LUISS

Dipartimento

di Scienze Politiche

Cattedra di Diritto dell'Unione Europea

Luci e ombre di una recente giurisprudenza del diritto all'oblio

Prof. Roberto Baratta

RELATORE

Caterina Ferettini Matr. 086562

CANDIDATO

Anno Accademico 2019/2020

Indice

INTRODUZIONE

La protezione dei dati personali è una tematica che negli ultimi anni ha assunto un'importanza centrale, data la rapidità con cui i mezzi informatici tendono ad evolversi. In effetti, dal momento in cui gli archivi storici degli enti di informazione sono stati digitalizzati e indicizzati, le conseguenze dell'accentramento di tutte le informazioni in *data base* informatici (sia relative a dati pubblici che relative a dati personali) sono divenute problematiche di primaria importanza per le conseguenze connesse al rischio di uso fraudolento e pubblica esposizione di dati sensibili.

Già nel 2002, nel discorso di presentazione della relazione per l'anno 2001 Stefano Rodotà - il primo Presidente italiano dell'Autorità Garante per la protezione dei dati personali - evidenziava come i cittadini si preoccupassero sempre più del loro "*corpo elettronico"*, vale a dire di un'esistenza sempre più affidata alla dimensione del trattamento elettronico delle loro informazioni[1]. Gli individui sono ormai riconosciuti dai soggetti pubblici e privati tramite i dati che li riguardano, tanto che si può affermare semplicemente che "*noi siamo le nostre informazioni"*[2].

Le trasformazioni tecnologiche e la crescente necessità degli individui di effettuare un controllo sui propri dati personali hanno posto il legislatore europeo di fronte alle sfide derivanti dalla continua evoluzione della società digitale: dalle nuove esigenze di tutela dei dati personali da parte degli utenti deriva, pertanto, il nuovo Regolamento UE 2016/679 sulla protezione dei dati personali, denominato anche GDPR, acronimo di *General Data Protection Regulation,* divenuto applicabile a partire dal 25 maggio 2018. Il Regolamento abroga la precedente direttiva 95/46/CE che per più di vent'anni ha costituito il fulcro della disciplina dell'Unione in materia di protezione di dati personali: la direttiva risultava rispondere sempre meno alle esigenze degli utenti di maggiore tutela dei dati personali, essendo quest'ultima stata approvata nel 1995, anno in cui *internet* e *smartphone* erano fenomeni ancora poco conosciuti[3].

[1] Citazione tratta dal discorso di presentazione della relazione per l'anno 2001 del prof. Stefano Rodotà, maggio 2002, testo completo disponibile su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955

[2] *Ibidem.*

[3] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 69.

Tra le novità più significative introdotte all'interno del GDPR va certamente registrato il riferimento esplicito che il Regolamento svolge riguardo al c.d. diritto all'oblio (*right to be forgotten),* ossia il diritto di un individuo ad essere dimenticato: è la prima volta che in una normativa europea si riconosce l'esistenza di tale diritto. L'introduzione del *right to be forgotten* all'interno dell'art. 17 del GDPR rappresenta uno degli aspetti più controversi in materia di protezione dei dati personali: il dibattito giurisprudenziale e dottrinale sul diritto in parola è stato fortemente influenzato dalla particolare evoluzione che il *right to be forgotten* ha subito nel passaggio dall'era analogica all'era digitale. Il diritto all'oblio, prima dell'avvento della rete, si configurava quale diritto a non subire gli effetti pregiudizievoli, a distanza di tempo, derivanti dalla ripubblicazione di una notizia contenente informazioni personali legittimamente diffusa in origine ma non più attuale[4]. Il rapporto tra attualità dell'informazione, pubblicazione e oblio è mutato profondamente con l'avvento di *internet:* dal momento che le notizie pubblicate in rete hanno acquisito carattere permanente, il diritto all'oblio evolve quale diritto di un individuo ad ottenere la cancellazione di informazioni personali pubblicate per un tempo indefinito all'interno del *web*[5].

Il presente lavoro di ricerca mira a comprendere se il diritto all'oblio, così come disciplinato attualmente all'interno del GDPR, risulti essere un diritto nuovo, autonomo ed efficace, in grado di innalzare il livello di protezione dei dati personali degli utenti all'interno dell'articolato mondo della rete. Si intende quindi procedere tramite un'analisi graduale, che si pone l'obiettivo di esaminare i principali passaggi che hanno condotto il legislatore europeo a prevedere esplicitamente il *right to be forgotten* all'interno del nuovo Regolamento. Nel primo capitolo tratteremo, dunque, del caso *Google Spain* ove la CGUE ha fornito una nuova interpretazione del diritto all'oblio, suscitando un forte dibattito in dottrina. Nel secondo capitolo verranno analizzate le principali innovazioni sulla disciplina del *right to be forgotten* introdotte dall'art. 17 del GDPR e i suoi relativi punti di ambiguità. Oggetto di studio del terzo capitolo, infine, sarà la portata territoriale del GDPR e la nuova sentenza della CGUE nel caso *Google Cnil* concernente l'ambito di applicazione territoriale del *right to be forgotten*.

Più specificatamente, la nostra disamina sul diritto all'oblio trae spunto dall'analisi della sentenza della CGUE, conosciuta come il caso *Google Spain,* che costituisce nel diritto dell'Unione il *leading case* in materia: all'origine della vicenda vi è la richiesta con la quale un

[4] FINOCCHIARO G., La memoria della rete, in *Il diritto dell'informazione e dell'informatica",* A. XXVI, Fasc. 3, 2010, pag. 391 e ss.
[5] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 60.

cittadino spagnolo aveva cercato di ottenere dal motore di ricerca *Google* la rimozione di alcuni dati personali pubblicati su un articolo di un giornale, ritenuti non più attuali. Nella sua pronuncia la Corte fornisce (tra l'altro discostandosi completamente dalle Conclusioni dell'Avvocato Generale) un'interpretazione alquanto rivoluzionaria del diritto all'oblio, che tiene conto del nuovo rapporto tra il *right to be forgotten* e *internet:* il diritto all'oblio viene interpretato dalla CGUE quale diritto di un utente ad ottenere la deindicizzazione delle informazioni personali correlate al proprio nominativo dai risultati del motore di ricerca. In sostanza, il motore di ricerca è tenuto a cancellare esclusivamente i *link* che rinviano all'informazione in cui sono contenuti i dati personali oggetto dell'istanza di cancellazione, mentre la notizia continuerà a permanere sul sito originale in cui è stata pubblicata.

