personali presuppone, quindi, pur sempre la presenza di un contratto o l'adozione di misure precontrattuali richieste esplicitamente dall'utente.

Tuttavia, l'EDPB è ben consapevole del fatto che esula dai propri compiti un giudizio sugli strumenti contrattuali utilizzati nei Paesi membri che possano contenere il riferimento normativo in analisi.

[26] GUCE del 18 dicembre 2000, C 364/3

Ciononostante, puntualizza il Comitato, i contratti e le condizioni contrattuali devono essere conformi ai requisiti delle leggi sui contratti.

Particolare attenzione viene rivolta ai contratti stipulati con i consumatori.

L'EDPB precisa che, oltre alla conformità con le leggi nazionali di tutela dei consumatori, i contratti di fornitura di servizi online devono, altresì, rispettare i limiti imposti dalla direttiva 93/13/CEE[27] concernente le clausole abusive nei contratti stipulati con i consumatori.

Pertanto, poiché strettamente connessa per la comune finalità di tutela dei diritti dei "consumatori" nei contratti stipulati con i "professionisti", così come la direttiva 93/13/CEE anche la disposizione contenuta nell'art. 6, par. 1, lett. b) del GDPR può trovare applicazione in contratti di fornitura di servizi online stipulati con "professionisti" domiciliati extra UE.

Anche in quest'ottica si può facilmente cogliere l'intento di elevare il diritto alla protezione dei dati personali al rango di diritto fondamentale dell'individuo e, per questo, oltre che incommerciabile anche suscettibile di tutela al di fuori dei confini comunitari.

I contratti di fornitura di servizi online, oltre al rispetto dei principii generali di liceità del trattamento dei dati personali, devono essenzialmente mirare ad un'effettiva limitazione di scopo del trattamento, nonché alla minimizzazione dei dati da trattare.

Tali necessità ravvisate nelle linee guida in esame sono particolarmente rilevanti se si tiene in debito conto il fatto che, generalmente, i contratti di fornitura di servizi online non sono negoziati su base individuale ma presentati al cospetto del consumatore ("interessato", in ambito privacy) solo per una "sottoscrizione", per lo più virtuale.

E'un fatto notorio che i contratti di colossi dei servizi online non possano essere in alcun modo ridiscussi dall'utente; è, pertanto, assai cogente garantire determinati diritti al consumatore intervenendo a monte e cioè obbligando *ab origine* l'azienda fornitrice di servizi ad adottare determinate accortezze negoziali a pena di illiceità dell'intero trattamento e, pertanto, all'impossibilità di eseguire il contratto.

L'EDPB avverte sul rischio acuto che i titolari di trattamenti di dati personali siano nella condizione di generalizzare eccessivamente le clausole dei contratti di fornitura di servizi che vengono presentati agli utenti, spesso in maniera anche difficil-

[27] GUCE del 21 aprile 1993, N. L 95/29

mente leggibile, per una formale adesione: ciò cagiona la massimizzazione della raccolta e dell'utilizzo dei dati senza alcuna specificazione degli scopi (eventualmente anche ulteriori) e minimizzazione dei dati carpiti.

In realtà, già con una precedente pronuncia (Cfr. WP29, 29 marzo 2009 sulla limitazione delle finalità, WP203, pp. 15-16) l'allora WP29 ammonì circa la necessità che lo scopo della raccolta dovesse essere "chiaramente e specificamente identificato: deve essere dettagliato abbastanza da determinare quale tipo di elaborazione è e non è inclusa nello scopo specificato, e per consentire di valutare la conformità alla legge e salvaguardare la protezione dei dati applicato".

Nel medesimo parere innanzi citato il WP29 richiamò l'attenzione sul fatto che "uno scopo che è vago o generale, come ad esempio "migliorare" l'esperienza degli utenti, "scopi di marketing", "scopi di sicurezza IT" o "ricerca futura" – senza più in dettaglio - di solito non soddisfano i criteri di essere 'specifici'"[28].

A tal riguardo, con le linee guida 2/2019, l'EDPB ha voluto esplicitamente analizzare alcune di queste finalità particolari che in precedenza erano state solamente richiamate.

In particolare, per ciò che attiene al trattamento dei dati avente come finalità il "miglioramento del servizio", l'EDPB non ritiene che l'articolo 6, paragrafo 1, lettera b) possa essere, in generale, una base giuridica appropriata per elaborazione ai fini del miglioramento di un servizio o dello sviluppo di nuove funzioni all'interno di un servizio esistente.

Generalmente, spiega l'EDPB, un utente stipula un contratto per avvalersi di un servizio esistente; pertanto, il contratto per la cui esecuzione è necessario il trattamento dei dati personali ha come oggetto il servizio esistente e non certo un altro servizio che è stato oggetto di miglioramenti.

In questo caso, quindi, la base giuridica più idonea per un trattamento lecito dovrebbe poggiarsi più sulla ricerca del consenso esplicito da parte dell'utente ex art. 6, par. 1, lett. a) del GDPR[29].

Altro caso specifico analizzato dall'EDPB riguarda l'elaborazione di dati personali ai fini di prevenzione delle frodi.

[28] Cfr. WP29, 29 marzo 2009, sulla limitazione delle finalità, WP203, pp. 15-16

[29] Art. 6, par. 1, lett. a) GDPR: "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"

Questa ipotesi appare di più agevole soluzione in termini di ricerca della base giuridica adeguata, in quanto, laddove il trattamento esorbiti la necessità derivante dall'esecuzione del contratto di servizio, potrebbe comunque facilmente trovare giustificazione nella necessità di adempiere ad obblighi legali (art. 6, par. 1, lett. c) del GDPR[30]) oppure per il perseguimento di un legittimo interesse del titolare del trattamento stesso (art. 6, par. 1, lett. f) del GDPR[31]).

Decisamente più spinosa la casistica che contempli il trattamento di dati personali finalizzato alla realizzazione di pubblicità comportamentale online.

Questa tipologia di trattamento afferente, peraltro, ad una tematica assai vasta e dai contorni non sempre ben definiti qual è quella della profilazione dei comportamenti dei consumatori, presenta un altissimo rischio di violazione del diritto alla protezione dei dati personali inteso come diritto fondamentale riconosciuto anche dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea.

