UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"TRATTAMENTO DEI DATI PERSONALI E SOCIAL NETWORK: ALCUNE QUESTIONI"

RELATORE:

CH.MO PROF. LAURENCE KLESTA

LAUREANDO/A: GIADA NAUVA

MATRICOLA N. 1114591

ANNO ACCADEMICO 2017 – 2018

INDICE

Introduzione

Il tema scelto per la prova finale riguarda la privacy o per meglio dire la protezione dei dati personali. Questa materia è molto attuale in quanto in tutta l'Unione Europea si sta assistendo a un processo di sostituzione delle norme in vigore. Infatti, dal 25 maggio 2018 è entrato in vigore il nuovo Regolamento europeo in materia di protezione dei dati personali che va a sostituire la precedente Direttiva 95/46/CE, portando così l'onere ai vari Stati di adeguarsi al nuovo ordinamento.

Nella prima parte dell'elaborato si esaminerà il nuovo testo normativa nelle sue parti più rilevanti, preoccupandosi anche di portare in rilievo eventuali differenze riscontrate con il vecchio ordinamento.

Nella seconda parte, invece, si prenderanno in esame due casi riferiti a due argomenti molto importanti: il diritto all'oblio e il contrasto alle frodi fiscali.

Si cercherà di capire come la giurisprudenza CEDU si pronuncia in merito al caso Fuchsmann c. Germania incentrato sul delicato diritto all'oblio disciplinato nel nuovo Regolamento UE 679/2016. Si tenterà in questo modo di comprendere meglio questo nuovo diritto disciplinato dal Regolamento in vigore.

In questa parte dell'elaborato si guarderà anche alle frodi fiscali, analizzando come la Corte di giustizia europea chiamata a pronunciarsi in merito al caso Puskar c. Repubblica slovacca, riconosca alle autorità competenti il compito e la possibilità di stilare liste di soggetti sospettati di frode per poter combattere questo problema.

1 Il Regolamento UE 679/2016

1.1 Oggetto e finalità e ambito di applicazione materiale e territoriale

Il nuovo Regolamento in materia di dati personali presenta alcune differenze rispetto al precedente testo normativo, principalmente nell'oggetto e finalità dello stesso e nel suo campo di applicazione territoriale. L'evoluzione della normativa è dovuta a un sostanziale impegno da parte del legislatore di normare le zone d'ombra che nel corso degli anni, con lo sviluppo della tecnologia, si erano andate a formare.

Dalla lettura dell'articolo 1 del Regolamento UE 2016/679 si può sin da subito notare i punti d'interesse di tale normativa: la tutela delle persone fisiche in riferimento al trattamento dei dati personali e la circolazione dei dati.
Come si può ben immaginare questi due temi sono molto collegati tra loro sopratutto nel caso di proteggere i dati quando questi vengono passati "di mano in mano".
Il problema della circolazione delle informazioni è diventato sempre più centrale con lo sviluppo tecnologico, difatti sono sempre di più i mezzi con cui si possono trasferire dati.
Il testo normativo vigente si prefigge il compito di tutelare le persone fisiche in materia di trattamento dei dati personali come sancito dallo stesso articolo 1, proteggendo i diritti e le libertà dei cittadini "in particolare il diritto alla protezione dei dati personali". È questa una novità introdotta ex novo dal Regolamento. Nella precedente Direttiva, difatti, si parla di "diritto alla vita privata" ovvero di "privacy".
Bisogna precisare che questi due diritti sono diversi tra loro, anche se potrebbe non sembrare così. Con il "diritto alla vita privata" si riferisce sostanzialmente "al diritto ad essere lasciati indisturbati e fondato sul criterio di esclusione degli altri dalla propria sfera privata"[1]. Con l'avvento della tecnologia e dei social network questo diritto ha iniziato, per così dire, a presentare i primi segnali di debolezza. In un mondo dove ogni giorno si condividono informazioni personali attraverso l'uso di Internet, questo diritto alla privacy è stato sostituito con il più ampio "diritto alla protezione dei dati personali". Quest'ultimo si riferisce alla facoltà che gli individui hanno di controllare come gli altri trattino i propri dati, avendo anche il potere di richiedere la loro rettifica o la loro cancellazione.
Questa protezione dei dati, come già anticipato, è sempre più importante, considerando che con lo sviluppo tecnologico, in ogni momento della giornata tutti gli individui sono tracciabili. A questo riguardo è necessario ricordare che oltre ai servizi di geolocalizzazione che permettono di individuare fisicamente un soggetto, ci sono altri metodi che consentono di

[1] SOFFIENTINI M., 2016. *Privacy.*

"seguire" un individuo. Si pensi alle tracce che si lasciano ogni qualvolta che si fa un acquisto in Internet o che si fa una semplice ricerca. In tutti questi casi milioni di dati vengono resi disponibili in rete senza che l'interessato ne sia consapevole. È per questo motivo che è indispensabile che ci sia un ordinamento che tuteli e permetta la protezione dei dati personali.

Il diritto alla protezione dei dati personali, così come il diritto alla circolazione dei dati, non è, però, un diritto assoluto altrimenti sarebbe necessaria solo una regola ovvero "vietato trattare dati". Invece va considerato alla luce della sua funzione sociale collegato anche al principio di proporzionalità, in altre parole i dati che vengono manipolati possono essere usati esclusivamente ai fini per cui sono stati inizialmente raccolti[2].

Bisogna precisare che i beneficiari di questo Regolamento sono le persone fisiche e di conseguenza non si può invocare la sua applicazione per la protezione di dati riferiti a persone giuridiche.

Anche un'organizzazione può avere ambiti di riservatezza e di tutela ma queste vengono regolate da altre tutele, diverse da quelle esaminate in questo elaborato.

Pertanto i soggetti oggetto d'interesse per questa disciplina sono le persone fisiche "viventi". Questo attributo è fondamentale poiché il Regolamento esclude espressamente le persone decedute dal suo campo di applicazione. Il considerando 27, però, precisa che è salva la volontà degli Stati membri di prevedere norme che regolino questo aspetto.

Il legislatore europeo ha riservato, poi, gli articoli 2 e 3 alla definizione dell'ambito applicativo rispettivamente materiale e territoriale.

In generale le disposizioni oggetto del Regolamento 2016/679 si applicano sia al trattamento automatizzato sia al trattamento non automatizzato dei dati personali con la particolarità che questi ultimi devono essere contenuti in un archivio o destinati a figurarvi. Questo campo di applicazione trova tuttavia delle limitazioni sancite espressamente dal comma 2 dell'articolo 2 che recita: “Il presente regolamento non si applica ai trattamenti dei dati personali:

- effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- effettuati dalle autorità competenti ai fini di prevenzione, indagini, accertamento o perseguimento di reati o di esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.”

[2] CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo.*

Il presente articolo sostanzialmente rimane invariato rispetto a quanto stabilito dalla Direttiva 95/46/CE, cambia invece significativamente l'ambito territoriale.

Per la normativa abrogata le disposizioni in materia di tutela e protezione dei dati personali trovavano applicazione tramite attuazione da parte dei singoli Stati soltanto quando il trattamento fosse effettuato nel contesto delle attività di uno stabilimento del titolare situato nell'UE.

Diverso è invece quanto disposto dal nuovo Regolamento entrato in vigore il 25 maggio 2018. Come anticipato in precedenza l'articolo di riferimento è il 3 rubricato proprio come "ambito di applicazione territoriale".

Questo articolo si può esaminare da due punti di vista: se si considera il soggetto che tratta i dati, se questo è stabilito nell'Unione Europea, anche se il trattamento avviene al di fuori di questa, la normativa da seguire e applicare è quella del Regolamento 2016/679.

In questo caso ciò che conta è la nazionalità del soggetto, se è "europeo" deve continuare ad applicare la normativa europea anche nel caso in cui decidesse di trasferire il trattamento in uno Stato non membro.

Una seconda ipotesi è prendere in considerazione l'ubicazione dell'interessato cioè della persona fisica a cui i dati si riferiscono. In questo caso, se si trova nell'Unione si applica il Regolamento che si sta esaminando.

"Trovarsi nell'Unione" si riferisce a "qualsiasi situazione (reale o virtuale) che collega la persona fisica al territorio europeo"[3].

Questa seconda ipotesi, però, si verifica solo quando ricorrono due situazioni tra loro alternative. Il secondo comma, infatti, prevede l'applicazione della legge europea quando il trattamento riguarda:

- "l'offerta di beni o la prestazioni di servizi ai suddetti interessati dell'Unione, indipendentemente dalla obbligatorietà di un pagamento dell'interessato;
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Le multinazionali come Google, Facebook, Apple o Microsoft hanno da sempre sostenuto che per le loro attività non trovavano applicazione le disposizioni europee in quanto non avevano alcun stabilimento nell'UE, ma solo agenzie di vendita commerciali di servizi. Per questi colossi, di conseguenza, il trattamento di dati non avveniva nel territorio europeo e quindi legittimati a non sottostare alle sue norme.

Con la stesura del nuovo testo normativo, il legislatore ha voluto superare questa lacuna normativa che si era creata, recependo l'orientamento che la Corte di giustizia aveva messo in

[3] CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo.*

atto. Infatti, la sentenza principe di questa evoluzione è quella sul caso Google Spain, nella quale si afferma che "anche solo la vendita di servizi compiuta nel territorio nazionale delle sedi di rappresentanza delle società fornitrici di servizi si configura come un trattamento dati, e quindi si legittima l'applicazione della normativa europea"[4].

Questo cambiamento di applicazione territoriale ha conseguenze negative nelle aziende fornitrici di servizi Internet (service provider), soprattutto quelle stabilite in Paesi extra-europei, USA in primis, dove le garanzie a protezione dei dati personali sono molto inferiori rispetto a quelle richieste dall'Unione Europea.

A conclusione di quanto esaminato si deve richiamare l'articolo 27 comma 1 nel quale si afferma che "ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione."