Tale interpretazione, seppur assolutamente innovativa, ha scatenato un forte dibattito in dottrina su una serie di punti salienti della decisione, in particolare, sul ruolo che i gestori dei motori di ricerca hanno assunto nell'applicazione del *right to be forgotten* e sul difficile bilanciamento tra il diritto all'oblio e la libertà di informazione e di essere informati[6].

Le "ombre" emerse a seguito del caso *Google Spain* hanno fortemente contribuito all'inserimento esplicito del *right to be forgotten* all'interno del GDPR. Nel secondo capitolo si cercherà pertanto di rispondere a due quesiti: in primo luogo, se la nuova disciplina del diritto all'oblio e alla cancellazione possa considerarsi innovativa rispetto a quanto precedentemente previsto dalla direttiva 95/46/CE; in secondo luogo, se l'art. 17 del GDPR, rubricato "diritto alla cancellazione (diritto all'oblio)" possa fornire una risposta concreta alle numerose critiche emerse a seguito del caso *Google Spain,* sancendo l'esistenza di un *right to be forgotten* autonomo, efficace e pienamente realizzabile.

Dall'analisi dell'art. 17 del GDPR emergeranno "luci" e "ombre" sulla nuova disciplina del diritto alla cancellazione e del *right to be forgotten:* di fatto, nonostante la previsione in esame risulti essere assolutamente innovativa rispetto a quanto precedentemente previsto dalla direttiva 95/46/CE, il testo della norma appare talvolta poco chiaro. Come si vedrà, infatti, il GDPR non determina l'esistenza di un diritto all'oblio autonomo, ma piuttosto configura quest'ultimo quale diritto alla cancellazione in forma rafforzata[7]. Eppure, tale nuova

[6] MARKOU C., The Right to be Forgotten: Ten Reason Why It Should Be Forgotten, in GUTRWIRTH, LEENES, DE HERT (ed. by.), *Reforming European Protection Law*, Springer Netherlands, 2015, pag. 72; JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 68.
[7] XANTHOULIS N., *Conceptualizing a Right to Oblivium in the Digital World: a Human Rights-based Approach,* SSRN (ATT 2064503): 17, 2012.

configurazione del diritto all'oblio non risulterà essere pienamente realizzabile. L'art. 17, seppur di grande impatto, risulta foriero di una serie di ambiguità e enigmaticità che non consentono di comprendere se il *right to be forgotten*, così come configurato dal Regolamento, possa effettivamente innalzare il livello di protezione dei dati personali degli individui.

Infine, la recentissima sentenza della CGUE del 29 settembre 2019 nel caso C-507/17 (*Google Cnil)* affronta l'interrogativo principale oggetto del presente lavoro di ricerca: sebbene il *right to be forgotten* sia esplicitamente previsto dal Regolamento, l'individuo ha realmente la possibilità di essere dimenticato, ossia rimosso totalmente, dal mondo della rete? Nel caso *Google Cnil* la Corte è stata chiamata a precisare la portata territoriale dell'obbligo di cancellazione, chiarendo se la deindicizzazione da parte dei gestori di un motore di ricerca operi solo a livello nazionale o europeo oppure se si estenda a livello globale.

Per comprendere le motivazioni che hanno condotto la dottrina maggioritaria a ritenere che la decisione della CGUE nel caso *Google Cnil* costituisca un limite alla piena realizzazione del *right to be forgotten,* verrà *in primis* analizzato nel terzo capitolo l'ambito di applicazione territoriale del GDPR, disciplinato all'art. 3. Tale disposizione amplia notevolmente l'orizzonte di riferimento della normativa, disciplinando una tutela adeguata non solo nel caso di trattamenti di dati personali all'interno dell'Unione, ma anche al di fuori dei suoi confini, data l'a-territorialità della rete.

Nonostante l'art. 3 del GDPR estenda l'applicazione della normativa anche al di fuori dei confini dell'UE, la CGUE nel caso *Google Cnil* ha stabilito che il diritto all'oblio può essere legittimamente esercitato da un individuo esclusivamente all'interno dell'Unione: le informazioni personali che vengono mostrate a seguito di una ricerca effettuata tramite un motore di ricerca saranno deindicizzate dal *search engine* esclusivamente nei domini europei, mentre permarranno al di fuori dei confini dell'UE. Tale decisione si scontra radicalmente con la nuova applicazione territoriale del GDPR: obiettivo del legislatore europeo era quello di garantire una tutela elevata dei dati personali degli individui sia all'interno che all'esterno delle frontiere dell'UE[8]. Al contrario, il diritto all'oblio di un individuo si arresta ai confini dell'Unione Europea.

[8] Considerando 24, GDPR.

CAPITOLO I - IL DIRITTO ALL'OBLIO NEL CASO GOOGLE SPAIN

1.1 La protezione dei dati personali nell'Unione Europea: dalla Direttiva 95/46/CE all'EU General Data Protection Regulation (GDPR)

L'evoluzione digitale permette sempre più di produrre, immagazzinare e diffondere dati con estrema facilità, aumentando l'esigenza di un individuo di proteggere ed effettuare un controllo sui propri dati personali che circolano in rete. Il diritto alla protezione dei dati personali e la normativa dell'Unione posta a sua tutela si sono sviluppati parallelamente allo sviluppo della tecnologia dell'informazione e delle comunicazioni.

Il primo intervento del legislatore europeo in materia di diritto alla protezione dei dati personali risale a più di vent'anni fa quando la Comunità Europea, oggi Unione Europea, avvertì il bisogno di coordinare le normative nazionali degli Stati Membri[9] in tema di protezione dei dati personali, al fine di facilitare il trasferimento di tali dati all'interno dell'UE e anche al di fuori dei suoi confini[10]. Per tale ragione nel 1995 venne adottata la direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[11].