In tale ottica, l'EDPB esclude categoricamente l'applicabilità della base giuridica prevista dall'art. 6, par. 1, lett. b) , in quanto va da sé che la pubblicità comportamentale non costituisce un elemento necessario dei servizi online: sarebbe assurdo, infatti, pensare che un contratto di fornitura di servizi online non possa trovare esecuzione se non in presenza di pubblicità comportamentale.

Inoltre, poiché la pubblicità comportamentale si fonda su di una previa attività di profilazione alla quale l'utente è stato già sottoposto, debbono valere i medesimi principi di liceità già previsti per le cookie policy.

In pratica, il trattamento dei dati personali prestati nell'ambito di un contratto di fornitura di servizi online e che comporti anche attività di profilazione può avvenire per finalità di pubblicità comportamentale solo laddove l'utente/interessato presti un esplicito e consapevole consenso allo stesso.

Considerazioni similari, infine, debbono essere rassegnate per l'ultima tipologia di trattamento "particolare" analizzata dall'EDPB con le linee guida 2/2019 e cioè l'elaborazione dei dati al fine di personalizzazione del contenuto.

[30] art. 6, par. 1, lett. c) del GDPR "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento"

[31] art. 6, par. 1, lett. f) del GDPR "il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore."

In questo caso, infatti, bisogna analizzare di volta in volta il caso concreto e, laddove non si intraveda un'oggettiva necessità di trattare i dati personali dell'utente/consumatore/interessato per una personalizzazione del contenuto del servizio necessariamente legata all'esecuzione del contratto, bisognerà raccogliere il consenso del fruitore.

CRIPTOVALUTE E DIRITTO.

di Alessia Narciso

SOMMARIO: 1. Premessa – 2. Natura giuridica – 3. Rilievi in ambito penale – 4. Rilievi in ambito civile – 5. Rilievi in ambito fiscale – 6. Rilievi in ambito commerciale – 7. Conclusioni.

The use of virtual currencies provides significant benefits due to safety, speed and savings in the transaction costs, but entails considerable risks in order to money laundering, terrorism and tax evasion. In fact the first jurisprudencial and legislative actions - as suggested by the Authorities - were made to fight those risks.

1. Premessa

Le criptovalute, come suggerisce già l'etimologia greca, sono valute nascoste, nel senso che tutte le informazioni relative alle loro movimentazioni sono cifrate per mezzo di complessi algoritmi.

Sono denominate anche valute virtuali per la loro immaterialità, ovvero sono generate e scambiate esclusivamente per via telematica.

Trattasi di rappresentazioni digitali di valore non emesse da banche centrali, istituti di credito o di moneta elettronica[32], bensì "minate" da soggetti privati grazie ad un sistema software open source e trasferite in maniera diretta tra le parti attraverso una rete decentralizzata *peer to peer*.

La base giuridica delle criptovalute è di tipo convenzionale in quanto non vi è il controllo da parte di alcuno stato nella loro circolazione, tutto è basato, invero sulla mera accettazione volontaria dei soggetti che intendono acquistarle o trasferirle il tutto corredato da un insieme di regole c.d. "protocollo" [33].

[32] European Banking Authority (EBA), *Opinion on virtual currencies*, 2014; European Central Bank (ECG – BCE), "*Virtual currency schemes – a further analysis*", 2015.

[33] Caratteristica su cui ha posto l'attenzione il Consiglio Nazionale del Notariato, il quale in un recente parere ha affermato che: *" La circolazione dei bitcoin, quali mezzi di pagamento, si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge.*". Consiglio Nazionale del Notariato Quesito Antiriciclaggio n. 3-2018/B

Occorre rilevare che l'assenza di un intermediario non inficia la sicurezza delle transazioni, invero, la dirompente tecnologia *blockchain*[34] sulla quale si fondano tutte le criptovalute, le rende estremamente sicure, veloci ed economiche.

Attualmente sono circa cinquecento le criptovalute in circolazione[35] e tra queste, le più conosciute e che godono della maggiore capitalizzazione sono *bitcoin* ed *ether* [36][37].

Quest'ultima è indubbiamente la più innovativa, in quanto pensata per favorire la diffusione degli *smart contracts* creati sulla sua piattaforma Ethereum[38].

Presto alla lista di valute virtuali circolanti si aggiungerà Libra[39], la criptovaluta che il gruppo Facebook lancerà nel 2020 e che avrà, come carattere distintivo, una maggiore stabilità data da un valore di scambio ancorato a valute aventi corso legale (Euro/Dollaro).

2. Natura giuridica

È necessario premettere che circa la natura giuridica delle criptovalute non vi è uniformità di vedute né in dottrina, né in giurisprudenza, né nelle comunicazioni fornite dalle autorità di vigilanza. Le diverse ipotesi che sono state prospettate possono

[34] La *blockchain* è un registro aperto e distribuito che memorizza tutte le transazioni in modo verificabile e permanente. Si tratta di un sistema nel quale un insieme di soggetti condivide risorse informatiche per rendere disponibile alla comunità di utenti un database virtuale generalmente di tipo pubblico. È una lista in continua crescita di record c.d. *blocks* collegati tra loro e resi sicuri mediante la crittografia che è sinonimo di autenticazione, integrità, non repudiabilità e autorizzazione. Ogni blocco ha la propria firma digitale (*hash*), quella del blocco precedente e i dati della transazione.

[35] Il dato è stato fornito dalla European Central Bank (ECG – BCE) con il report *Virtual currency schemes – a further analysis*, del febbraio 2015.

[36] Creata nel 2009 da un inventore anonimo noto con lo pseudonimo di Satoshi Nakamoto. Il termine, se scritto con l'iniziale minuscola, indica la criptovaluta, scritto con la maiuscola invece, indica la piattaforma di riferimento.

[37] Altre criptovalute che meritano di esser menzionate sono: Ripple (XRP) che di recente ha anche concluso un'importante *partnership* con la MoneyGram, società leader a livello mondiale nel trasferimento di denaro; Dash Digital Cash (DASH) e Litecoin (LTC).

[38] Gli *smart contracts*, in breve, sono applicazioni software che garantiscono che al verificarsi delle condizioni previamente fissate dalle parti, si producono gli effetti da loro voluti. La sicurezza delle operazioni è garantita dalla crittografia e dalla tecnologia *blockchain*.