Un ultimo caso preso in esame dall'articolo 3 e al quale si applica il presente Regolamento riguarda il trattamento dei dati personali "in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico."

1.2 Dato personale

Il Regolamento europeo 2016/679 si concentra sulla protezione dei dati personali dei cittadini. Rispetto alla Direttiva 95/46/CE, il vigente testo normativo riporta una definizione di "dato personale" più ampia e dettagliata. Questo ampliamento della nozione è dovuto di fatto alla tecnologia, si pensi alle telecamere di videosorveglianza o a innovativi sistemi medici. Il legislatore, di conseguenza, cerca sempre più di entrare nello specifico per non lasciare nulla nello spazio del non disciplinato introducendo le definizioni di "dati genetici" o "biometrici" e ancora introducendo la "pseudonimizzazione".

In base alla lettura dell'articolo 4, si può considerare dato personale "qualsiasi informazione riguardante una persona identificata o identificabile ("interessato")." La definizione continua precisando che "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero d'identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."

E' proprio in questa seconda parte di definizione che si nota la differenza con la precedente disposizione, nella quale non si faceva riferimento ad alcun esempio di identificativi.

[4] Sentenza della Corte di giustizia sul caso *Google inc. e Google Spain* del 13 maggio 2014.

Per comprendere meglio la nuova formulazione bisogna prendere in esame anche alcuni considerando del Regolamento, in cui viene affermato che: “per stabilire l’identificabilità di una persona è opportuno considerare tutti i mezzi, come l’individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica, direttamente o indirettamente”[5].

Per identificare una persona è quindi sufficiente la sua individuazione all'interno di un contesto. Un esempio può essere quello dei vicini di casa; infatti non è necessario conoscere il loro nome per essere in grado comunque di identificarli.

Inoltre non è rilevante che la persona fisica sia individuabile da chiunque, basta che questa lo sia da qualcuno in una specifica circostanza di luogo e di tempo.

Un'ulteriore precisazione, la definizione di “dato personale” non è relativa bensì assoluta. Questo sta a significare che il fatto che solo alcuni soggetti siano in grado di individuare un interessato non significa che questo sia “dato personale” solo per questi soggetti. Bisogna ricordare che una volta che l'informazione è definita come “dato personale” in un contesto, questa lo è in ogni altro contesto. Ciò porta anche alla conseguenza che un “titolare di trattamento” potrebbe non conoscere l'identità dell'interessato.

Come detto sopra, una persona può essere identificata in modo diretto o indiretto. Alcuni esempi di identificativi da considerare diretti sono: il nome anagrafico, l'immagine della persona, la voce o le rappresentazioni visive. Per quanto riguarda quelli indiretti, si pensi a una targa automobilistica, al codice fiscale, al numero di telefono o, ancora, a una mail o a un indirizzo IP.

A questo proposito bisogna ribadire che è lo stesso Regolamento che menziona espressamente gli indirizzi IP, infatti se si legge il considerando 30 questo recita “le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle”. Questo quindi conferma la qualificazione degli indirizzi IP come dati personali e di conseguenza legittimati a essere tutelati.

Una novità introdotta ex novo dal Regolamento europeo riguarda la definizione della “pseudonimizzazione”, non presente nella precedente Direttiva n. 46/1995. La “pseudonimizzazione” si riferisce al fatto che i dati personali raccolti non possono essere ricondotti ad alcuna persona fisica identificata o identificabile. Questo processo, infatti, è

[5] Considerando 26 del Regolamento UE 679/2016.

possibile solo con l'aiuto di informazioni aggiuntive con la conseguenza, dunque, che queste siano conservate separatamente dal resto dei dati rendendo impossibile il collegamento con l'interessato specifico. Si può definire, pertanto, come un processo utilizzato per mascherare l'identità quell'individuo ma non per cancellare tutte le informazioni che permettono la sua identificazione.

I dati pseudonimizzati ricadono in qualunque modo nel campo applicativo del Regolamento europeo preso in esame, in quanto si riferiscono a dati personali riconducibili a "una persona identificata o identificabile". Bisogna precisare, però, che questo tipo di dati presentano un minor grado di rischio concreto per i diritti fondamentali, lasciando così maggior spazio di manovra per i titolari e responsabili[6].

Il Regolamento europeo, al considerando 26, si sofferma sui dati anonimi. Leggendo il considerando si arriva alla conclusione che i principi di protezione dei dati personali non vengono presi in causa per quelle informazioni considerate anonime, "vale a dire informazioni che non si riferiscono a una persona identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato". Questo significa che il Regolamento non trova applicazione per le informazioni anonime utilizzate per fini statistici o di ricerca.

Quello dell'anonimizzazione è un aspetto importante nel caso di dati conservati oltre l'utilità della finalità per cui sono stati raccolti. Tanto è vero che in questo caso la legge chiede che i dati vengano resi anonimi.

Al giorno d'oggi nessun individuo dovrebbe essere discriminato per il colore della pelle o per le sue idee politiche o religiose. Non si dovrebbe quindi prendere in considerazione l'origine etnica o la religione professata per poter identificare una persona o per classificare un gruppo. Queste informazioni sono dati aggiuntivi riferibili a una persona ma che non devono costituire un mezzo per etichettare un individuo.

E' proprio per questo motivo di non discriminazione che questi dati vengono considerati meritevoli di tutela; il nostro "Codice della privacy" italiano li definisce come "sensibili".

Per la normativa italiana sono "dati sensibili", infatti, l'insieme di "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale".

[6] PIZZETTI F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.*

Questa categoria di dati rispecchiano quelli dell'articolo 9 del Regolamento UE 2016/679 rubricato “trattamento di categorie particolari di dati personali”.

Dalla lettura della norma s’individuano altri tipi di dati oltre a quelli citati qui sopra che la nuova normativa europea definisce meritevoli di tutela.

I primi sono i “dati genetici” qualificati come “dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall’analisi di un campione biologico della persona fisica in questione”.

Nella nozione di dato personale il Regolamento 679 del 2016 introduce anche i “dati biometrici”, ovvero “i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici” e ancora quelli relativi alla salute “attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”.

Concorrono a una migliore comprensione di ciò che si intende “dati genetici” e “relativi alla salute” i considerando 34 e 35, nei quali sono riportati esempi di ciò che rientra in una o nell'altra categoria e che per completezza di informazione si riportano in nota[78].

Come già detto, queste tipologie di dati si trovano all'interno dell'articolo 9. Come suggerito dalla rubrica della norma appena menzionata, il Regolamento prevede che questi dati siano soggetti a un trattamento speciale di cui se ne parlerà più avanti nel capitolo dedicato proprio al trattamento.

È importante ricordare che per la qualificazione di un dato come soggetto a trattamento speciale, bisogna tenere conto del contesto. Ad esempio, l'immagine di un individuo che indossa abiti religiosi non è considerata dato soggetto a trattamento speciale, in quanto l'individuo in questione esercita la sua professione, così come non lo è l'immagine di un politico ritratta col simbolo del partito. Invece, l'immagine di una persona che entra in un luogo di culto o in una sede di partito è dato soggetto a trattamento speciale in quanto è indice della scelta effettuata.

[7] (34) “E’ opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall’analisi di un campione biologico della persona fisica in questione, in particolare dall’analisi dei cromosomi, dell’acido desossiribonucleico (DNA) o dell’acido ribonucleico (RNA), ovvero dall’analisi di un altro elemento che consenta di ottenere informazioni equivalenti.”

[8] (35) “Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell’interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono […] un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; […].”

A conclusione di questa disamina si ricorda, come già menzionato precedentemente in questo elaborato, come sia per la Direttiva 95/46 che per il vigente Regolamento europeo i dati meritevoli di tutela e protezione siano quelli riferiti alle persone fisiche escludendo in toto le persone giuridiche.

1.3 Trattamento e soggetti del trattamento

Il trattamento e i suoi soggetti hanno subito modificazioni all'interno del nuovo ordinamento europeo. In modo particolare si hanno avuto novità in tema di consenso degli interessati e nella nascita e intensificazione dei soggetti adibiti al trattamento dei dati personali raccolti, attribuendogli anche l'onere della responsabilizzazione, divenuta anch'essa un principio da osservare.

1.3.1 Principi

Le prime disposizioni in materia di trattamento si trovano al Capo II. Il GDPR, qui infatti, ribadisce i principi che sono alla base del trattamento dei dati, confermando di fatto quanto già disposto nella precedente Direttiva in materia di tutela del trattamento dei dati personali.
Prima di iniziare ad esaminare in dettaglio i vari principi, bisogna però chiarire a cosa ci si riferisce con il termine “trattamento”.
A questo proposito viene in aiuto, ancora una volta, l'articolo 4 che definisce il trattamento come “qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali” proseguendo con un lungo elenco di esempi che per comodità viene riportato in nota[9]. Questo concetto necessita però di una precisazione, infatti, con l'espressione “trattamento” ci si riferisce a qualsiasi attività svolta sui dati personali, dunque anche il mero accesso ai dati.
Questa puntualizzazione viene confermata anche dal provvedimento del Garante della privacy in materia di videosorveglianza pubblicato nella Gazzetta Ufficiale il 29 aprile 2010 n. 99. Questo provvedimento, infatti, accerta come la videosorveglianza senza registrazione venga considerata una tipologia di trattamento.

[9] Art. 4 Regolamento UE 679/2016, «trattamento»: “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione.”

Come detto in precedenza, il Regolamento 2016/679 dedica l'articolo 5 ai “Principi applicabili al trattamento dei dati personali”.

Dalla lettura della norma si nota come la lettera a) impone i primi tre principi, ovvero quelli della liceità, della correttezza e infine della trasparenza.

Per quanto riguarda il primo dei principi citati, per comprendere il suo significato bisogna ricorrere ai considerando 44 e 46. Nello specifico, il trattamento è da considerarsi lecito “se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto” e ancora “è altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica”.