La direttiva 95/46/CE- definita anche "direttiva madre", in quanto ha costituito per molto tempo il testo di riferimento, a livello europeo, in tema di protezione dei dati personali- fu adottata allorché l'Unione Europea risultava essere ancora suddivisa nella tradizionale struttura a tre pilastri di cui: il primo pilastro riguardava le Comunità Europee (CEE), il mercato comune Europeo, l'unione economica e monetaria; il secondo pilastro si occupava della Politica Estera e di Sicurezza Comune (PESC), ossia la costruzione di una politica unica verso l'esterno; il terzo, la Cooperazione giudiziaria e di polizia in materia penale (GAI), rivolto alla costruzione di uno spazio europeo di libertà, sicurezza e giustizia, in cui vi fosse collaborazione contro la criminalità a livello sovranazionale.

[9] La direttiva 95/46/CE è stata, infatti, adottata nel 1995 quando già diversi Stati membri avevano promulgato leggi nazionali in materia di protezione dei dati personali. Ad esempio, il Land tedesco dell'Assia ha adottato la prima legge al mondo sulla protezione dei dati nel 1970 che era applicabile solo in tale Stato. Successivamente la Svezia ha adottato il *Datalagen* nel 1973; la Germania ha adottato il *Bundesdatenschutzgestez* nel 1976 e la Francia la *a Loi relative à l'informatique, aux fichiers et aux libertés* nel 1977. Più tardi Regno Unito e Belgio hanno adottato rispettivamente il *Data Protection Act* nel 1984 e il *Wet Persoonregistraties* nel 1989.

[10] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 1.

[11] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

La direttiva 95/46/CE si fondava, pertanto, nell'ambito del primo pilastro e aveva l'obiettivo di creare uno strumento giuridico di armonizzazione delle legislazioni nazionali in materia di protezione dei dati personali, in grado di contemperare la tutela delle libertà delle persone fisiche con l'esigenza della libera circolazione dei dati tra gli Stati membri, strumentale a sua volta alla libera circolazione di beni, capitali, servizi e persone all'interno del mercato unico, e dunque funzionale al suo corretto funzionamento[12].

Tuttavia, l'esplosione del *web 2.0*[13] e dell'evoluzione della società digitale hanno fatto emergere l'esigenza di una maggiore tutela giuridica dei dati personali: è indubbio che il *web,* se da un lato permette un ampio accesso alle informazioni, dall'altro tende a creare conflitti con altri diritti fondamentali posti a presidio dell'individuo. Il diritto di essere informati, la libertà di comunicazione, la trasparenza (tutte caratteristiche fondamentali di una società libera e democratica) non possono sopprimere il bisogno di intimità, il diritto di costruire liberamente la propria sfera privata o il diritto di essere liberi di sviluppare la propria identità[14].

L'entrata in vigore del Trattato di Lisbona[15] il 1° dicembre 2009 costituisce il passaggio fondamentale che ha legittimato l'Unione ad attuare una revisione e una uniformazione della sua legislazione in tema di protezione di dati personali, per due precise ragioni. In primo luogo, in base all'art. 6 (I), comma 1, del TUE, l'Unione *"riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione Europea"* che assume *"lo stesso valore giuridico dei trattati"*. Con il Trattato di Lisbona, dunque, la Carta dei diritti fondamentali dell'Unione[16] è elevata allo *status* di documento legale vincolante a livello di diritto primario; le disposizioni di quest'ultima si applicano agli organi e alle istituzioni dell'UE imponendo loro, nell'assolvimento delle loro funzioni, il rispetto dei diritti riconosciuti da quest'ultima e

[12] AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI (FRA), "*Manuale sul diritto europeo in materia di protezione dei dati"*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, pag. 32.

[13] Il *web 2.0* può essere indicativamente definito come un insieme di tecnologie, di modi di essere e di comunicare totalmente nuovi rispetto all'*Internet* a cui eravamo abituati; ecco perché prende il suffisso 2.0. Si indica come *web 2.0* l'insieme di tutte quelle applicazioni *online* che consentono un elevato livello di interazione tra il sito *web* e l'utente, come le chat, i forum o i blog o le piattaforme di condivisione dei media come You Tube, Facebook, Twitter o Instagram. Al contrario, il *web 1.0* era composto da siti *web* prevalentemente statici, a navigazione lineare, senza possibilità di interazione eccetto la normale navigazione ipertestuale delle pagine, l'uso della posta elettronica e dei motori di ricerca.

[14] IASSELLI M., I fondamenti e l'evoluzione del diritto all'oblio, in CASSANO G. (a cura di), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio,* Wolters Kluwer, Vicenza, 2017, pag. 231-337.

[15] Il Trattato di Lisbona firmato il 13 dicembre 2007 ed entrato in vigore il 1° dicembre 2009, modifica il Trattato sull'Unione Europea e il Trattato che istituisce la Comunità Europea, apportando significative innovazioni al diritto primario UE. Cfr. versione consolidata del Trattato sull'Unione Europea (TUE) e del Trattato sul funzionamento dell'Unione Europea (TFUE), GU C 326/01 del 2012.

[16] La Carta dei diritti fondamentali dell'Unione Europea, conosciuta anche come Carta di Nizza, è stata proclamata a Nizza il 7 dicembre 2000 e una seconda volta a Strasburgo nel dicembre 2007. Con l'entrata in vigore del Trattato di Lisbona guadagna valore giuridico vincolante di un trattato.

anche gli Stati Membri sono vincolati dalle disposizioni della Carta nell'applicazione del diritto dell'Unione.

La Carta non solo garantisce il rispetto della vita privata e della vita familiare[17] (art. 7), ma stabilisce anche il diritto alla protezione dei dati di carattere personale (art. 8), innalzando esplicitamente il livello di tale protezione a quello di un diritto fondamentale nell'ambito del diritto dell'Unione.

La Carta di Nizza riconosce il diritto alla protezione dei dati personali quale diritto distinto e autonomo dal diritto al rispetto della vita privata. Il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata, sebbene strettamente connessi- in quanto entrambi mirano a proteggere valori simili, vale a dire l'autonomia e la dignità umana degli individui, accordando loro una sfera personale nella quale possano sviluppare liberamente la loro personalità e modellare le loro opinioni[18]- sono diritti distinti. Il diritto al rispetto della vita privata consiste in un divieto generale di ingerenza su vicende strettamente personali. A differenza del diritto alla protezione dei dati personali, è un diritto a contenuto negativo, quello di non rendere note e riservare determinate informazioni, piuttosto che a contenuto positivo, ossia quello di esercitare un controllo sulle medesime. Al contrario, il diritto alla protezione dei dati personali consiste nel diritto del soggetto cui i dati si riferiscono, di esercitare un controllo, anche attivo, sulle modalità di trattamento di detti dati[19].