[39] Con l'intenzione di rivoluzionare il sistema bancario globale, Facebook, lo scorso 18 giugno, ha presentato ufficialmente la sua criptomoneta, una valuta senza confini utilizzabile come metodo di pagamento non solo nel mondo virtuale (con transazioni effettuate sui social network Facebook, What's App e Messenger), ma anche nel mondo reale (grazie ad accordi conclusi e a concludersi con diverse società come Mastercard, Visa, PayPal, Booking ed Uber). Libra dovrebbe entrare in circolazione nella prima metà del 2020.

esser raggruppate in due macrocategorie: la prima che predilige lo scopo di scambio, la seconda che si basa sul valore di investimento delle criptovalute[40].

La valorizzazione della finalità di scambio è propria delle analisi che tentano di qualificare le criptovalute come valuta, ovvero moneta, bene giuridico o documento informatico.

Certamente può affermarsi che le criptovalute non possono rientrare nel concetto puro di valuta, così come intesa dalla teoria statalista, in quanto non hanno corso legale o forzoso in nessuno Stato e dunque, sono prive del potere solutorio nell'ambito delle obbligazioni pecuniarie e per intenderci, il creditore è legittimato a rifiutare una simile forma di pagamento[41].

Parimenti risulta complesso riconoscere alle criptovalute la natura di moneta, in quanto per le loro peculiarità non sono in grado di svolgere integralmente le tre funzioni principali individuate dalla teoria economica per le monete in senso stretto[42].

In particolare, la base convenzionale e la scarsa accettazione pubblica delle criptovalute frenano la loro utilizzabilità per l'acquisto di beni e servizi (funzione di mezzo di scambio) e l'elevata volatilità dei tassi di cambio contrasta con la stabilità nel tempo del loro potere d'acquisto (funzione di riserva di valore). Infine, per le caratteristiche suesposte, le criptovalute non possono essere un idoneo strumento di misurazione del valore di beni e servizi (funzione di unità di conto).

Le criptovalute non sono monete elettroniche[43], anzi si differenziano da queste sia per l'assenza di un soggetto intermediario nella transazione sia in quanto i fondi

[40] Si segnala che in proposito la Banca d'Italia non ha preso posizione definendo le valute virtuali come "*rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente".* Banca d'Italia, *Avvertenze sull'utilizzo delle cosidette "valute virtuali"*, gennaio 2015.

[41] Quanto affermato è pacifico in dottrina. Si veda ad esempio: R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'Informazione e dell'Informatica*, II, 1, 2017; G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario critto anarchico o soluzione tecnologica in cerca di un problema?*, in *Diritto dell'Informazione e dell'Informatica*, II, 3, 2015; P. Iemma e N. Cuppini, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *www.dirittobancario.it.* L'impossibilità di qualificare le criptovalute come valuta in senso tradizionale è sostenuta anche da ECG, *op. ult. cit*.; Banca d'Italia, *op. ult.cit*.

[42] In tal senso: G. Gasparri, *op. ult. cit*.; ECG, *op. ult. cit*.; ma in senso contrario: R. Bocchini, *op. ult. cit*.

[43] Disciplinate dalla Direttiva 16 settembre 2009, n.110

non sono espressi nell'unità di calcolo tradizionale (ad esempio in euro), ma nell'unità di calcolo virtuale (es. *bitcoin*)[44].

Tali elementi portano ad escludere la natura di mezzo di pagamento e dunque l'applicabilità della relativa normativa di cui al D.Lgs. n. 11/2010[45].

Tuttavia, occorre evidenziare che l'Autorità di vigilanza europea come la Corte di Giustizia europea hanno avuto modo di precisare che le valute virtuali, seppur non emesse da banche centrali o istituti di credito, possono esser accettate come mezzo di pagamento alternativo al denaro[46].

Analizzate da altro punto di vista, le valute virtuali, possono costituire uno strumento di investimento.

Ci si è interrogati, quindi, sulla possibilità di inquadrarle come veri e propri prodotti finanziari.

In Italia il nostro legislatore ha definito i prodotti finanziari nella norma di cui all'art. 1, comma 1, lett. u) del Testo Unico delle disposizioni in materia di intermediazione finanziaria[47], come l'insieme di strumenti finanziari e ogni altra forma di investimento di natura finanziaria.

Allo stesso modo, si ritiene che anche la natura di strumenti finanziari in senso stretto, debba essere esclusa per le criptovalute[48], sia perché non rientrano nell'elenco tassativo di cui all'art. 1, comma 2 del TUF e sia perché, una tale definizione, impedirebbe di qualificarle come strumenti di pagamento[49].

---

[44] La diversità delle criptovalute o valute virtuali dalle monete elettroniche è stata sottolineata anche dalla Corte di Giustizia dell'Unione Europea con la sentenza del 22/10/2015, n. 264/14.

[45] In particolare l'art. 1, comma 1, lett. s) del citato decreto definisce lo strumento di pagamento come "*qualsiasi dispositivo personalizzato e/o insieme di procedure concordate tra l'utente e il prestatore di servizi di pagamento e di cui l'utente si avvale per impartire ordini di pagamento*", D. Lgs. 27 gennaio 2010, n. 11/2010 in attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno.

[46] European Banking Authority, "*Opinion on virtual currencies",* luglio 2014 e ECG, *Virtual Currency Schemes – A Further Analysis,* 2015.

[47] D. Lgs. 24 febbraio 1998, n. 58 "*Testo Unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52*".

[48] Concorda la dottrina maggioritaria, ma il primo giudice di merito italiano chiamato a pronunciarsi su un acquisto di criptovalute, le ha qualificate come strumenti finanziari. La scelta, severamente criticata dalla dottrina, appare dettata dall'intenzione del Tribunale di riconoscere all'acquirente la maggior tutela possibile: quella del consumatore. Trib. Verona, 24.01.2017, n. 195.

[49] Il legislatore, infatti, nell'elenco degli strumenti finanziari non include gli strumenti di pagamento, in quanto sono più vicini al consumo che all'impiego del risparmio in vista di un ritorno economico: T.U.F., art. 1, comma 2.

La categoria di investimento di natura finanziaria, invece, essendo a carattere aperto appare pi50ù adeguata a ricomprendere anche le criptovalute con la conseguente applicabilità della disciplina dettata in materia di intermediazione finanziaria[51].