Questo principio viene integrato nell'articolo 6 “Liceità del trattamento” dove si fa una lunga elencazione di condizioni che permettono di qualificare il trattamento come lecito. È da precisare, come riportato nell'articolo stesso, che basta che venga soddisfatta una delle condizioni perché ci sia questa qualificazione.

Un principio introdotto ex novo dal Regolamento europeo, invece, riguarda la trasparenza del trattamento.

Secondo il considerando 39 “il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro”.

La trasparenza viene collegata all'informazione sulle modalità e finalità del trattamento[10]. Lo si può ben notare riprendendo il considerando 39 quando afferma che dovrebbero essere trasparenti “le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali [...] nonché la misura in cui i dati personali sono o saranno trattati”.

Viene anche confermato dalla presenza dell'articolo 12 (“Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato”) contenuto nella Sezione 1 intitolata “Trasparenza e modalità” del Capo III del Regolamento.

Il nuovo Regolamento è molto attento anche alla nuova realtà digitale che con l'evoluzione comporta difficoltà per gli interessati a comprendere quali siano i dati trattati e con quali finalità. Al giorno d'oggi le informazioni circolano in maniera frenetica grazie l'avvento di social network ed Internet in generale. Per questo il considerando 58 richiede l'applicazione del principio di trasparenza anche quando le informazioni vengono “fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell’operazione fanno sì che sia difficile per l’interessato comprendere se, da chi e per quali

[10] PIZZETTI F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.*

finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online", inoltre continua tutelando i bambini sulla rete "dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente".

Tornando al principio di liceità, un tema fondamentale e molto importante riguarda il consenso dell'interessato. Questo istituto è cruciale per il trattamento dei dati in quanto rappresenta una condizione legittimante del trattamento stesso.

Per il Regolamento in vigore il consenso è "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".

L'interessato deve quindi manifestare il consenso in modo inequivocabile mediante dichiarazione scritta, anche con l'utilizzo di mezzi elettronici, o in forma orale. In altre parole il soggetto deve compiere un'attività positiva e di conseguenza non si può considerare consenso il silenzio, l'inattività o la precompilazione di caselle. È da sottolineare che il consenso, nel caso di trattamento con molteplici finalità, deve essere prestato per tutte queste.

Un ambito importante quando si parla di consenso del trattamento dei dati è sicuramente quando questo avviene in rete. In questi casi, come ripetuto più volte, grandi mole di dati vengono continuamente trasferiti e immessi nel web ed è quindi necessario che gli utenti siano informati delle finalità del trattamento dei loro dati personali.

Con l'avvento dei social network ogni giorno foto e informazioni che rientrano nella sfera dei dati personali degli individui vengono trasmessi in rete con il rischio che altri possano usufruirne senza il loro consenso. È per questo che nella nuova legge europea si è imposto che la richiesta del consenso in Internet deve essere chiara e concisa. Rientra in questo campo d'interesse i "cookies", ovvero quei piccoli trafiletti che si aprono ogni qualvolta si visita un sito web. Il nuovo Regolamento ha disposto che per questi strumenti sia necessario ricevere il consenso da parte degli interessati, spiegando come vengono utilizzate le informazioni raccolte.

Il Garante della privacy si è espresso in tale materia precisando che per quanto riguarda i cookies tecnici o di sessione non è richiesto il preventivo consenso degli utenti. Il provvedimento del Garante precisa che questi cookies sono utilizzati "al solo fine di effettuare la trasmissione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio". Essi quindi non vengono utilizzati per

scopi ulteriori e, come già precisato, non è richiesto il preventivo consenso ma rimane ugualmente necessaria un'informativa.

Diverso è quanto disposto per i cookies di profilazione ovvero "volti a creare profili relativi all'utente e utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell´ambito della navigazione in rete. In ragione della loro particolare invasività nella sfera privata degli utenti, la normativa europea prevede che l´utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere così il proprio consenso"[11].

Tutte le condizioni necessarie per il consenso vengono normate dall'articolo 7 del nuovo testo normativo rubricato espressamente "condizioni per il consenso".

Una tutela particolare è riservata ai minori che sempre più spesso usufruiscono del mondo tecnologico. Viene disposto, infatti, che il consenso e quindi il trattamento dei dati è lecito solo se il minore ha compiuto il sedicesimo anno di età. Al di sotto di questa soglia, pertanto, è indispensabile che il consenso venga fornito da un genitore. Per la verità la disposizione lascia una certa libertà agli Stati membri in riferimento all'età del minore imponendo, però, come limite invalicabile i 13 anni.

Il presente articolo chiede al titolare del trattamento di adoperarsi per verificare che il consenso provenga effettivamente dal lato genitoriale, tenendo conto delle tecnologie disponibili.

Per quanto riguarda le particolari categorie di dati, definiti "sensibili", l'articolo 9 prevede espressamente il divieto di trattamento. Il presente articolo, però, predispone anche delle cause di esclusione di questo divieto che elenca nel secondo paragrafo. In questi casi per il trattamento dei dati è richiesto il consenso, ma questa volta deve avvenire per iscritto non essendo concesso un'altra tipologia di forma.

L'articolo 5, comma 2, introduce il cosiddetto principio di responsabilizzazione (o dell'accountability). Questo principio, come disposto dall'articolo 24, chiede al titolare del trattamento "di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento".

Come specificato nei considerando, le misure adottate dovrebbero "tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento", ma anche del rischio per i diritti e le libertà delle persone fisiche. Questi rischi possono derivare dal trattamento di dati suscettibili di cagionare un danno fisico, materiale o immateriale come può essere una discriminazione o un furto d'identità.

[11] Provvedimento 8 maggio 2014 [doc. web n. 3118884] "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" (G.U. n. 126 del 3 giugno 2014);
Comunicato stampa 4 giugno 2014 "Internet: Garante privacy, no ai cookie per profilazione senza consenso".

Come si può ben capire, quindi, la protezione dei dati viene affidata al titolare del trattamento che deve deciderne le modalità, le garanzie e le limitazioni nel rispetto delle disposizioni normative.
Come sottolinea il Garante della privacy, per rispettare il principio di responsabilizzazione si devono rispettare criteri imposti dall'articolo 25, ovvero “privacy by design” e “privacy by default”.
Il primo dei due criteri si riferisce quindi alla protezione dei dati fin dalla progettazione. E' una modalità di riduzione del trattamento dei dati ex ante. Questo porta a valutare il rischio preventivamente e determinare così la responsabilità del titolare o del responsabile del trattamento.
Il “privacy by default” si sostanzia nell'adozione di misure tecniche e organizzative come la pseudonimizzazione o la minimizzazione, per garantire che vengano trattati solo i dati necessari per le finalità che si vogliono perseguire. In altre parole significa che la tutela della protezione dei dati deve divenire l'impostazione predefinita. Secondo questo principio, inoltre, non deve consentirsi l'accesso dei dati a una grande mole di persone fisiche ma ci deve essere l'intervento di una persona fisica individuata cui assegnare i poteri di accesso.

1.3.2 Soggetti del trattamento

Data la complessità del trattamento e della protezione dei dati, il Regolamento richiede espressamente l'individuazione di varie figure con rispettivi compiti. Nell’odierna era tecnologica, come ricordato più volte, la mole di dati che circolano nel web è consistente e quindi il legislatore europeo cerca il più possibile di regolare il suo trattamento e assicurare la protezione dei dati che vengono raccolti dai vari soggetti. È per questo che impone l'individuazione di figure come il titolare, rappresentante e responsabile del trattamento, alle quali si accosta e aggiunge il responsabile della protezione dei dati, il cosiddetto DPO (Data Protection Officer).

Tra le definizioni dell'articolo 4 del nuovo Regolamento troviamo specificazioni alle figure del titolare del trattamento, del responsabile del trattamento e del rappresentante. Così si chiarisce che per titolare del trattamento s’intende “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali”. Il titolare è il capo che decide, ma è anche

quello che sopporta le conseguenze dei trattamenti effettuati[12]. È per questo motivo che all'articolo 24 si parla di responsabilità del titolare del trattamento. Il "principio dell'accountability" sopra analizzato coinvolge in pieno il titolare.

Il Regolamento 2016/679 prevede anche la possibilità di avere una contitolarità del trattamento. Questa ipotesi viene regolata dall'articolo 26 affermando che si ha contitolarità "quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento".

In questi casi i soggetti devono preoccuparsi di redigere un accordo dove vengono specificati alcuni punti. Questo è abbastanza intuitivo, infatti, l'interessato deve sapere che i suoi dati saranno trattati da due o più titolari. È proprio ciò che si deve dare voce nell'accordo: per essere a norma quindi i contitolari dovranno chiarire le responsabilità di ognuno in riferimento agli obblighi previsti dal Regolamento europeo. Di questo accordo dovrà essere informato il proprietario dei dati personali raccolti in modo che quest'ultimo possa esercitare i diritti a esso riconosciuti.

Come già anticipato precedentemente in questo elaborato, qualora il titolare del trattamento non è stabilito nel territorio dell'Unione, ma il Regolamento prevede comunque l'assoggettamento del trattamento alla normativa europea (si veda articolo 3, comma 2), si deve nominare per iscritto un rappresentante nell'Unione Europea.

Bisogna precisare, però, che l'articolo 27 del Regolamento UE 2016/679 disciplina questa materia e prevede al secondo comma due situazioni in cui decade l'obbligo della nomina: esenti da questo obbligo sono infatti le autorità e gli organismi pubblici oppure il trattamento occasionale.