In secondo luogo, il Trattato di Lisbona è da considerarsi una pietra miliare nello sviluppo della legislazione UE in materia di protezione di dati personali, in quanto è lo stesso Trattato, all'art. 16 del TFUE, nella parte dedicata ai principi generali dell'UE, a prevedere il diritto alla protezione dei dati personali. In base all'art. 5, par. 2 del TUE, l'azione dell'Unione deve essere legittimata da una precisa competenza prevista nei Trattati; ciò che non risulti espressamente attribuito all'Unione rimane di competenza esclusiva degli Stati membri[20]. L'art.

[17] Nel diritto internazionale in materia di diritti umani, il diritto alla vita privata, conosciuto nel diritto europeo come diritto al rispetto della vita privata, è stato sancito per la prima volta come uno dei diritti umani fondamentali protetti, nell'art. 12 della Dichiarazione Universale dei diritti dell'uomo (UDHR), adottata nel 1948. Poco dopo l'adozione di tale dichiarazione, anche l'Europa ha sancito questo diritto, all'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), un trattato giuridicamente vincolante per le parti contraenti, redatto nel 1950.

[18] AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI (FRA), "*Manuale sul diritto europeo in materia di protezione dei dati"*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, pag. 21.

[19] AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI (FRA), *op. cit.*, pag. 22; v. anche FINOCCHIARO G., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017, pag. 7.

[20] L'art. 5, par. 2, del Trattato sull'Unione Europea (TUE) afferma che: "*in virtù del principio di attribuzione, l'Unione agisce esclusivamente nei limiti delle competenze che le sono attribuite dagli Stati membri nei Trattati per realizzare gli obiettivi da questi stabiliti. Qualsiasi competenza non attribuita all'Unione nei Trattati appartiene agli Stati membri".*

16 crea, pertanto, una nuova base giuridica indipendente e conferisce all'UE la competenza a legiferare in materia di protezione dei dati personali. Si tratta sicuramente di un progresso sostanziale, se si considera che in origine la legislazione dell'UE in materia di protezione dei dati, in particolare la direttiva 95/46/CE, si fondava sulla base giuridica del mercato interno e sull'esigenza di armonizzare le legislazioni nazionali al fine di non pregiudicare la libera circolazione dei dati all'interno dell'Unione Europea[21].

Il consolidarsi, dunque, di un mondo sempre più digitalmente interconnesso ha richiesto inevitabilmente una riforma degli strumenti giuridici fino ad allora attuati in ambito comunitario sul tema della protezione dei dati personali. In particolare, la direttiva 95/46/CE risultava rispondere sempre meno alle nuove richieste di tutela armonizzata dei dati in rete in quanto - conformemente al sistema giuridico dell'UE - le direttive non sono direttamente applicabili ma devono essere recepite nel diritto nazionale degli Stati membri[22]. Sebbene obiettivo della direttiva fosse un'armonizzazione delle leggi nazionali promulgate in materia di protezione dei dati personali, in realtà essa era stata recepita in modo differente dagli Stati membri, e questo aveva portato inevitabilmente alla creazione di norme diversificate e ad applicazioni e interpretazioni differenti delle legislazioni nazionali.

La riforma della legislazione UE in materia di protezione dei dati personali trae origine, dunque, dalla constatazione della frammentazione della disciplina sulla protezione dei dati personali e dalla diffusa incertezza giuridica relativa all'applicazione della normativa[23]. Tale riforma si è definitivamente conclusa il 4 maggio 2016 con la pubblicazione del Regolamento (UE) n. 2016/679[24] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. "GDPR") e che abroga la direttiva 95/46/CE, divenuto pienamente applicabile a partire dal 25 maggio 2018. Il Regolamento meglio risponde alla necessità di uniformazione, dal momento che è direttamente applicabile e non richiede attuazione a livello nazionale[25].

[21] AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI (FRA), "*Manuale sul diritto europeo in materia di protezione dei dati"*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, pag. 32.
[22] art. 288, comma 3, TFUE.
[23] considerando n. 9, GDPR.
[24] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, Regolamento generale sulla protezione dei dati personali (GDPR).
[25] art. 288, comma 2, TFUE.

1.2 Il caso *Google Spain*

Nell'era digitale, ciascun utente della rete può facilmente rendere disponibile al pubblico su scala mondiale informazioni personali che lo riguardano. Tuttavia, potrebbe accadere che informazioni precedentemente pubblicate possano divenire con il trascorrere del tempo pregiudizievoli per la reputazione del soggetto interessato e che conseguentemente quest'ultimo possa ritenere indispensabile ottenere la rimozione di dette informazioni dai siti *web* ove quest'ultime figurino.

Il diritto alla protezione dei dati personali, si è precedentemente sottolineato, comporta un controllo attivo da parte di un individuo sui propri dati personali; tale controllo può anche implicare la richiesta di cancellazione dal *web* di informazioni precedentemente divulgate. A tal proposito, si segnala che una delle principali novità introdotte nel GDPR è rappresentata dall'art. 17, che disciplina il diritto alla cancellazione ("diritto all'oblio"): per la prima volta in un testo normativo di matrice europea il diritto all'oblio (*right to be forgotten)*, ossia il diritto di un individuo ad essere dimenticato, viene esplicitamente menzionato.

L'inserimento del diritto all'oblio all'interno del GDPR costituisce ad oggi uno degli aspetti più controversi e dibattuti all'interno del Regolamento[26]: in particolare il dibattito dottrinale e giurisprudenziale sul *right to be forgotten* ha risentito fortemente della peculiare evoluzione - che negli ultimi anni - ha subito l'attività informativa delle moderne società. Il diritto all'oblio ha assunto, infatti, sfumature e connotazioni differenti a seconda delle piattaforme utilizzate per la diffusione delle notizie.