3. Rilievi in ambito penale

Da un punto di vista penalistico, le criptovalute per le loro caratteristiche offrono la possibilità di un loro utilizzo distorto per scopi criminali quali il riciclaggio e il finanziamento del terrorismo[52].

Costituiscono un potenziale strumento per far circolare fondi illeciti per tre ordini di ragioni: l'anonimato di chi dispone la transazione e di chi ne beneficia, l'assenza di intermediari e/o controlli statali e l'accesso delocalizzato che offrono le piattaforme di scambio.

Per poter effettuare transazioni con criptovalute, è sufficiente possedere un wallet, un conto che può esser aperto in pochi minuti indicando semplicemente un username e una password (e, se è previsto il sistema di doppia autenticazione, un numero di telefono) senza alcuna preliminare procedura di verifica sull'identità , né la stipula di un contratto di tipo bancario.

A ciò si aggiunge che le transazioni avvengono online e attraverso una forma di accesso delocalizzata che permette di eseguire trasferimenti di criptovalute anche transfrontalieri, tra Stati che non hanno adeguate normative per combattere il riciclaggio e il finanziamento del terrorismo.

Nel nostro ordinamento con il D.lgs. 25 maggio 2017 n. 90 è stata data attuazione alla IV Direttiva UE[53] relativa alla prevenzione dell'uso del sistema finanziario a fini

[50] Per la CONSOB si è in presenza di investimenti di natura finanziaria in tutti quei casi in cui l'investitore impieghi capitale con un'aspettativa di profitto, assumendosene il relativo rischio Tra le tante comunicazioni si segnala: CONSOB, 6 maggio 2013, n. DTC/13038246.

[51] G. Gasparri, *op. ult. cit.*, P. Iemma e N. Cuppini, *op. ult.cit.*

[52] I rischi di riciclaggio e finanziamento del terrorismo derivanti dall'utilizzo anomalo di criptovalute sono stati segnalati più volte dalle Autorità di vigilanza bancarie sia europee che nazionali come l'European Banking Authority (EBA) con la relazione "*Opinion on virtual currencies"* del 4 luglio 2014 e l'Unità di informazione finanziaria per l'Italia (UIF) con la comunicazione "*Utilizzo anomalo delle valute virtuali*" del gennaio 2015. Eguale attenzione a tali pericoli era già stata riposta sia dalla European Central Bank (ECB – BCE) con l'analisi "*Virtual Currency Schemes*" dell'ottobre 2012 e dall'organismo intergovernativo Financial Action Task Force (FATF – conosciuto anche con l'acronimo GAFI: Gruppo d'Azione Finanziaria Internazionale) con il report "*Virtual Currencies - Key Definitions and Potential AML/CFT Risks*", 2014.

[53] Direttiva 20 maggio 2015, n. 849/2015.

di riciclaggio o finanziamento del terrorismo, apportando una serie di modifiche alle normativa vigente in materia[54] e in materia di contratti di credito ai consumatori[55].

Per la prima volta, il legislatore italiano definisce la valuta virtuale, in particolare come "la rappresentazione digitale di valore, non emessa da una banca centrale o da un ente pubblico, non necessariamente legata ad una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente"56. Si tratta di una definizione che conferma il carattere decentralizzato della valuta virtuale, della sua distinzione dalla moneta elettronica e che ne valorizza la funzione di scambio.

Altri aspetti innovativi del D.lgs. 90/2017 riguardano i prestatori di servizi relativi all'utilizzo di valuta virtuale, intesi come "ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale"57, che li inquadra all'interno della disciplina dei c.d. "cambiavalute"[58].

Ciò comporta, in particolare, per tutti i prestatori di servizi relativi all'emissione di criptovalute, l'obbligo di iscrizione in una sezione speciale del Registro istituito presso l'OAM[59].

I prestatori di servizi relativi all'utilizzo valuta virtuale dovranno comunicare la propria operatività nel territorio nazionale, al Ministero dell'economia e delle finanze (e quest'ultimo verificherà il rispetto dei termini e modalità di presentazione.)[60], in ciò

[54] D.Lgs. 21 novembre 2007, n. 231, che a sua volta aveva dato attuazione alla Direttiva 26 ottobre 2005, n. 2005/60/CE.

[55] D.Lgs. 13 agosto 2010, n. 141 che aveva dato attuazione alla Direttiva 23 aprile 2008, n. 2008/48/CE, nonché apportato modifiche del Titolo VI del T.U.B. in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi.

[56] D.Lgs. 231/2007, art. 1, comma 2 lett. *qq*, introdotta dal D.lgs. 90/2017, art. 1.

[57] D.Lgs. 231/2007, art. 1, comma 2, lettera *f*), così come inserito dall'art. 1 D.Lgs. 90/2017

[58] È quanto stabilito dal comma 8 *bis*, dell'art. 17 *bis* del D.Lgs. 141/2010, introdotto dall'art. 8 del D.Lgs. 90/2017.

[59] L'acronimo sta per "Organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi" il quale è disciplinato dall'art. 128 *undecies* del T.U.B. L'iscrizione a tale registro è subordinata al ricorrere dei requisiti prescritti dall'art. 17 *bis*, comma 2, D.Lgs. 141/2010. In dettaglio, per le persone fisiche è necessario il possesso della cittadinanza italiana o di uno Stato UE o di altri Stati individuati; per le persone giuridiche è necessario che la sede legale o la stabile organizzazione (per i soggetti comunitari) sia nel territorio della Repubblica.

[60] D.Lgs. 141/2010, art. 17 *bis*, comma 8 *ter*

anticipando anche il legislatore europeo che con la V Direttiva antiriciclaggio ha previsto l'obbligo per tutti gli Stati membri di prevedere una procedura di registrazione per i prestatori di servizi di criptovalute[61].

Tale Direttiva, in un'ottica di maggior controllo degli Stati membri sull'uso delle criptovalute, amplia l'ambito di applicazione della precedente includendo nel novero dei soggetti obbligati anche i fornitori di servizi di cambio tra valute virtuali e valute aventi corso legale e i cd. *wallet providers*.

Nel nostro ordinamento i prestatori di servizi relativi all'utilizzo di valuta virtuale "limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso" già erano assoggettati alla normativa antiriciclaggio[62].