Altra figura necessaria e obbligatoria in materia di trattamento dei dati è quella del responsabile del trattamento. Questo soggetto è designato dal titolare del trattamento tenendo conto delle capacità proprie del soggetto in tema di privacy. Il responsabile agisce sotto le dipendenze del suo designatore che indica la strada maestra dell'operato. Per essere precisi quindi, il responsabile viene nominato con un contratto o "da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri" come disciplinato dall'articolo 28. All'interno di questo atto si delineano le misure entro le quali il responsabile può agire. Questo è molto importante in quanto la responsabilità ricade sul titolare del trattamento, ciò, però non avviene nel caso in cui il responsabile ecceda tali limiti. In quest'ultima ipotesi il responsabile sarà anch'esso responsabile delle sue azioni divenendo quindi una sorta di contitolare.

Il titolare e il responsabile del trattamento condividono gli stessi obblighi disciplinati nel Regolamento UE 2016/679 nel Capo IV alla Sezione I rubricata "Obblighi generali". In

[12] CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo.*

particolare queste due figure del trattamento dati sono tenute a predisporre un registro delle attività di trattamento, ex articolo 30. Questa disposizione disciplina il contenuto dei presenti registri, che per comodità si rimanda all'articolo.

Il titolare e il responsabile sono i principali responsabili anche per quanto concerne la sicurezza dei dati raccolti e trattati. A tal proposito si richiede l'applicazione di misure volte a proteggere i dati come per esempio l'utilizzo della pseudonimizzazione.

Il trattamento dei dati è un mondo molto delicato e pieno di pericoli. È necessario che le informazioni a disposizione dei soggetti autorizzati siano protette e al sicuro. È per questo motivo che il legislatore europeo ha imposto l'obbligo di comunicazione all'autorità di controllo da parte del titolare del trattamento in caso di violazione dei dati personali. Qualora sia il responsabile ad accorgersi di questa evenienza deve informare in modo tempestivo il suo titolare e questo provvederà senza ritardo ad avvisare l'autorità competente.

L'articolo 33, comma 3, dispone gli elementi essenziali della notifica. Il presente comma recita: “la notifica [...] deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l’adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi”.

In caso di violazione dei dati non è, però, sufficiente avvisare l'autorità di controllo. Indubbiamente è richiesta anche la comunicazione al legittimo proprietario dei dati che sono stati sottratti. Data la natura non competente dell'interessato, il linguaggio da utilizzare per comunicare l'infrazione deve essere semplice e chiaro. Attraverso la comunicazione, di conseguenza, l'interessato ha la possibilità di attivarsi in modo da minimizzare le possibili conseguenze negative.

È da precisare che l'avviso di violazione non è richiesto nel caso che il titolare avesse sin dall'origine utilizzato misure che rendessero inutilizzabili i dati per eventuali soggetti non autorizzati al trattamento dei dati oggetto di violazione. Queste misure si riferiscono in particolare alla cifratura o ad altre misure che rendono incomprensibili i dati nel caso venissero a contatto con persone diverse dal titolare o legittimate ad accedervi.

A questo riguardo il Garante della privacy con un provvedimento generale[13] ha disposto che gli Internet provider avvisino "il Garante privacy e gli utenti quando i dati trattati per fornire i servizi subiscono gravi violazioni a seguito di attacchi informatici o di eventi avversi, come incendi o altre calamità, che possano comportare perdita, distruzione o diffusione indebita di dati".

È da notare che nel caso d'infrazione nei confronti di dati personali di utenti su larga scala, la comunicazione da parte dei titolari a ciascun soggetto interessato sarebbe molto gravosa. Per questo motivo l'articolo 34 prevede una comunicazione pubblica in questo modo gli interessati si possono dire informati al pari dell'avviso che avrebbero ricevuto singolarmente.

Un tema di nuova impostazione nel Regolamento n. 679 del 2016 riguarda il "responsabile della protezione dei dati", il cosiddetto DPO. Questo soggetto è disciplinato dagli articoli 37, 38, e 39. In base alla legge europea questa figura è da considerarsi obbligatoria in tre casi individuati dallo stesso legislatore all'articolo 37, comma 1:

"Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10."

La designazione spetta al titolare o al responsabile del trattamento; come nel caso del responsabile del trattamento si deve tenere conto delle qualità professionali della persona individuata come DPO quanto disposto dal comma 5 del presente articolo.

Analizzando la norma si comprende come il testo normativo richieda che il DPO sia una persona fisica e non giuridica. Si ha la conferma, infatti, leggendo il comma 6 (il DPO "può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi").

Il DPO è una figura essenziale nella protezione dei dati personali, per questo motivo nonostante sia nominato da titolare o responsabile del trattamento, non è soggetto alla loro dipendenza bensì deve poter espletare le sue funzioni in modo indipendente.

[13] Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) del 4 aprile 2013 [doc. web n. 2388260].

Più volte si è detto che il DPO ha funzioni e compiti da compiere. Questi ricadono nella consulenza ai soggetti destinati al trattamento dei dati o ai dipendenti stessi riguardo agli obblighi in materia di protezione e circolazione dei dati. A questo si aggiunge la formulazione di pareri e non meno importante la cooperazione con l'autorità di controllo.
Questa figura, quindi, ha una molteplicità di compiti: rappresenta colui che deve sorvegliare che il trattamento dei dati rispetti il Regolamento e lo deve poter fare in modo indipendente; come detto poco sopra, è in contatto con l'autorità di controllo ma è anche a disposizione degli stessi interessati per eventuali problemi[14].
Il nuovo testo normativo europeo ha introdotto questa figura professionale molto importante, per molte aziende però questo è un campo pieno di dubbi e incertezze per questo il Garante ha emanato delle linee guida in ambito del DPO e ha risposto a domande in merito alla sua designazione, ai criteri per l'individuazione del soggetto più consono al ruolo, rimarcando che questo individuo può svolgere anche altri compiti all'interno della stessa azienda, precisando però, che non deve trovarsi in conflitto d'interessi.

1.4 Diritti dell'interessato

Come ben noto ogni individuo ha dei diritti, possano essere civili, politici o economici. Quindi non dovrebbe stupire il fatto che anche in materia di protezione dei dati personali, ovviamente, l'interessato goda di precisi diritti. Come già discusso, infatti, i soggetti che trattano i dati altrui devono rispettare delle regole imposte dalla legge. L'interessato, cioè la persona cui si riferiscono i dati, ha dal canto suo dei diritti da poter far valere nei confronti di titolari e responsabili del trattamento. Gli individui, quindi, hanno la possibilità di non subire in modo passivo il trattamento dei loro dati.
Il Regolamento n.679 del 2016 riserva a questo tema il Capo III rubricato espressamente "Diritti dell'interessato".
Questi diritti, più volte citati, sono il "diritto d'accesso", "alla portabilità dei dati", "alla rettifica", "alla limitazione", "all'opposizione", e non da ultimo il "diritto all'oblio".
Di seguito verranno chiariti uno alla volta, per il momento si inizia con il diritto d'accesso.

Tutti hanno diritto di essere informati nel caso in cui qualcuno sta trattando dati che li riguardano ed è quello che prevede l'articolo 15 del Regolamento europeo. Il titolare, pertanto, è tenuto a confermare o smentire, in caso di richiesta da parte del soggetto interessato, le

[14] PIZZETTI F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.*

eventuali attività di trattamento di dati personali. Nel caso in cui queste attività si stiano svolgendo, deve comunicare all'interessato alcune informazioni previste dall'articolo 15 che possono essere "le finalità del trattamento, le categorie dei dati in questione, il periodo di conservazione"; tra le informazioni non ricade la modalità del trattamento[15]. Il titolare in base a questo diritto dell'interessato dovrà anche presentare "una copia dei dati personali oggetto di trattamento"[16]. Il diritto di accesso è quindi quel diritto che permette al soggetto proprietario dei dati trattati di venirne a conoscenza e quindi di accedervi anche da remoto, come prescrive il considerando 68.

L'individuo può anche richiedere e pretendere che il titolare del trattamento rettifichi i propri dati che sono erroneamente detenuti. Al giorno d'oggi, infatti, i dati riferiti a una persona si modificano in modo frenetico dovuto alla velocità con cui si è abituati a vivere in questi ultimi anni, segnati dallo sviluppo tecnologico che si trascina dietro tutti gli aspetti della vita di un individuo.

Un'altro diritto collegato ai dati personali, affiancato al diritto di rettifica, riguarda la cancellazione. Il "diritto all'oblio" è stato disciplinato espressamente per la prima volta dal Regolamento 679/2016 all'articolo 17. Un individuo, quindi, può chiedere che i suoi dati vengano cancellati, ma per esercitare questo diritto il testo normativo impone delle situazioni specifiche riportate di seguito:

a) "i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l’interessato revoca il consenso su cui si basa il trattamento conformemente all’articolo 6, paragrafo 1, lettera a), o all’articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l’interessato si oppone al trattamento ai sensi dell’articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell’articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all’offerta di servizi della società dell’informazione di cui all’articolo 8, paragrafo 1."

[15] Garante privacy, Guida all’applicazione del Regolamento europeo in materia di protezione dei dati personali – DIRITTI DEGLI INTERESSATI.

[16] Art. 15, comma 3 del Regolamento UE 679/2016.

Attraverso l'introduzione di questo diritto si riconosce al cittadino la facoltà di pretendere che il titolare cancelli le informazioni detenute o trasmesse in qualsiasi parte, sia questo un sito web o copie rese ad altri soggetti autorizzati, novità quest'ultima introdotta dal nuovo Regolamento. A questo riguardo il Garante è intervenuto più volte in materia soprattutto digitale, e ha disposto che nel caso di informazioni che pregiudicano la sfera personale di un individuo, il titolare del trattamento di quei dati deve deindicizzare tutti gli URL che contengono informazioni pregiudizievoli per l'individuo, siano questi in versioni europee o extraeuropee[17].