Il diritto all'oblio nasce storicamente in rapporto all'esercizio di cronaca giornalistica, in particolare, prima dell'avvento della rete, il diritto in parola era da intendersi quale diritto di un individuo a non vedere reinserite nella divulgazione informativa fatti di cronaca lecitamente pubblicati in passato, che a seguito del trascorre di un consistente lasso di tempo risultavano dimenticate o ignote alla maggioranza[27]. La pubblicazione di una notizia, lecitamente effettuata in un determinato momento storico, perde di giustificazione perché riproposta in un altro momento storico, tanto lontano dal precedente da far venir meno la finalità dell'originaria divulgazione. In questa iniziale declinazione del diritto all'oblio il tempo rappresenta il criterio

[26] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 156.
[27] FINOCCHIARO G., La memoria della rete, in *Il diritto dell'informazione e dell'informatica",* A. XXVI, Fasc. 3, 2010, pag. 391 e ss.

principale cui dipende la valutazione di meritevolezza della pretesa del soggetto nel legittimo esercizio del *right to be forgotten*[28].

Con l'avvento del *web* e delle reti telematiche le modalità di diffusione delle informazioni sono state completamente rivoluzionate, e conseguentemente anche l'interpretazione del diritto all'oblio, così come precedentemente concepita, ha subito una rilevante variazione. Le informazioni pubblicate in rete sono divenute permanenti e fruibili a chiunque. Con la digitalizzazione, infatti, i quotidiani hanno reso disponibile nel *web* il proprio archivio storico, rendendo accessibile al grande pubblico tutte le notizie ivi pubblicate negli anni passati. Inoltre, l'indicizzazione automatica attuata dai motori di ricerca consente di trovare informazioni su un individuo inserendo semplicemente il nominativo del soggetto ricercato. Il carattere permanente delle notizie in rete e la loro facile fruibilità non consentono più di riconoscere nel fattore tempo l'elemento chiave su cui basare la valutazione di meritevolezza del legittimo esercizio del diritto all'oblio: non si tratta più, infatti, di verificare la legittimità di una ripubblicazione di una notizia lecitamente pubblicata in passato, ma piuttosto di valutare la legittimità della permanenza della stessa su *internet.* Con lo sviluppo della società digitale, dunque, il diritto all'oblio si è affermato quale diritto del soggetto interessato di ottenere la cancellazione delle informazioni personali che sono accessibili per un tempo tendenzialmente indefinito su *internet*, potenzialmente dannose per il libero godimento della vita privata[29].

Il rapporto tra *internet* e diritto all'oblio è stato al centro di una importante sentenza della Corte di Giustizia europea (di seguito, CGUE), emessa il 13 maggio 2014 (*Google Spain)*[30], ove il significato del diritto all'oblio viene ad assumere un'ulteriore e innovativa declinazione. È doveroso segnalare sin da subito che il termine "diritto all'oblio" verrà richiamato esclusivamente nelle Conclusioni dell'Avvocato Generale[31] , e non all'interno della pronuncia della CGUE. La direttiva 95/46/CE infatti non disciplinava in alcun modo tale diritto, ma riconosceva agli artt. 12 e 14 rispettivamente il diritto dell'interessato di ottenere la cancellazione dei propri dati personali e il diritto all'opposizione del trattamento[32].

[28] RICCI A., I diritti dell'interessato, in FINOCCHIARO G. (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, 2017, pag. 179-250.
[29] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement,* Springer, 2017, pag. 60.
[30] CGUE, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [*GC*], 13 maggio 2014
[31] Conclusioni dell'Avvocato Generale nella causa C-131/12, *Google Spain*, presentate il 25 giugno 2013.
[32] In particolare, con riguardo al diritto di accesso dei dati da parte della persona interessata, l'art. 12 stabiliva il diritto a qualsiasi persona interessata di ottenere dal responsabile del trattamento liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi, a seconda dei casi, la rettifica, la cancellazione o il

Dall'interpretazione fornita dalla CGUE degli articoli sopra citati discenderà la nuova definizione di diritto all'oblio, quale diritto ad ottenere la deindicizzazione dei dati personali dagli esiti delle ricerche effettuate tramite un motore di ricerca a partire dal nome di un individuo. Al fine di comprendere le argomentazioni che hanno condotto la CGUE a fornire tale nuova declinazione del diritto all'oblio è indispensabile esaminare nel dettaglio la sentenza *Google Spain.*

Nel 1998, un giornale di ampia diffusione in Spagna pubblicava in edizione cartacea due annunci relativi ad un'asta di beni immobili, collegata a un procedimento esecutivo derivante da debiti contratti con il sistema previdenziale. La persona interessata, Costeja González, veniva menzionata come proprietario dell'immobile. L'editore, successivamente, rendeva disponibile *online* una versione digitale del giornale.

Il 5 marzo 2010, il sig. Costeja Gonzalez presentava reclamo dinanzi all'Agencia Española de Protección de Datos (AEDP) contro la società editrice del quotidiano "La Vanguardia" nonché contro *Google Spain* e *Google Inc.,* lamentando che, allorché il proprio nome veniva introdotto nel motore di ricerca del gruppo *Google ("Google Search"),* l'elenco dei risultati mostrava dei *link* verso due pagine del quotidiano La Vanguardia, datate gennaio e marzo 1998, pagine in cui si annunciava una vendita all'asta di immobili organizzata a seguito di un pignoramento effettuato per la riscossione coattiva di crediti previdenziali nei confronti nel sig. Costeja Gonzalez.

Mediante detto reclamo, il sig. Costeja Gonzalez chiedeva, da un lato, che fosse ordinato a La Vanguardia di sopprimere o modificare le pagine suddette affinché i suoi dati personali non apparissero più, e dall'altro lato, che fosse ordinato a *Google Spain* o *Google Inc.* di eliminare o occultare i suoi dati personali, affinché cessassero di comparire tra i risultati di ricerca, e non figurassero più nei *link* di La Vanguardia. Peraltro, il ricorrente affermava che il pignoramento effettuato nei suoi confronti fosse stato interamente definito da svariati anni e che la menzione dello stesso risultasse, dunque, essere ormai priva di rilevanza.

Con decisione del 30 marzo 2010 L'AEDP accoglieva l'istanza solo parzialmente: da un lato, respingeva il reclamo contro La Vanguardia considerando che la pubblicazione da parte

congelamento dei dati il cui trattamento non è conforme alle disposizioni della direttiva 95/46/CE, in particolare a causa del carattere incompleto o inesatto dei dati. Invece, l'art. 14 riconosceva alla persona interessata il diritto di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato del responsabile non può più riguardare tali dati.

della testata giornalistica fosse legalmente giustificata, e dall'altro accoglieva il reclamo contro *Google Spain* e *Google Inc.,* ordinando ai gestori del motore di ricerca, in quanto soggetti alla normativa dei dati personali, di adottare tutte le misure necessarie per ritirare i dati dal loro indice e impedire l'accesso futuro ai medesimi.