La novità, pertanto, riguarda solo i cd wallet providers definiti come coloro che forniscono "servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali"[63].

L'attrazione nel campo di operatività della normativa antiriciclaggio comporta per i fornitori di servizi di cambio e gli *wallet providers* il rispetto di una serie di obblighi quali l'adeguata verifica della clientela, la conservazione e la segnalazione di operazioni sospette, tutti volti a contrastare i rischi derivanti da un uso illecito delle valute virtuali.

Tuttavia non va dimenticato che gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori di servizi e in completo anonimato.

L'anonimato potrebbe esser superato laddove le Unità di Informazione Finanziaria dei singoli Stati membri riuscissero ad ottenere informazioni capaci di associare ciascun *wallet* all'identità del suo effettivo titolare.

4. Rilievi in ambito civile

Una questione prettamente civilistica che è stata di recente sollevata, attiene alla possibilità di acquistare un bene (immobile) corrispondendo il relativo prezzo in valute virtuali.

Sulla questione si è pronunciato il Consiglio Nazionale del Notariato con parere n. 3-2018/B del marzo 2018.

[61] Direttiva 30 maggio 2018, n. 2018/843

[62] D.Lgs. 231/2007, art. 3, comma 5, lett. i)

[63] D.Lgs. 231/2007, art. 3, paragrafo 1, punto 3, lett. g) e) h)

Il problema principale è che la tracciabilità dei pagamenti in criptomonete è solo di natura per così dire "informatica", in quanto ogni transazione è registrata tramite *blockchain*, ma non è possibile identificare chi - realmente - la effettua, né chi la riceve.

In altre parole, non può esser verificato se l'acquirente è il reale titolare del *wallet* dal quale viene disposto il pagamento, né se il venditore è il titolare effettivo del *wallet* cd. beneficiario.

L'impossibilità di identificare e verificare l'identità dei titolari effettivi dei portafogli virtuali non è idonea secondo il CNN all'assolvimento degli obblighi previsti dalla normativa antiriciclaggio.

5. Rilievi in ambito fiscale

Dal punto di vista fiscale, viene in rilievo la ricerca del regime tributario applicabile alle operazioni di cambio che avvengono tra valute aventi corso legale e valute virtuali e viceversa.

Sul punto è intervenuta l'Agenzia delle Entrate[64] che, interpretando da un punto di vista fiscale la sentenza della Corte di Giustizia dell'Unione Europea del 2015 che ha definito tali operazioni come prestazioni a titolo oneroso riconducibili all'art. 135, comma 1, lettera e) della Direttiva 2006/112/CE[65].

Di conseguenza tali operazioni di cambio rientrano nelle prestazioni esenti dall'IVA ex art. 10, comma 1, n. 3 del D.P.R. n. 633/1972, i margini di profitto generati da tali operazioni, invece, saranno imponibili sia ai fini IRES che a quelli IRAP.

6. Rilievi in ambito commerciale

La principale problematica che si è posta sull'utilizzo delle valute virtuali, invece, nell'ambito del diritto commerciale, è quella legata alla idoneità di queste ultime a costituire oggetto di conferimento, come bene in natura, nel capitale sociale di una s.r.l.[66]

[64] Risoluzione 2 settembre 2016, n. 72/E

[65] Direttiva 28 novembre 2006, n. 2006/112/CE relativa al sistema comune d'imposta sul valore aggiunto

[66] Il caso a cui ci si riferisce è quello di una delibera assembleare di aumento del capitale sociale mediante conferimenti in natura, nello specifico opere d'arte e criptovalute. Il Notaio incaricato si era rifiutato di verbalizzare la delibera di assemblea ai fini dell'iscrizione al registro delle imprese, in considerazione del fatto che l'elevata volatilità delle valute virtuali non consente di attribuire loro un valore certo nel *quantum*, né di valutare l'effettività del conferimento. Avverso il diniego del Notaio, l'amministratore unico della s.r.l. proponeva ricorso *ex* art. 2436, comma terzo, Cod.Civ.

La questione - finita dinanzi all'Autorità Giudiziaria - è stata risolta in senso negativo in entrambi i gradi di giudizio, in particolare la sentenza della Corte di Appello di Brescia ha esteso tali considerazioni ad ogni forma di criptovaluta, e non solo a quella oggetto del giudizio.

Ciò che rileva, ai fini di un conferimento di un bene in natura non è tanto la suscettibilità di tale bene alla espropriazione forzata - che le criptovalute in quanto beni immateriali non possiedono – quanto quella di una chiara valutazione economica ai sensi dell'art. 2464, comma 2, Cod. Civ.[67].

Il giudice di primo grado, considerando la natura e le caratteristiche della criptovaluta oggetto di causa, ha ritenuto non soddisfatto il requisito della valutabilità economica effettiva e certa di quest'ultima poiché la stessa non era presente in alcuna piattaforma di scambio con moneta avente corso legale[68].

La Corte d'Appello, invece, pur giungendo alle stesse conclusioni del giudice di prime cure, ha esteso tale valutazione a tutte le criptovalute, ritenendo che nessuna valuta virtuale esistente può esser conferita nel capitale sociale di una società, a causa dell'elevata volatilità che le caratterizza ed alla struttura non regolamentata che le governa[69].

Occorre segnalare, inoltre, che la CONSOB tra il 2017 e il 2019 ha adottato numerosi provvedimenti con i quali ha ordinato la cessazione delle operazioni di vendita di criptovalute, poiché condotte - dai providers - in violazione dell'art. 18 T.U.F.[70], emettendo, finanche, provvedimenti di sospensione in via cautelare[71], o addirittura di divieto della diffusione di annunci pubblicitari su siti internet e/o su social network relativi ad offerte al pubblico di "pacchetti di estrazione di criptovalute"[72].

7. **Conclusioni**

[67] La giurisprudenza ritiene, infatti, che in sede di aumento di capitale l'oggetto del conferimento deve essere un bene che seppur non suscettibile di espropriazione forzata, abbia una consistenza economica (Tra le tante: Cass. n. 3946/2018)

[68] Tribunale di Brescia – Sez. Specializzata in materia di Impresa, decreto 18 luglio 2018, n. 7556/2018

[69] Corte di Appello di Brescia, decreto n. 26/2018

[70] La più recente è la Delibera 12 giugno 2019, n. 20959 con la quale la CONSOB ha disposto un ordine ai sensi dell'art. 7 *octies*, comma 1, lett. b), del D.lgs. 24 febbraio 1998, n. 58 (T.U.F.)