Risulta chiaro che il diritto descritto si contrappone al diritto di cronaca. Tutti hanno il diritto infatti di essere informati e vige, fortunatamente ai giorni d'oggi, la libertà di espressione e d'informazione. Per questo motivo, in alcuni casi il Garante ha respinto la domanda di cittadini che chiedevano l'eliminazione o la deindicizzazione di informazioni a loro riferiti, ritenendo il diritto di cronaca prevalente rispetto al diritto all'oblio. Qualora, invece, le informazioni fossero prodotte per arrecare danno alla sfera privata dell'interessato, il Garante si pronuncia a favore della loro deindicizzazione.

Potrebbe capitare che l'interessato non sia sempre portato ad esercitare il "diritto alla cancellazione", ma voglia limitare il trattamento dei propri dati. Questo gli è concesso dal Regolamento ex articolo 18. Proprio come per il diritto alla cancellazione, anche per il "diritto di limitazione" il legislatore prevede delle ipotesi entro le quali esercitare questo diritto. L'interessato, infatti, può decidere liberamente dopo aver concesso il trattamento dei suoi dati, di chiederne la limitazione, così come nel caso in cui scoprisse di un trattamento illecito, invece di opporsi ne limita l'utilizzo.

Un nuovo diritto riconosciuto agli interessati, che si va così ad aggiungere agli altri, è il "diritto alla portabilità dei dati", in stretto contatto con il "diritto di accesso", già esaminato.

Questo diritto, infatti, permette all'interessato di ricevere, dal titolare del trattamento, i propri dati per poi consegnarli ad un altro titolare. In questo modo si facilita la trasmissione dei dati da un titolare ad un altro, oltre che a permettere all'interessato un controllo sui propri dati[18]. Per poter usufruire di questo diritto, però, è necessario che i dati in oggetto siano trattati con il consenso dell'interessato e che "il trattamento sia effettuato con mezzi automatizzati"[19]. Un'altra precisazione da fare riguarda i dati portabili. Non tutte le informazioni, infatti, si possono classificare tali, con la conseguenza che non tutti i dati beneficiano del diritto che si

[17] Garante privacy, Newsletter n. 437 26/01/2018 – Diritto all'oblio: cittadini italiano tutelati anche al di fuori dei confini europei.
Provvedimento del 21 dicembre 2017 [doc. web n. 7465315].
[18] Considerando 68 del Regolamento UE 679/2016.
[19] Lettera b) comma 1 dell'art. 20 del Regolamento UE 679/2016.

sta esaminando. Rientrano nel campo di applicazione dell'articolo 20 i dati personali che "riguardano l'interessato" e che sono stati "forniti a un titolare del trattamento". Prendendo in considerazione le linee Guida del WP29 si comprende come non rientrano di conseguenza in questa categoria di dati quelli che sono stati dedotti dai titolari utilizzando i dati che, invece, lo stesso interessato gli ha fornito.

Un'ultima cosa da specificare riguarda l'"informativa". Nelle linee Guida, difatti, s'impone ai titolari del trattamento di informare gli interessati dell'esistenza di questo diritto e di evidenziare con un linguaggio semplice, le differenze che ha con il precedente "diritto di accesso".

Una volta dato il consenso al trattamento dei dati, gli individui dovrebbero essere liberi di scegliere di revocarlo. Per questo il legislatore europeo ha riconosciuto, tra gli altri, il "diritto all'opposizione". Qualora l'interessato lo voglia, ha il diritto di esercitare questo potere e richiedere la cessazione del trattamento, anche nel caso della "profilazione". In base all'articolo 4 del GDPR questa si riferisce a "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati (...) per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica." Questo diritto, a differenza di quanto disposto dalla Direttiva 95/46/CE, si può esercitare "in qualsiasi momento, per motivi connessi alla situazione particolare" dell'interessato. Sta, quindi al titolare del trattamento provare la maggioranza dell'interesse al trattamento rispetto alle esigenze dell'interessato.

Per concludere sui diritti degli interessati riconosciuti dal Regolamento n. 679 del 2016, è obbligo riportare che tutte queste facoltà non sono esenti da limitazioni, come suggerito dallo stesso articolo 23. Questa disposizione infatti riporta un lungo elenco di situazioni in cui i diritti appena esaminati non trovano possibilità di essere applicati.

1.5 Trasferimento di dati verso Paesi terzi

Con l'odierna era tecnologica tutto il mondo è collegato, le imprese sono in continua comunicazione così che le informazioni si spostano da una città ad un'altra, da un Paese ad un altro con estrema facilità. Il problema sorge quando tra questi Paesi ci sono differenze sulla base della protezione riconosciuta ai dati oggetto di trattamento. I cittadini europei infatti godono di una ampia tutela dei dati rispetto agli altri cittadini extra-UE. Per questo motivo il legislatore europeo con il nuovo Regolamento cerca di intensificare quanto già disposto in tale

materia dalla Direttiva 95/46/CE. La normativa vigente tenta di assicurare che le tutele che sono state riconosciute agli interessati non vengano disilluse ma allo stesso tempo cerca che queste misure non precludano la comunicazione tra Stati europei ed extra-UE e quindi non vadano intaccare lo scambio, anche commerciale, che si può instaurare.

Sostanzialmente il nuovo testo normativo, come detto poco sopra, rispecchia quanto deciso dalla Direttiva precedente, ma un punto di novità risiede nel fatto che le norme riferite ai Paesi terzi si applicano anche alle Organizzazioni Internazionali.

Il Regolamento 679/2016 dispone che il trasferimento dei dati verso Paesi terzi avviene solo quando sono rispettate le condizioni imposte per legge, inoltre si allargano a questo campo di applicazione anche gli eventuali trasferimenti successivi che si avranno da Paese terzo o organizzazione internazionale ad un altro[20]. In questo modo si cerca di assicurare che la tutela dei dati personali sia sempre garantita.

Per avere un trasferimento dei dati legittimo è necessario che la Commissione abbia adottato una "decisione di adeguatezza". Con questa ci si riferisce al fatto che la Commissione stessa ha verificato che la protezione dei dati e le garanzie offerte dai Paesi terzi e dalle organizzazioni internazionali siano adeguate. Quello che il Regolamento prevede non è quindi una completa adozione della normativa europea da parte dei Paesi terzi, bensì si richiede che la protezione sia adeguata[21]. La decisione della Commissione, però, è soggetta a una revisione periodica, nell'ordine di almeno quattro anni, ed è possibile anche che la decisione venga revocata, modificata o sospesa nel caso in cui non siano più garantiti i livelli di protezione richiesti. È onere della Commissione darne comunicazione al Paese terzo o organizzazione internazionale, specificando le motivazioni di tale scelta, e avviare "consultazioni [...] per porre rimedio alla situazione"[22]. Bisogna, però precisare che le autorità di controllo nazionali hanno il diritto e l'obbligo di esaminare se effettivamente il trasferimento verso Paesi terzi rispetti le condizioni imposte dal Regolamento. Nel caso in cui si evidenziano delle discrepanze tra le garanzie date dai Paesi terzi e i requisiti richiesti dalla normativa europea, le autorità non possono decidere e agire in modo indipendente ma devono presentare le loro perplessità in merito alla decisione di adeguatezza alla Commissione. È, infatti, solo quest'ultima che ha il potere di revocare una decisione[23].

[20] Art. 44 del Regolamento UE 679/2016.

[21] MENEGHETTI M.C., *Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali*, in FINOCCHIARO (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* .

[22] Art. 45, comma 6 del Regolamento UE 679/2016.

[23] Sentenza della Corte di giustizia UE, nella causa C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, del 6 ottobre 2015.

Il testo normativo vigente accetta anche altri tipi di strumenti per permettere il trasferimento dei dati personali verso soggetti stabiliti fuori dal territorio europeo. All'articolo 46, infatti, si afferma che "in mancanza di una decisione [...], il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate". Il presente articolo si preoccupa di citare, al secondo comma, alcune garanzie che rientrano in questo ambito e che non richiedono alcuna autorizzazione, a differenza di quelle garanzie riportate al terzo comma. Queste garanzie fanno si che in ogni momento la protezione dei dati personali degli interessati sia assicurata e che quest'ultimi hanno la disponibilità di "diritti azionabili e di mezzi di ricorso effettivi"[24]. Quest'ultima precisazione è una novità introdotta ex novo dal Regolamento che si va così ad aggiungere a quanto già previsto dalla Direttiva 95/46/CE e confermato nel presente ordinamento.

Il Regolamento così come la Direttiva permette alcune deroghe al trasferimento dei dati verso Paesi terzi o organizzazioni internazionali. Viene quindi concessa questa possibilità anche nel caso in cui non ci sia una "decisione di adeguatezza" da parte della Commissione o la presenza di "garanzie adeguate". Le condizioni sono situazioni specifiche disciplinate dall'articolo 49, comma 1. Tra queste si trova il "trasferimento [...] per importanti motivi di interesse pubblico". Perché ciò avvenga, è necessario che sia l'Unione stessa o lo Stato membro che qualifichi l'interesse come tale. Si è disposto in questo modo per evitare che il Paese terzo dichiari l'interesse come pubblico con il solo fine di sfuggire al divieto di trasferimento[25].

A conclusione del primo comma, inoltre, si dispongono altri causi in cui è possibile trasferire i dati anche qualora non ricorrano le condizioni richieste dal Regolamento. Questo è possibile, infatti, solo se il trasferimento è "non ripetitivo" e "riguarda un numero limitato di interessati".

Il principale problema che riguarda questo tema è il fatto che una volta usciti dal territorio europeo i dati personali degli interessati rischiano di perdere quella tutela e protezione riconosciuta dall'UE. Per questo motivo si cerca di far sì che i Paesi terzi e le organizzazioni internazionali attraverso la cooperazione internazionale attribuiscano alla protezione dei dati l'importanza che merita. Tutto questo avviene attraverso "misure appropriate" adottate dalla Commissione e dall'autorità di controllo.

[24] Art. 46, comma 1 del Regolamento UE 679/2016.