Conseguentemente, contro tale decisione *Google Spain* e *Google Inc.* proponevano ciascuna ricorso chiedendo l'annullamento della decisione davanti all'Audencia Nacional. Il Tribunale di Madrid sospendeva il ricorso e con rinvio pregiudiziale sottoponeva una serie di questioni alla Corte di Giustizia Europea.

La prima questione pregiudiziale posta all'attenzione della Corte concerne l'ambito di applicazione territoriale della direttiva 95/46/CE. La Corte su questo punto ha osservato che *Google Spain* costituisce una filiale di *Google Inc.* nel territorio spagnolo, e per tale motivo rientra nella definizione di "stabilimento" fornita dalla direttiva 95/46/CE all'art. 4 comma 1, lett. a) e c)[33]. La Corte ha respinto, pertanto, l'argomento secondo cui il trattamento di dati personali da parte di *Google Search* non sia effettuato nel contesto delle attività di stabilimento in Spagna.

La Corte, riprendendo le argomentazioni dell'Avvocato Generale[34], ha ritenuto che la direttiva 95/46/CE deve trovare applicazione nell'ipotesi in cui il gestore di un motore di ricerca stabilito in uno Stato terzo apra una propria filiale in uno Stato membro al fine della promozione e della vendita di comunicazione commerciale ai cittadini di quest'ultimo. Nel caso specifico, *Google Spain* costituisce una filiale di *Google Inc.* (società che ha sede negli Stati Uniti, quindi uno Stato terzo) e dunque uno stabilimento di quest'ultima a norma della medesima direttiva. Di conseguenza, le attività di ricerca e di pubblicità del motore di ricerca sono da considerarsi inscindibili e analoghe alle finalità attuate nel contesto delle attività di stabilimento delle filiali nazionali di *Google Inc.* Qualora, dunque, i dati siano trattati per le esigenze di un motore di ricerca in uno Stato terzo che, tuttavia, possiede un proprio stabilimento in uno Stato membro,

[33] L'art. 4 comma 1, lett. a), della direttiva 95/46/CE stabiliva che ciascuno Stato membro dovesse applicare le disposizioni adottate per l'attuazione della direttiva al trattamento di dati personali: "*effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto internazionale applicabile".* Nonché ai sensi del medesimo art., comma 1, lett. c): "*il cui responsabile non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea".*
[34] v. punti 63-67 delle Conclusioni dell'Avvocato Generale nella causa C-131/12, *Google Spain.*

tale trattamento è da considerarsi, secondo la Corte, "nel contesto delle attività", della medesima filiale[35].

Secondo la Corte, pertanto, la visualizzazione di dati di una pagina di risultati di una ricerca costituisce un trattamento di dati personali. Dal momento che suddetta visualizzazione di risultati è accompagnata, sulla stessa pagina, da quella di pubblicità correlate ai termini di ricerca, è giocoforza constatare che il trattamento di dati in questione viene effettuato nel contesto dell'attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro, in questo caso il territorio spagnolo. Di conseguenza, non si può accettare che il trattamento di dati personali effettuato per le esigenze del funzionamento del suddetto motore di ricerca venga sottratto agli obblighi e alle garanzie previste dalla direttiva 95/46/CE, poiché ciò pregiudicherebbe la tutela efficace delle libertà e dei diritti fondamentali che la medesima direttiva mira a garantire, quale il diritto al rispetto della vita privata con riguardo al trattamento dei dati personali[36]. La conseguenza pratica di tale decisione è l'applicabilità del diritto comunitario, sebbene *Google Spain* risulti una filiale di un'organizzazione con sede legale in California.

La seconda questione pregiudiziale riguarda il riconoscimento del gestore del motore di ricerca come titolare e responsabile del trattamento dei dati personali contenuti nei *database* frutto dell'attività di indicizzazione del *web*. A tal riguardo, *Google* ha contestato la responsabilità che le veniva attribuita, sostenendo di limitarsi a fornire un collegamento ipertestuale alla pagina *web* dell'editore che deteneva l'informazione e che, dunque, la richiesta di eliminare informazioni obsolete da una pagina *web* dovesse essere presentata a quest'ultimo piuttosto che a *Google*, che si limita a fornire un *link* che indirizza alla pagina d'origine.

La Corte, al contrario, ha constatato che le operazioni svolte dal gestore del motore di ricerca *Google* rientrano nella nozione di "trattamento" fornita dall'art. 2, lett. b), della direttiva 95/46/CE[37]. In effetti, la Corte ha affermato anzitutto che, esplorando *internet* in modo costante, automatizzato e sistematico alla ricerca delle informazioni *ivi* pubblicate, il gestore di un motore di ricerca svolge un'attività di trattamento dei dati, dal momento che "raccoglie" , "estrae", "registra" e "organizza" tali dati nell'ambito dei suoi programmi di indicizzazione, prima di

[35] Si veda la sentenza in esame, punto 60.
[36] *Idem*, punto 57 e 58.
[37] L'art. 2, lett. b), della direttiva 95/46/CE definiva "trattamento di dati personali" *qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione".*

"conservarli" nei suoi *server* e eventualmente di "comunicarli" e di "metterli a disposizione" dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche[38].

Sulla questione concernente il riconoscimento del motore di ricerca come responsabile del trattamento di dati personali è da considerare che la posizione assunta dalla Corte si discosta da quanto sostenuto dall'Avvocato Generale. Infatti, l'Avvocato Generale aveva ritenuto che il fornitore di servizi di un motore di ricerca su *internet* non potesse essere considerato "responsabile del trattamento" di tali dati personali ai sensi dell'art. 2, lett. d) [39], della direttiva 95/46/CE, fatta eccezione per i contenuti dell'indice del suo motore di ricerca, sempre che il fornitore di servizi non indicizzi o archivi dati personali contro le istruzioni o le richieste dell'editore della pagina *web.* In particolare, l'Avvocato Generale aveva sostenuto che "il fornitore di servizi di motore di ricerca su *internet* non ha alcun rapporto con il contenuto delle pagine *web source* di terzi su *internet* in cui possono comparire dati personali. Inoltre, dato che il motore di ricerca lavora sulla base di copie di pagine *web source* che il *crawler* ha estratto e copiato, il fornitore di servizi non ha mezzi per cambiare le informazioni sul *server host.* Fornire uno strumento di localizzazione non implica alcun controllo sul contenuto, né tale attività mette il fornitore di servizi di motore di ricerca su *internet* in condizione di distinguere tra dati personali ai sensi della direttiva, ossia i dati che si riferiscono ad una persona fisica identificata e identificabile, e gli altri dati"[40].