[71] La più recente è la Delibera 29 maggio 2019 n. 20944, con la quale la CONSOB ha disposto la sospensione dell'attività pubblicitaria in questione ai sensi dell'art. 101, comma 4, lett. b), del T.U.F.

[72] Le più recenti sono: Delibera 14 febbraio 2019, n. 20815 e Delibera 13 marzo 2019, n. 20845 con le quali la CONSOB ha disposto il divieto dell'attività pubblicitaria in questione rispettivamente ai sensi dell'art. 101, comma 4, lett. c) e ai sensi dell'art. 99, comma 1, lett. d), del T.U.F.

Le valute virtuali sono il frutto dell'odierno sviluppo tecnologico digitale, così rapido ed incessante, che il Diritto può, inevitabilmente, solo rincorrere.

Nei paragrafi precedenti, si è cercato di evidenziare come qualsiasi sforzo classificatorio delle criptovalute risulti vano e superfluo.

Risulta più agevole riconoscere loro una natura giuridica nuova ed ibrida in considerazione del fatto che possono essere - e sono utilizzate - sia come mezzo di scambio che come forma di investimento finanziario.

Infine, in considerazione della circostanza che l'utilizzo delle criptovalute viene in rilievo non solo dal punto di vista "patologico" del riciclaggio, del finanziamento del terrorismo ed dell'evasione fiscale, si avverte l'esigenza *de jure condendo* di un intervento strutturale da parte del legislatore che ne detti una disciplina completa ed organica.

LA PORTATA FORTEMENTE INNOVATIVA DEL DIRITTO ALLA PORTABILITÀ DEI DATI COME ARTICOLATO NEL GDPR E NELLE LINEE GUIDA WP29.

di Giuliano Palma

SOMMARIO. 1. Premessa. – 2. Il diritto alla portabilità. – 3. Cenni sul procedimento. – 4. Conclusioni.

The introduction of the GDPR has assumed significant importance as it has provided for a series of "new rights" which, by their nature, are not "generic and general in scope". They are rights aimed at controlling essential aspects of the protection of personal data processing in a framework that aims to stimulate and foster the development of the digital society. Among the new rights introduced by the GDPR, a central place is occupied by the right to data portability, as per art. 20, which also takes into account the Guidelines adopted by the Working Party (WP No. 242 rev.01, issued in December 2016 and revised on April 5, 2017). The right to data portability allows interested parties to receive the personal data provided by them to the data controller, in a structured format, commonly used and readable mechanically, and to transmit them to a different owner. The ultimate goal is to increase the control of interested parties on their personal data. By allowing the direct transmission of personal data from one data controller to the other, the right to portability also represents an important tool to support the free circulation of personal data in the EU and in favor of competition between cardholders.

1. Premessa

Il Gruppo dell'articolo 29 per la tutela dei dati, noto anche come *Article 29 Working Party* o WP29 è, o per meglio dire era, un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione.

Il gruppo di lavoro è stato costituito sulla base di quanto previsto dall'articolo 29 della direttiva Europea 95/46/CE al fine di perseguire specifiche finalità[73].

Il WP29 è stato sostituito il 25 maggio 2018 dal Consiglio Europeo per la Protezione dei Dati **(**EDPB), ai sensi del Regolamento generale Europeo sulla protezione dei dati 2016/679[74] (cd. GDPR).

Rilevante importanza ha assunto l'introduzione del GDPR in quanto ha previsto una serie di "nuovi diritti" i quali, per loro natura, non sono a "portata generica e generale".

Al contrario: sono diritti mirati a presidiare aspetti essenziali della tutela dei trattamenti di dati personali in un quadro che intende stimolare e favorire lo sviluppo della società digitale. Tra i nuovi diritti, introdotti dal GDPR, un posto centrale è occupato dal diritto alla portabilità dei dati, di cui all'art. 20[75], il quale tiene conto anche delle Linee Guida adottate dal Working Party (WP n. 242 rev.01, rilasciato a dicembre 2016 e rivisto il 5 aprile 2017).

2. Il diritto alla portabilità

Il diritto alla portabilità dei dati permette agli interessati di ricevere i dati personali da loro forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare. L'obiettivo ultimo

[73] In particolare, secondo la direttiva Europea 95/46/CE, il gruppo di lavoro avrebbe dovuto: (i) fornire un parere esperto agli Stati in merito alla protezione dei dati; (ii) promuovere l'applicazione coerente della direttiva sulla protezione dei dati in tutti gli Stati membri dell'UE; (iii) dare alla Commissione un parere sulle leggi comunitarie (primo pilastro) che riguardano il diritto alla protezione dei dati personali; (iv) fornire raccomandazioni al pubblico su questioni relative alla protezione delle persone con riguardo al trattamento dei dati personali e alla privacy nell'Unione Europea.

[74] Il Regolamento generale per la protezione dei dati personali n. 2016/679, d'ora in avanti GDPR (General Data Protection Regulation) è la normativa europea in materia di privacy e di protezione dei dati personali. Esso è stato pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta dal 25 maggio 2018. Il suo principale scopo è stato l'armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.

[75] Art. 20 GDPR: "Diritto alla portabilità dei dati": 1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'art. 6, paragrafo 1, lettera a), o dell'art. 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'art. 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. 2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'art. 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

è accrescere il controllo degli interessati sui propri dati personali, consentendo la trasmissione diretta dei dati personali da un titolare del trattamento all'altro; il diritto alla portabilità rappresenta anche uno strumento importante a supporto della libera circolazione dei dati personali nell'UE ed in favore della concorrenza fra i titolari.[76]

Questo nuovo diritto faciliterà il passaggio da un fornitore di servizi all'altro e potrà, quindi, favorire la creazione di nuovi servizi nel quadro della strategia per il mercato unico digitale.

Questa *ratio* è stata individuata specificamente dal considerando 68 del GDPR, e specificata ulteriormente nelle Linee Guida WP242.