[25] MENEGHETTI M.C., *Trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali*, in FINOCCHIARO (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali.*

2 Alcune questioni

2.1 L'interpretazione del diritto all'oblio da parte della CEDU

2.1.1 I fatti

Il caso Fuchsmann in esame prende il via da un ricorso (numero 71233/13) presentato alla Corte europea dei diritti dell'uomo (CEDU). In particolare gli attori della controversia sono il Signor Fuchsmann contro la Repubblica Federale di Germania.

Fuchsmann è un cittadino tedesco ma ucraino di nascita, è un investitore immobiliare oltre ad essere un imprenditore nel campo dei media, infatti, è amministratore delegato della società Innova Film GmbH.

Nel 2001 un articolo pubblicato dal New York Times afferma che l'imprenditore è collegato ad una rete internazionale del crimine organizzato e che per questo motivo gli è impedito di entrare in America. Questo articolo viene pubblicato anche nel sito web del quotidiano.

Il Signor Fuchsmann nel 2002 si attiva per chiedere alle corti tedesche dei provvedimenti contro la pubblicazione dell'articolo.

In un primo momento le richieste di Fuchsmann sono rigettate in quanto la Corte regionale e la Corte d'appello di Düsseldorf dichiarano che l'articolo non aveva connessione con la giurisdizione tedesca perché la versione on-line non era accessibile in modo diretto ai cittadini tedeschi[26].

Quando nel 2010 la questione arriva alla Corte di giustizia federale, questa rileva, a differenza delle altre Corti, che gli effetti dell'articolo sulla reputazione di Fuchsmann si sono prodotti anche in Germania in quanto in questo Paese molte persone hanno accesso a Internet e così alla versione on line del quotidiano statunitense. Inoltre dato che l'articolo parla di un cittadino tedesco, la sua pubblicazione da alla giurisdizione tedesca la possibilità e l'obbligo di intervenire e di pronunciarsi se viene interpellata da un cittadino.

Ancora una volta interpellata, la Corte d'appello riconosce che quanto riportato dal New York Times porti pregiudizi sulla reputazione del Signor Fuchsmann, ma allo stesso tempo riconosce l'importanza dell'articolo per la pubblica utilità. Per questi motivi la domanda del richiedente ancora una volta è stata negata.

[26] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13. Disponibile su https://www.echr.coe.int/Pages/home.aspx?p=home&c=fre

2.1.2 Questioni poste alla CEDU

È a questo punto che Fuchsmann fa ricorso alla CEDU lamentando come "i giudici nazionali non erano riusciti a proteggere la sua reputazione ed il diritto al rispetto della sua vita privata"[27] come previsto dall'articolo 8 della Convenzione.
Nell'argomentazione del richiedente si cerca di invocare anche il diritto all'oblio affermando che questo "potrebbe essere trasferito al caso in specie".
I criteri adottati dalla Corte europea dei diritti dell'uomo per deliberare su questa sentenza sono:

- il contributo dell'articolo a un dibattito di interesse pubblico;
- il grado di notorietà della persona interessata e l'oggetto della notizia;
- il metodo di ottenimento delle informazioni e la loro veridicità;
- la condotta preventiva dell'interessato;
- il contenuto, la forma e le conseguenze della pubblicazione.

<u>Il contributo dell'articolo a un dibattito di interesse pubblico</u>

Come rivelato dalla Corte d'appello con la sentenza emanata nel 2011, l'articolo presenta un interesse pubblico in quanto un cittadino tedesco con rapporti d'affari internazionali è stato sospettato di avere rapporti con la criminalità organizzata russa. Il fatto che l'articolo in questione sia datato 2001 e che si riferisca ad avvenimenti accaduti anni prima non è rilevante. Questa decisione infatti è avvalorata dalla nuova attualità degli eventi dovuti al sospetto di coinvolgimento di un ex candidato a sindaco di New York nella vicenda.
L'attualità è un criterio molto importante, infatti quando si guarda alla liceità della divulgazione di una notizia bisogna rispettare, oltre ai criteri di veridicità, pertinenza e continenza, anche quello dell'attualità.
È riconosciuto che un articolo non può essere ripubblicato nuovamente dopo che è trascorso un lasso di tempo che ha permesso all'interessato di ricostruirsi una reputazione. In verità, però come precisato anche sopra, quando i fatti sono divenuti per qualche motivo ancora di attualità, questo divieto viene meno e quindi viene riconosciuto come principale il diritto all'informazione e alla cronaca.
La Corte d'appello prima e la CEDU poi, hanno dichiarato che l'evento della candidatura a sindaco di un sospettato ha reso attuale fatti avvenuti nel passato e che "per la comprensione

[27] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13 par. 25.

dei lettori era stato necessario ripubblicare l'articolo" nel quale si approfondivano i sospetti nei confronti del richiedente.

Grado di notorietà della persona interessata ed oggetto della notizia

Un criterio importante da prendere in considerazione riguarda il ruolo della persona interessata. Esiste, infatti, una differenza tra persone private e persone che invece rivestono una posizione pubblica. I soggetti che rientrano nel primo tipo si vedono riconosciuti più diritti riferiti alla protezione della propria vita privata; non si può dire lo stesso per quei soggetti pubblici che si devono sempre confrontare tra vita privata ed interesse pubblico.
Nel caso preso in esame, il Signor Fuchsmann è un uomo d'affari tedesco che opera a livello internazionale nel settore dei media e questo fa di lui una figura importante sul piano pubblico. È la stessa Corte con sentenze precedenti che delibera in questo senso, e conforme alla dichiarazione di considerare un manager di un'impresa prestigiosa come un personaggio pubblico[28].
La notizia nuovamente ripubblicata ha il fine di facilitare la comprensione ai lettori di quanto accaduto. Il sospetto dell'ex candidato a sindaco ha riportato attualità su fatti passati in cui era coinvolto anche il richiedente e quindi è ritenuta legittima la divulgazione dell'articolo in cui si esponevano i fatti con indicazione di soggetti e imprese coinvolte.
La Corte d'appello ha analizzato anche che l'articolo incriminato è rimasto accessibile al pubblico in quanto pubblicato on line, questo però non ha inficiato la decisione. La notizia è di interesse pubblico e quindi è ammesso che questa sia a disposizione dei cittadini per informazioni che riguardano il passato. A questa conclusione si affianca anche la Corte europea dei diritti dell'uomo che dichiara che "gli archivi Internet costituiscono una fonte importante per l'istruzione e la ricerca storica, in quanto sono facilmente accessibili al pubblico e sono generalmente liberi"[29].

Metodo di ottenimento delle informazioni e loro veridicità

L'articolo 10 della Convenzione sancisce il diritto alla libertà di espressione ma allo stesso tempo al paragrafo 2 impone dei limiti: infatti, si parla di doveri e responsabilità. Si chiede quindi ai giornalisti di agire in buona fede e quindi di accertare che le informazioni che si stanno promulgando corrispondano al vero, che abbiano un fondamento di verità.

[28] CEDU 14 dicembre 2006, *Verlagsgruppe Notizie GmbH c. Austria*, n. 10520/02.
[29] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13 par. 39.

Tornando nel caso in esame, si nota come le informazioni fornite dal New York Times soddisfino quanto richiesto dalla Convenzione. La Corte ha osservato che il giornalista, come riporta anche nella stesura del pezzo, ha utilizzato dati legittimati da rapporti dell'FBI interni e da altri organi inquirenti.

Le informazioni considerate per la redazione dell'articolo hanno quindi un fondamento di credibilità perché oltre ad essere state fornite dall'FBI sono state anche confermate e riportate in rapporti di altre autorità investigative.

L'unica nota fuori dal coro riguarda l'affermazione di impedimento di entrata negli Stati Uniti. Per questo motivo, data l'infondatezza dell'informazione la Corte d'appello si è pronunciata a favore dell'ingiunzione. Decisione quest'ultima confermata in sede di ricorso dalla Corte EDU.

Condotta preventiva dell'interessato

Un altro criterio utilizzato per decidere in merito al caso alla quale la CEDU è stata chiamata a pronunciarsi è la condotta preventiva dell'interessato.

Ai giornalisti viene chiesto, prima di procedere con la pubblicazione di un articolo, di informare l'interessato e lasciare così la possibilità di difendersi.

Nel caso in oggetto il dipendente del quotidiano newyorkese si è attivato per rispettare questo dovere. Questi aveva, infatti, avvisato tramite e-mail il richiedente dell'uscita dell'articolo presentando anche alcune domande. Non avendo risposta, il redattore telefona a un collaboratore del Signor Fuchsmann per avere un riscontro: questi ha confermato che il richiedente aveva ricevuto le domande ma che si è astenuto dal rispondere o di commentare.

Tutto questo aggiunto al fatto che il richiedente si è attivato solo dopo un anno dalla pubblicazione dell'articolo fa supporre alla Corte che questi non vedesse pregiudicata la sua vita privata.

Contenuto, forma e conseguenze della pubblicazione

Ultimo fattore che la Corte EDU analizza per prendere la propria decisione concerne l'articolo nella sua interezza.

La notizia riportava fatti realmente accaduti, confermati dagli stessi rapporti delle varie autorità investigative e quindi sono da ritenersi affidabili; inoltre il giornalista nella stesura del suo elaborato si è astenuto da fare polemiche o insinuazioni rispetto quanto accaduto, riportando di fatto solo gli accadimenti. La Corte d'appello nella sua sentenza riporta come le

informazioni oggetto di pubblicazione riguardavano esclusivamente la vita professionale del Signor Fuchsmann, e quindi la vita privata del richiedente non venga violata.
Lo scritto viene pubblicato oltre che nella versione cartacea anche in formato digitale. Questo però non ha portato maggiore pregiudizio nei confronti del richiedente in quanto come comprovato dalla stessa Corte d'appello l'articolo on line "era accessibile solo a seguito di una ricerca diretta con un motore di ricerca on line"[30]. Quindi la portata delle conseguenze della notizia erano limitate.
Il giornalista, come riportato sopra, aveva anche provveduto a informare Fuchsmann prima di procedere con la pubblicazione e questi non si è prestato a fare commenti a riguardo, con l'aggiunta che l'azione inibitoria ha preso il via dopo un anno di distanza. Questo conferma quanto rilevato dalla Corte d'appello, cioè che il richiedente non vedeva come insopportabile l'interferenza nella proprio vita del manoscritto[31].