Al contrario, la CGUE, alla luce delle definizioni fornite dall'art. 2, lett. d) della citata direttiva, ha ritenuto che lo stesso gestore del motore di ricerca debba qualificarsi come responsabile del trattamento, in quanto è lui a determinare le finalità e gli strumenti del trattamento stesso[41]. Anzi, la Corte sembra completamente respingere le argomentazioni di *Google,* secondo cui il motore di ricerca si limita a fornire un collegamento ipertestuale alle pagine dell'editore *web.* La CGUE, infatti, ha affermato che il motore di ricerca fornisce, a seguito di una semplice ricerca di un utente su *internet* con il nome di un individuo, informazioni complessive sulla persona ricercata che potrebbero toccare potenzialmente aspetti della vita privata di un soggetto, e che probabilmente, in assenza di un motore di ricerca, difficilmente avrebbero potuto essere connesse tra loro. Questo conseguentemente offre agli

[38] Si veda la sentenza in esame, punto 28.
[39] L'art. 2, lett. d), della direttiva 95/46/CE definiva "responsabile del trattamento": *"la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per al sua designazione possono essere fissati dal diritto nazionale o comunitario"*
[40] Conclusioni dell'Avvocato Generale nella causa C-131/12, punto 86.
[41] Si veda la sentenza in esame, punto 32.

utenti la possibilità di costruire un profilo piò o meno dettagliato della persona ricercata in rete. Pertanto, alla luce della sua potenziale gravità, tale ingerenza non può essere giustifica dal mero interesse economico dell'operatore di un siffatto motore di ricerca in tale trattamento di dati[42].

Dopo aver riconosciuto il gestore di un motore di ricerca quale responsabile del trattamento, la Corte risponde all'ultimo quesito pregiudiziale concernente il "diritto all'oblio". La Corte è stata interrogata a definire se la direttiva 95/46/CE consenta alla persona interessata di esigere direttamente dal gestore di un motore di ricerca la cancellazione dei *link* verso pagine *web* dall'elenco di risultati per il fatto che detta persona ritenga che la divulgazione di tali informazioni possa arrecarle pregiudizio o che essa desideri che queste informazioni siano oggetto di "oblio" dopo un certo lasso di tempo. Tale questione pone di fatto due interrogativi distinti: se l'interessato possa rivolgersi direttamente al motore di ricerca invece che al soggetto che abbia pubblicato l'informazione in rete, e se il presupposto della domanda di cancellazione possa essere costituito dalla considerazione che la divulgazione arrechi pregiudizio, o dal desiderio che le informazioni siano dimenticate[43].

Su questo punto l'Avvocato Generale nelle sue Conclusioni aveva ammonito la Corte sui rischi legati al sacrificio della libertà di informazione dovuti all'affermazione del diritto all'oblio in maniera assoluta, senza un adeguato bilanciamento[44], e pertanto aveva ritenuto che "il diritto di cancellazione, previsto all'art.12, lett. b), e il diritto di opposizione, previsto all'art. 14, lett. d), non consentono alla persona interessata di rivolgersi essa stessa ad un fornitore di servizi di motore di ricerca per impedire l'indicizzazione di informazioni che la riguardano personalmente, pubblicate legalmente su pagine *web* di terzi, facendo valere la sua volontà che tali informazioni non giungano a conoscenze degli utenti di *internet* quando la persona interessata ritenga che le suddette potrebbero arrecarle pregiudizio o desideri che vengano dimenticate".

La posizione assunta dalla Corte si discosta da quanto sostenuto dall'Avvocato Generale. Infatti, la Corte ha stabilito che gli individui hanno il diritto a richiedere direttamente al motore di ricerca la cancellazione dei dati personali, in ragione del fatto che il gestore del motore di ricerca è considerato il titolare del trattamento.

[42] *Idem*, punto 81.
[43] FINOCCHIARO G., Il diritto all'oblio nel quadro dei diritti della personalità, in *Il diritto dell'informazione e dell'informatica",* A. XXVI Fasc. 4-5- 2014, p.591-604.
[44] Conclusioni dell'Avvocato Generale nella causa C-131/12, punto 133.

Rispetto al secondo interrogativo, la Corte ha considerato che, per quanto disposto dall'art. 12, lett. b) in tema di cancellazione dei dati - la cui applicazione è subordinata alla condizione che il trattamento di dati personali sia incompatibile con la direttiva 95/46/CE - occorre ricordare che tale incompatibilità può derivare non solo dall'inesattezza dei dati ma anche dall'inadeguatezza, non pertinenza o eccessività in rapporto alle finalità del trattamento dei medesimi, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario[45]. Pertanto, anche un trattamento inizialmente lecito di dati esatti può divenire, con il trascorrere del tempo, incompatibile con la direttiva 95/46/CE, se tali dati non siano più necessari in rapporto alle finalità per le quali sono stati trattati o raccolti, e più precisamente se tali dati risultassero "inadeguati, non siano o non siano più pertinenti ovvero eccessivi in rapporto alle finalità per le quali sono stati trattati e al tempo trascorso"[46]. La Corte ha concluso sottolineando come, a seguito di una ricerca *online* tramite un motore di ricerca, l'inclusione nell'elenco di risultati dei *link* verso pagine *web*, sia incompatibile con l'art. 6[47], par. 1, lettere da c) a e), della direttiva 95/46/CE, poiché tali informazioni, alla luce delle circostanze del caso di specie, appaiono inadeguate, non pertinenti o non più pertinenti o eccessive in rapporto alle finalità del trattamento in questione realizzato dal motore di ricerca, sicchè tali *link* dovranno essere omessi dai risultati della ricerca[48].