In linea generale, la portabilità dei dati è il diritto di un soggetto di ottenere la restituzione dei propri dati personali forniti ad un'azienda o ad un fornitore di servizi on line e di trasmetterli ad un diverso fornitore (*social network*, fornitori di servizi *internet*, ecc.) ovvero di chiedere la trasmissione dei dati direttamente da un titolare ad un altro.

A prima vista potrebbe sembrare che il diritto alla portabilità dei dati sia una sorta di diritto di accesso rafforzato, ma in realtà opera in una logica e un contesto del tutto diversi.

L'art.20 del GDPR, in particolare, stabilisce che il diritto alla portabilità dei dati è composto da due elementi.

Il primo è rappresentato dal *"diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano"***.**

Come chiarito dalle Linee guida WP 242[77], tale conservazione può avvenire su un supporto personale o su un cloud privato, senza comportare necessariamente la trasmissione dei dati a un altro titolare del trattamento. Sempre le WP 242 ci fanno l'esempio dell'interessato che potrebbe voler recuperare l'elenco dei brani musicali preferiti (o ascoltati) detenuto da un servizio di musica in streaming, per scoprire quante volte ha ascoltato determinati brani o stabilire cosa acquistare o ascoltare su un'altra piattaforma di musica digitale; oppure che potrebbe voler recuperare la rubrica

[76] F. Pizzetti, *Portabilità dei dati nel GDPR: cosa significa e cosa implica questo nuovo diritto,* in *https://www.agendadigitale.eu/sicurezza/portabilita-dei-dati-nel-gdpr-cosa-significa-e-cosa-implica-questo-nuovo-diritto/,* 2019.

[77] W.P. art. 29, Linee guida sul diritto alla portabilità dei dati – WP242, 5.04.2017, in *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.*

dei contatti di posta elettronica su web, magari per costruire una lista degli invitati al proprio matrimonio.

Il secondo elemento della portabilità è *"il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti"*. Sotto questo secondo profilo, il comma 2 dell'art.20 specifica che l'interessato ha *"il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile"***.** Come precisato dalle Linee guida WP 242 su questo punto, il considerando 68 del GDPR promuove lo sviluppo di formati interoperabili da parte dei titolari così da consentire la portabilità dei dati, ma non configura un obbligo in capo ai titolari di introdurre o mantenere sistemi di trattamento tecnicamente compatibili. Pertanto, sempre secondo le Linee guida, occorrerà prestare particolare attenzione al formato dei dati trasmessi in modo da garantire che i dati siano riutilizzabili dall'interessato o da un diverso titolare con un minimo sforzo. Questo aspetto della portabilità dei dati vuole consentire all'interessato di trasmettere i suoi dati a un diverso fornitore di servizi (appartenente allo stesso o a un diverso settore di attività).

Appare opportuno, inoltre, specificare che l'esercizio del diritto di accesso previsto dalla direttiva sulla protezione dei dati (95/46/CE) è vincolato al formato che il titolare decide di utilizzare nel fornire le informazioni richieste.

Il nuovo diritto alla portabilità offre anche la possibilità di "riequilibrare" il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

Invero, l'esercizio di tale diritto, richiede la coesistenza di due presupposti: in primo luogo, ai sensi dell'art 20, 1° co., è previsto che ai fini della portabilità dei dati, il trattamento deve essere fondato sul consenso o su un contratto come base giuridica. Dunque, ad esempio, secondo le Linee guida WP 242 non sussiste alcun obbligo per gli istituti finanziari di ottemperare ad una richiesta di portabilità relativa ai dati personali oggetto di trattamento nell'ambito degli obblighi di prevenzione e di accertamento del reato di riciclaggio o di altri reati finanziari.

In secondo luogo, il diritto alla portabilità dei dati sussiste esclusivamente se il trattamento è *"effettuato con mezzi automatizzati"* e non si applica, conseguentemente, alla maggioranza degli archivi o dei registri cartacei.

Inoltre, a ben vedere, ad una lettura più attenta dell'art 20, in particolare l'ultimo

comma, emerge la sussistenza di un'ulteriore condizione da rispettare in quanto prevede che "*il diritto alla portabilità dei dati non deve ledere i diritti e le libertà altrui*". Sul punto, ad esempio, il WP 242 ci dice che il "nuovo" titolare che ha ricevuto dati personali, a seguito della loro portabilità, non può utilizzare i dati riferiti a terzi per le proprie finalità – per esempio, per proporre offerte di marketing e servizi ai suddetti terzi, o per arricchire il profilo dei terzi interessati e ricostruire il loro contesto sociale – a loro insaputa e senza il loro consenso.

Aspetto altresì rilevante da analizzare è l'individuazione dei dati suscettibili di essere portabili. Sul punto sempre l'art.20 del GDPR ci dice che devono essere portabili i dati personali che *"riguardano"* l'interessato e che sono stati da lui *"forniti a un titolare del trattamento"*, in particolare il l'WP 242 fa l'esempio delle informazioni inserite in un modulo di registrazione online, come l'indirizzo postale, il nome utente, l'età, ecc., ma anche dei dati derivanti dall'osservazione delle attività svolte da tale interessato, quali, ad esempio, la cronologia della navigazione su un sito web o delle ricerche effettuate; mentre non appartengono a quest'ultima categoria i "*dati inferenziali*" e "*dati derivati*", cioè quelli generati dal titolare, utilizzando come input i dati osservati o forniti direttamente, per esempio il profilo-utente creato a partire dall'analisi dei dati grezzi generati da un contatore intelligente[78].

3. Cenni sul procedimento.

Dal punto di vista procedimentale, appare a tal uopo opportuno soffermarci brevemente su alcuni aspetti rilevanti. Innanzitutto, gli articoli 13 e 14 del GDPR prescrivono che i titolari del trattamento di dati personali devono informare gli interessati dell'esistenza di tale diritto e l'WP 242 afferma che, nel dare l'informativa, i titolari devono aver cura di distinguere il diritto alla portabilità da altri diritti primo tra tutti il diritto di accesso. Espressamente l'art.20, co.3 GDPR afferma che il diritto alla portabilità dei dati lascia impregiudicato il diritto alla loro cancellazione previsto all'art. 17 del medesimo Regolamento.