La Corte EDU respinge la domanda che il Signor Fuchsmann ha posto in merito alla violazione dell'articolo 8 della Convenzione. Riconosce che il bilanciamento operato dalla Corte d'appello riguardo il diritto alla libertà d'espressione e il diritto alla vita privata, sia in linea con quanto stabilito dalla giurisprudenza della Corte EDU. Il diritto d'espressione prevale sul secondo data la notorietà dell'interessato e la nuova attualità degli eventi raccontati, esiste quindi un interesse pubblico da tutelare e da far emergere.
La Corte EDU ricorda che, come nel presente caso, quando il bilanciamento operato da altre istituzioni rispetta i criteri dettati dalla giurisprudenza della Corte in questione, questa deve avere motivi di un certo spessore per deliberare in maniera differente rispetto le Corti nazionali.

2.1.3 Un diritto all'oblio ancora da scoprire

La sentenza presa in esame è forse più importante per quanto concerne il silenzio della Corte EDU in merito al diritto all'oblio.
Nel caso in oggetto per la verità il diritto all'oblio viene preso in considerazione nell'accezione di "diritto alla deindicizzazione". Quest'ultimo, come analizzato nel primo capitolo del presente elaborato, si riferisce al diritto che ha l'interessato di vedere eliminati tutti i link associati al proprio nome, in sostanza che digitando il nome dell'interessato in un motore di ricerca, questa non produca risultati.

[30] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13 par. 52.
[31] Bonavita S. e Pardolesi R., *La Corte EDU contro il diritto all'oblio?*, Danno e Responsabilità 2/2018.

Tra le richieste del Signor Fuchsmann alla Corte europea dei diritti dell'uomo figura, oltre come già analizzata la richiesta di violazione dell'articolo 8 della Convenzione, l'applicazione del diritto all'oblio al presente caso.

La CEDU nella sentenza tace nel punto in questione. Analizza i criteri per quanto riguarda la violazione della Convenzione ma non si preoccupa di approfondire il tema del diritto all'oblio. Questa scelta è forse dettata dal fatto che il richiedente ha utilizzato questo espediente per approdare in Corte EDU, dato che fino a quel momento nei precedenti giudizi non si è mai menzionata la volontà di chiedere l'applicazione del diritto all'oblio[32].

Nella decisione, i giudici di Strasburgo rigettano la richiesta in esame affermando che il richiedente non ha fornito alcuna informazione "riguardo agli sforzi fatti per avere il link rimosso dall'articolo dai motori di ricerca on line"[33].

Questa propensione della Corte europea dei diritti dell'uomo a negare il diritto all'oblio viene rafforzata dall'affermazione, della stessa Corte, della fondamentale importanza di Internet per la diffusione di informazione e notizie che hanno un interesse storico e pubblico, dato anche la facilità di accesso a tutti gli utenti[34].

In conclusione la CEDU riconosce maggiore importanza al diritto d'espressione ed in generale all'interesse pubblico rispetto al diritto di reputazione di un singolo cittadino quando questo riveste una posizione pubblica.

2.2 Riconoscimento della protezione dei dati in caso di frode fiscale

2.2.1 I fatti

Il contrasto alle frodi fiscali è un problema molto ostico per qualsiasi Stato. Le autorità di tutto il mondo cercano sempre nuove misure per arginare questo problema. Con riferimento a questa realtà, si può prendere in esame una sentenza della Corte di Giustizia dell'Unione europea. La causa C-73/16 ha per oggetto proprio la protezione dei dati personali in ambito di contrasto alle frodi fiscali.

La questione ha luogo in Slovacchia, dove la Direzione delle finanze e l'Ufficio crimini dell'amministrazione finanziaria hanno stilato un elenco di possibili sospettati di frode fiscale. In particolare sono stati inseriti 1227 nomi di persone fisiche che per le autorità sarebbero colpevoli di operare come prestanome per alcune società ai danni dello Stato.

[32] Bonavita S. e Pardolesi R., *La Corte EDU contro il diritto all'oblio?*, Danno e Responsabilità 2/2018.
[33] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13 par. 53.
[34] CEDU 19 ottobre 2017, *Fuchsmann c. Germania*, n. 71233/13 par. 39.

Il Signor Puskar viene a conoscenza di questo elenco e presenta ricorso davanti alla Corte suprema della Repubblica slovacca per chiedere l'intimazione alla Direzione delle finanze ed a tutte le altre autorità in questione, di eliminare il proprio nome dalla lista controversa.
Il ricorso viene considerato infondato e rigettato per il fatto che il richiedente "non aveva esaurito tutti i rimedi dinanzi alle autorità amministrative nazionali"[35].
Interrogata sulla questione, la Corte costituzionale slovacca annulla quanto disposto dalla precedente Corte, affermando che quest'ultima ha violato i diritti dei cittadini ad un equo processo oltre che alla protezione dei dati personali.
La Corte suprema della Repubblica slovacca prima di pronunciarsi nuovamente, decide di interpellare la Corte di giustizia europea in merito ad alcune questioni a lei poco chiare.

2.2.2 Questioni

Le informazioni contenute nell'elenco redatto dalla Direzione delle finanze in base alla normativa europea rientrano nella definizione di "dato personale". Centrale è quindi il tema del "trattamento dei dati personali" in quanto questi dati sono stati raccolti e trattati. In base alla Direttiva 95/46 prima e con il Regolamento 679/2016 poi, il trattamento viene escluso dall'ambito di applicazione della legge europea quando si riferisce ad attività legate "alla pubblica sicurezza, alla difesa, alla sicurezza dello Stato". La Corte di giustizia ricorda a riguardo che siccome si tratta di un'eccezione alla norma di base, questa deve essere analizzata in senso restrittivo. Ciò porta alla conseguenza che il trattamento in esame non è da ricondurre a tale eccezione poiché i dati trattati "sono raccolti e utilizzati ai fini della riscossione delle imposte e della lotta alla frode fiscale"[36].
La Direttiva 95/46 all'articolo 7 elenca in modo tassativo i casi in cui il trattamento è da considerare lecito. Tra questi alla lettera e) si prevede il trattamento lecito nel caso in cui "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati". Alla luce di questo inciso, la Corte di giustizia europea afferma che l'elenco redatto dalla Direzione delle finanze rientra in questa disposizione. La riscossione delle imposte e la lotta alla frode fiscale rientra tra i compiti che le amministrazioni finanziarie devono esercitare e di conseguenza si trattano di compiti con interesse pubblico.

[35] Corte di giustizia dell'Unione europea, causa C73/16, *Puskar c. Direzione delle finanza e Ufficio crimini dell'amministrazione finanziaria* del 27 settembre 2017. Disponibile su https://curia.europa.eu/jcms/jcms/j_6/it/
[36] Corte di giustizia dell'Unione europea, causa C73/16, *Puskar c. Direzione delle finanza e Ufficio crimini dell'amministrazione finanziaria* del 27 settembre 2017 par. 39.

Questo riconoscimento di liceità del trattamento deve però sottostare ugualmente al rispetto del principio di proporzionalità. La Corte, al paragrafo 112 della sentenza, ricorda come è essenziale che "le deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario". Questo significa che l'elenco controverso è da considerare lecito se non esistono altri strumenti che ledono i diritti del richiedente in modo meno oppressivo per raggiungere il medesimo scopo.

La Corte nella pronuncia della sentenza ricorda che qualora la stesura della lista sia necessaria per portare a termine il compito di contrasto alla frode fiscale, si deve sempre rispettare le altre condizioni imposte dalla Direttiva europea. In particolare si deve verificare che le disposizioni all'articolo 6 e dall'articolo 10 al 12 siano soddisfatte.

Con la sentenza del caso C-73/16, quindi, si dichiara che per combattere la frode fiscale, le autorità competenti possano stilare una lista degli evasori anche senza il consenso degli interessati. Quest'ultimo tuttavia non è richiesto solo nel caso in cui alle autorità sono stati conferiti compiti di interesse pubblico ma allo stesso tempo si deve continuare a far rispettare le condizioni di liceità imposte dalla Direttiva 95/46.

Questo significa che è concesso combattere la frode fiscale stilando una lista di possibili evasori ma nel farlo si deve perseguire la protezione dei dati personali.

Un'altra questione innalzata dal ricorrente riguarda l'ammissibilità dell'elenco controverso come prova.

Nel rispetto di quanto sancito dalla Carta dei diritti fondamentali dell'Unione Europea, la Corte rileva che una negazione del riconoscimento della prova provoca una restrizione del diritto ad un ricorso effettivo. Per la verità, questa restrizione può essere legittima, ovvero quando è "prevista dalla legge, se rispetta il contenuto essenziale di tale diritto e se, in osservanza del principio di proporzionalità, è necessaria e risponde effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui"[37].

Nel caso in esame, la Corte suprema slovacca aveva di fatto respinto la lista discussa in quanto il Signor Puskar ne è venuto in possesso senza il consenso del responsabile del trattamento e quindi in modo illegittimo.

Bisogna, però, ricordare che, come già detto nel corso dell'elaborato, l'interessato ha il diritto di accesso in riferimento ai propri dati, e che il responsabile del trattamento comunichi allo stesso determinate informazioni prescritte per legge dal testo normativo europeo.

[37] Corte di giustizia dell'Unione europea, causa C73/16, *Puskar c. Direzione delle finanza e Ufficio crimini dell'amministrazione finanziaria* del 27 settembre 2017 par. 88.