Quanto alla tempistica, in base all'articolo 12, paragrafo 3 GDPR, il titolare fornisce *"informazioni relative all'azione intrapresa"* all'interessato *"senza ingiu-*

[78] E. Pelino, C. Bistolfi, L. Bolognini, *Il regolamento privacy europeo: commentario alla nuova disciplina europea sulla protezione dei dati, in vigore da maggio* 2016, Milano, 2016.

stificato ritardo" e comunque *"entro un mese dal ricevimento dalla richiesta"* ovvero, in casi di particolare complessità, entro un massimo di tre mesi, purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale. I titolari devono rispettare l'obbligo di ottemperare nei termini previsti, anche in caso di diniego. In altri termini, l'inattività non è ammessa qualora un titolare riceva una richiesta di portabilità[79].

Poi il WP 242 suggerisce che *"il ricorso a sistemi automatizzati quali le interfacce di programmazione di applicazioni (API, Application Programming Interfaces) può facilitare le interazioni con l'interessato e, quindi, ridurre gli oneri"***.**

Dopo di che i dati devono essere trasmessi, a norma dell'art.20 GDPR, *"senza impedimenti da parte del titolare cui li hanno forniti***.** Inoltre, l'articolo 20, paragrafo 2, obbliga il titolare a trasmettere i dati portabili direttamente a un diverso titolare *"se tecnicamente fattibile"*. Il WP 242 chiarisce che sul piano tecnico, i titolari dovrebbero esplorare e valutare due approcci diversi e complementari per mettere a disposizione degli interessati o di altri titolari dati che siano portabili: - trasmissione diretta dell'intero insieme di dati portabili; - utilizzo di uno strumento automatizzato che consenta l'estrazione dei dati pertinenti. Per implementare questi due approcci, il WP suggerisce, poi, varie metodologie, cui rinvio.

Quanto al formato previsto per i dati, l'articolo 20, paragrafo 1, del GDPR stabilisce che i dati personali devono essere forniti *"in un formato strutturato, di uso comune e leggibile da dispositivo automatico"***.** Nel considerando 68 si chiarisce ulteriormente che il formato in questione dovrebbe essere *"interoperabile"*. Come chiarito dalle Linee guida WP 242, l'interoperabilità – peraltro lì meglio definita - è l'obiettivo finale, mentre i termini *"strutturato"***,** *"di uso comune"* e *"leggibile da dispositivo automatico"* sono specificazioni dello strumento da utilizzare; e ancora, *"qualora non vi siano formati di impiego comune in un determinato settore di attività o in un determinato contesto, i titolari dovrebbero fornire i dati personali utilizzando formati aperti di impiego comune (per esempio: XML, JSON, CSV, ecc.) unitamente a metadati utili, al miglior livello possibile di granularità, mantenendo un livello elevato di astrazione"*.

[79] M.G. Bloise, *GDPR, Diritto alla portabilità dei dati: cos'è e cosa comporta*, in *Giuricivile,* 9, 2018, *https://giuricivile.it/gdpr-portabilita-dei-dati/.*

4. Conclusioni.

L'interoperabilità è essa stessa uno strumento di qualità perché è strumento di «trasparenza»: non ci si può nascondere dietro pratiche scorrette o adozione di standard di cattiva qualità. Anzi, i titolari sono incoraggiati a migliorare la qualità dei propri processi di gestione dei dati sia per trattenere i propri clienti che per evitare cattiva reputazione.

A norma dell'art.83, comma 5 GDPR la violazione dei diritti degli interessati (ivi compreso, quindi, quello alla portabilità dei dati) potrebbe dare luogo a sanzioni amministrative pecuniarie fino a euro 20.000.000,00, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (salvi, comunque, naturalmente, i criteri generali di graduazione delle sanzioni). Non si tratta, dunque, di un obbligo da prendere in scarsa considerazione.

Queste riflessioni ci inducono a riflettere sulla reale portata di tale "nuovo diritto".

Vengono messi in gioco interessi economici molto rilevanti e la tutela di diritti di primario livello che devono trovare un equilibrio non solo con la tutela dei dati ma anche con altri diritti, anche economici, di pari valore, come la libertà di concorrenza che è sottesa al diritto alla portabilità dei dati in quanto finalizzata anche a facilitare la scelta tra fornitori diversi del medesimo servizio, evitando pratiche di "*lock-in tecnologico*" da parte del precedente titolare[80].

Il diritto alla portabilità dei dati, però, non si limita a "potenziare il controllo dei singoli sui dati personali che li riguardano assicurando agli interessati un ruolo attivo nell'ecosistema delle informazioni", ma favorisce anche la libera circolazione dei dati stimolando l'economia digitale.

[80] Lo scopo della portabilità dei dati è quello di aprire il mercato e mettere in gioco delle alternative. Ciò in quanto, gli effetti distorsivi sulla concorrenza dell'azione dei giganti del *web* (*google, facebook*, ecc.) non sono ancora abbastanza percepiti; uno dei motivi principali che consente loro di avere tanto potere è proprio il possesso esclusivo dei dati personali. Eppure il processo di attuazione della portabilità dei dati comporterà un lungo tempo di adattamento, in quanto l'interoperabilità dei dati è più facile nei settori, come quello bancario, in cui già opera la concorrenza e più difficile in quelli come i motori di ricerca o nei *social network*. Cfr. L. De Biase, *Il mercato dei dati personali tra portabilità e concorrenza*, 2019, in *https://www.il-sole24ore.com/art/il-mercato-dati-personali-portabilita-e-concorrenza--AEcVl26E*.

Garantire il trasferimento dei propri dati da un servizio online ad un altro promuove la concorrenza tra aziende, e l'innovazione e lo sviluppo di nuovi servizi. Esercitando il suo diritto, infatti, l'interessato può facilmente spostare un contratto di servizi ad altro gestore senza dover fornire nuovamente tutti i suoi dati ma semplicemente chiedendo al vecchio gestore di trasportare i dati al nuovo gestore.

Con in più un "effetto collaterale" notevole: il diritto alla portabilità, favorendo la condivisione controllata e limitata delle informazioni personali fra più soggetti, consente *de facto* anche di arricchire l'esperienza dell'utente nella fruizione di servizi sempre più tecnologici, nonché di favorire "*cross-sector data flows*", cioè la trasmissione e il riutilizzo di dati personali fra più servizi di interesse per il singolo utente.

Coordinamento editoriale:
Gruppo di lavoro *Data Protection Law*

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it