La stessa Direttiva sancisce anche alcune limitazioni ai diritti esercitabili dall'interessato esclusivamente per salvaguardia, tra gli altri casi, "della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali [...] o di un rilevante interesse economico o finanziario di uno Stato membro anche in materia [...] tributaria, o di un compito di controllo, ispezione o disciplina"[38].

La Corte di giustizia europea, quindi, rileva che prima di rigettare un elenco come quello redatto dalla Direzione delle Finanze si deve considerare alcuni aspetti.

Infatti ogni persona ha diritto ad un effettivo ricorso qualora senta che i suoi diritti siano stati violati. Quindi è ammissibile il rigetto di una prova solo quando quest'ultimo non pregiudichi questo diritto e qualora il rigetto sia previsto da una legge nazionale come prescrive il su citato articolo 13 della direttiva europea.

L'ultima questione riguarda l'esaurimento dei rimedi possibili.

In base alla legge slovacca, infatti, è possibile richiedere un ricorso giurisdizionale una volta aver esaurito tutti i rimedi disponibili davanti alle autorità nazionali.

Questo è permesso e quindi da ritenersi lecito, dallo stesso articolo 22 della Direttiva 95/46 che esprime la possibilità che gli Stati membri subordinino il ricorso giurisdizionale al soddisfacimento di rimedi nazionali.

È fondamentale, tuttavia, precisare che questo procedimento di esaurire tutti i rimedi possibili non deve scontrarsi con il diritto dei cittadini di presentare ricorso giurisdizionale e di avere un processo in tempi ragionevoli. Inoltre questa posticipazione al ricorso non deve comportare costi eccessivi per il richiedente.

Per questi motivi la Corte di giustizia ammette la possibilità che la legge slovacca richieda l'espletamento di tutti i rimedi nazionali prima di ricorrere ad un ricorso giurisdizionale, sempre che si rispettano le condizioni poco sopra menzionate.

Ciò che è rilevante di questa sentenza è la prima questione analizzata. La frode fiscale è un problema che si deve combattere, ma le autorità competenti non possono spingersi oltre il lecito. Devono agire nel rispetto della protezione dei dati delle persone interessate, nel compiere il loro lavoro è necessario che applichino l'ordinamento in materia di tutela dei dati personali sancito dall'Unione Europea.

Benché l'importanza di contrastare un fenomeno di grande portata come la frode fiscale, bisogna sempre ricordare che non tutti i mezzi sono leciti, che non è concesso alle amministrazioni competenti di operare al di sopra della legge, ma al contrario è richiesto loro un comportamento rispettoso dell'ordinamento giuridico.

[38] Art. 13, comma 1 della Direttiva 95/46.

Conclusioni

In conclusione la tutela dei dati personali è un argomento sempre di attualità e in continua evoluzione. Questo dinamismo è dovuto essenzialmente al mondo tecnologico che è costantemente in fase di sviluppo. Per questo motivo il legislatore europeo si è sentito in dovere di promulgare un nuovo Regolamento in materia di protezione dei dati in quanto la Direttiva 95/46 era divenuta ormai obsoleta e insufficiente.

Il nuovo Regolamento, per certi aspetti, riprende quanto già disposto dalla precedente Direttiva come nel caso dei principi del trattamento di liceità, correttezza e trasparenza o nei diritti dell'interessato all'accesso, alla limitazione o alla rettifica dei propri dati.

Dall'altra parte, questo nuovo ordinamento ha introdotto alcune novità importanti. In primis c'è l'ampliamento di applicazione della normativa europea anche oltre i propri confini e il nuovo campo di tutela, abbandonando lo stretto diritto alla vita privata per abbracciare la protezione dei dati personali.

Questo ha portato all'introduzione di diritti come la "portabilità dei dati" o al "diritto all'oblio".

Data la complessità della materia, il legislatore europeo ha richiesto alle imprese una nuova figura di controllo, il cosiddetto DPO.

L'insieme di tutte le novità del Regolamento UE 679/2016 cerca di arginare tutte le lacune che si erano formate nella vecchia normativa, ma non si esclude l'insorgere di molte altre problematiche.

La nuova legge europea è di recente attuazione quindi è difficile capire se si è fatto fronte a tutti i problemi in modo chiaro e diretto, e se i vari Stati membri siano stati in grado di attuarla in modo corretto e secondo quanto disposto dall'Unione Europea.

Questi sono tutti quesiti che troveranno risposta nel trascorrere dei prossimi giorni e mesi.

Come evidenziato nel caso Fuchsmann, è solo con il passare del tempo che si delineerà la corretta linea da seguire.

Quello del "diritto all'oblio" è un campo ancora da esplorare. È un diritto che deve essere preso in considerazione con un altro diritto fondamentale: quello dell'informazione. Sono diritti che si intrecciano per poi dividersi e compito dei cittadini è capire l'ambito di ognuno di essi, aiutati dalle autorità competenti. Il diritto all'oblio, infatti, soccombe al diritto di cronaca quando si è in presenza di un interesse pubblico.

Quest'ultimo funge da discriminante anche nel secondo caso analizzato. Infatti, si riconosce la legittimità della lista dei sospettati di frode fiscale solo perché si riferisce a un compito di interesse pubblico, come è quello al contrasto alla frode fiscale. Per questo motivo si consente

un leggero superamento rispetto alla protezione dei dati dei sospettati. Ciò però che rimane fermo è il rispetto degli altri diritti e doveri imposti dal Regolamento n. 679.

Quello dei dati personali e del loro trattamento è un tema in cui ci si imbatte in continuazione, molto più spesso di quello che si crede.

La nostra è un'era in cui tutto gira attorno ai social media, ciò porta alla trasmissione dei propri dati in modo anche inconsapevole. Per questo c'è sempre più bisogno di un sistema che tuteli questi dati, che permetta alle persone di essere libere di decidere come le informazioni su loro stesse vengono trattate.

È purtroppo vero che questo è e rimarrà sempre un tema molto delicato dato la sua vastità e al fatto che in ogni momento ci sono cambiamenti evolutivi che portano alcuni utenti a riuscire ad aggirare i limiti imposti loro dalla legge.

I primi da dover tutelare sono i giovani che utilizzano questi strumenti tecnologici con l'innocenza che li caratterizza. Per questo motivo il legislatore europeo ha voluto disporre articoli proprio su questo campo. Ha previsto una maggiore tutela e richiede che gli individui che si relazionino con i minori utilizzano linguaggi semplici e di facile comprensione.

Per sapere se il nuovo Regolamento è riuscito a proteggere in maniera più dettagliata e approfondita i dati delle persone fisiche si deve solo aspettare, sicuramente non sarà lontano da critiche, ma come si è più volte ribadito, questo è un campo che per sua natura dovrà essere aggiornato in modo continuo per poter essere a passo con i tempi.

Conteggio parole: 13068

Bibliografia

BONAVITA S. e PARDOLESI R., 2018.

- *La Corte EDU contro il diritto all'oblio?.* Danno e Responsabilità 2/2018 pag. 149 – 155.
- *Privacy, protezione dei dati personali e contrasto alle frodi fiscali.* Danno e Responsabilità 2/2018 pag. 156 – 162.

CICCIA MESSINA A. e BERNARDI N., 2017. *Privacy e regolamento europeo.* Milano: Wolters Kluwer Italia.

FINOCCHIARO G. (opera diretta da), 2017. *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali.* 1° ed. Torino: Zanichelli editore.

PIZZETTI F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli.

SOFFIENTINI M., 2016. *Privacy.* 1° ed. Milano: IPSOA.

Garante privacy,

- *Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali - DIRITTI DEGLI INTERESSATI.* Disponibile su https://www.garanteprivacy.it/regolamentoue/diritti-degli-interessati
- *Nuove FAQ sul Responsabile della Protezione dei Dati (RPD) in ambito privato.* [doc. web n. 8036793]. Disponibile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8036793#1
- *Provvedimento in materia di videosorveglianza* (G.U. n. 99 del 29 aprile 2010) del 8 aprile 2010 [doc. web n. 1712680]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680
- Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) del 4 aprile 2013 [doc. web n. 2388260]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2388260

- *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie* (G.U. n. 126 del 3 giugno 2014). Provvedimento del 8 maggio 2014 [doc. web n. 3118884]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884
- *Internet: Garante privacy, no ai cookie per profilazione senza consenso*. Comunicato stampa 4 giugno 2014 [doc. web n. 3167231]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231
- *Linee-guida sul diritto alla portabilità dei dati - WP 242.pdf.* Del 13 dicembre 2016 [doc. web n. 6058842]. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842
- *Provvedimento del 21 dicembre 2017 [doc. web n. 7465315]*. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7465315
- *Newsletter 26/01/2018 - Diritto all'oblio: cittadini italiani tutelati anche al di fuori dei confini europei.* Del 26 gennaio 2018. Disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7570001

Normativa e Giurisprudenza

Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995.

Regolamento del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile.

Sentenza della CEDU sul caso *Verlagsgruppe Notizie GmbH c. Austria*,del 14 dicembre 2006 n. 10520/02.

Sentenza della Corte di giustizia sul caso *Google inc. e Google Spain* del 13 maggio 2014. Disponibile su http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT

Sentenza della Corte di giustizia UE sul caso *Maximilian Schrems c. Data Protection Commissioner*, del 6 ottobre 2015, causa C-362/14.

Sentenza della Corte di giustizia dell'Unione europea sul caso *Puskar c. Direzione delle finanza e Ufficio crimini dell'amministrazione finanziaria*, del 27 settembre 2017, causa C73/16.
Disponibile su https://curia.europa.eu/jcms/jcms/j_6/it/

Sentenza della CEDU sul caso *Fuchsmann c. Germania*, 19 ottobre 2017 n. 71233/13.
Disponibile su https://www.echr.coe.int/Pages/home.aspx?p=home&c=fre