Tuttavia, la CGUE, pur avendo stabilito il diritto di individuo di richiedere direttamente la cancellazione dei dati personali e pur avendo imposto a *Google* di eliminare i *link* legati al ricorrente, ha riconosciuto che il diritto di ottenere la cancellazione dei *link* collegati alle informazioni personali da parte del motore di ricerca non è assoluto: è indubbio che ogni richiesta di cancellazione debba essere valutata caso per caso, al fine di trovare un bilanciamento tra i diritti fondamentali alla protezione dei dati personali e della vita privata dell'interessato, da un lato, e gli interessi legittimi di tutti gli utenti di *internet,* dall'altro. Per tale ragione, la stessa Corte ha fornito indicazioni sui fattori da considerare nella valutazione della domanda di cancellazione, sulla base della natura dell'informazione trattata. Dunque, se

[45] Sentenza *Google Spain*, punto 92.
[46] *Idem*, punto 93.
[47] L'art. 6, par. 1, lettere da c) a e), della direttiva 95/46/CE stabiliva che i dati personali dovessero essere: *c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati; d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici".*
[48] Sentenza *Google Spain*, punto 94.

l'informazione si riferisce alla vita privata di una persona e non vi è un interesse pubblico alla sua fruibilità, la protezione dei dati e della vita privata prevarrebbe sul diritto pubblico generale di avere accesso all'informazione. Al contrario, qualora risulti che l'interessato sia una figura pubblica o che l'informazione è di natura tale da giustificarne l'accessibilità al pubblico, l'interesse generale ad avere accesso all'informazione potrebbe giustificare l'ingerenza nei diritti fondamentali alla protezione e alla vita privata dell'interessato[49].

Pertanto, risulta sussistere un limite alla soppressione di *link* dall'elenco di risultati, fondato sull'interesse sotteso alla pubblicazione della notizia. Di conseguenza la Corte ha disposto che il motore di ricerca non deve cancellare i dati personali presenti presso il soggetto (titolare del trattamento dei dati che ha pubblicato l'informazione), ma deve rimuovere solo il collegamento a questi dati derivanti da una ricerca a partire dal nominativo dell'interessato. Parimenti, la società editrice non può essere condannata a rimuovere la notizia, poiché nel caso in esame vengono in considerazione obblighi di pubblicità legale, in materia di procedure esecutive immobiliari.

Alla luce di tali argomentazioni, emerge come in tale pronuncia la CGUE non abbia riconosciuto il diritto all'oblio quale diritto assoluto, scevro da limiti di esercizio, sui dati trattati dai motori di ricerca: non si tratta di un diritto a cancellare i dati *tout court,* ma di un diritto che va ponderato ed esercitato in ragione delle caratteristiche dei dati costituite dall'adeguatezza, dalla pertinenza o dalla non pertinenza del trattamento rispetto alle finalità. La cancellazione riguarda esclusivamente i contenuti della ricerca compiuta attraverso l'inserimento di dati identificativi dell'interessato, non l'informazione originaria pubblicata sul sito ad esempio della testata telematica.

Nell'interpretazione fornita dalla Corte il diritto all'oblio è da intendersi quale diritto alla de-indicizzazione, ossia un diritto alla cancellazione non dei dati stessi, ma dei collegamenti ai medesimi ottenuti tramite l'utilizzo del motore di ricerca. Pertanto, i motori di ricerca (in questo caso specifico *Google)* elimineranno il *link* che il soggetto vuole sia dimenticato tra i risultati, anche se l'informazione rimarrà disponibile sul sito *web* originale. Per effettuare una ricerca su un individuo, a seguito della cancellazione del *link* da parte del gestore del motore di ricerca, sarà necessario digitare il nome del soggetto direttamente, ad esempio, sulle pagine *web* delle testate giornalistiche.

[49] *Idem*, punto 99.

Il merito della Corte, dunque, risulta essere l'individuazione di una interpretazione innovativa del diritto all'oblio che tiene conto del nuovo rapporto che caratterizza il *right to be forgotten* e il mondo della rete, in cui i motori di ricerca assumono sempre più un ruolo centrale nella diffusione delle informazioni personali. Il diritto all'oblio, così come declinato dalla CGUE, aumenta certamente il livello di tutela dei dati personali all'interno della rete: è la stessa Corte, di fatto, all'interno della decisione, ad aver dichiarato la preminenza del diritto alla protezione dei dati personali a scapito degli interessi economici del gestore del motore di ricerca e dell'editore web e del diritto all'informazione degli utenti della rete, imponendo come unico limite alle richieste di deindicizzazione il ruolo che riveste l'individuo nella vita pubblica cui la notizia si riferisce[50].

Sebbene il caso *Google Spain* abbia messo in luce l'importanza dell'esercizio legittimo del diritto all'oblio in riferimento allo sviluppo della società digitale, in cui le informazioni personali circolano sempre più velocemente, determinando un'interferenza con il libero godimento della vita privata e della protezione dei propri dati personali, esso ha innescato un forte dibattito su alcune "ombre" che sono emerse nella nuova interpretazione del *right to be forgotten.*

1.3 Analisi dei risultati applicativi del caso *Google Spain*

Dall'analisi della sentenza *Google Spain* emerge una nuova declinazione del diritto all'oblio che tiene conto non solo del rapporto che intercorre tra oblio e *internet* e, dunque, del nuovo fattore temporale collegato alla pubblicazione delle notizie sul *web* che assumono carattere permanente, ma anche del ruolo fondamentale che ad oggi assumono i motori di ricerca nella diffusione delle informazioni personali degli individui. Tuttavia, è da considerare che la decisione della CGUE sul caso *Google Spain*, nonostante abbia fornito un'interpretazione innovativa del diritto all'oblio, quale diritto ad ottenere la cancellazione dell'indicizzazione dei risultati a partire dal nome di un individuo dal motore di ricerca, ha scatenato un forte dibattito in dottrina su una serie di interrogativi lasciati insoluti dalla decisione della Corte e che hanno contribuito fortemente all'introduzione del *right to be forgotten* all'interno del GDPR.

Per comprendere, dunque, le motivazioni che hanno condotto la dottrina maggioritaria a criticare fortemente la nuova interpretazione del diritto all'oblio, è necessario porre attenzione

[50] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 65.

ai punti salienti della sentenza di cui trattasi, evidenziando le "ombre" che sono sorte su alcuni passaggi chiave della decisione. In particolare, sono tre le questioni maggiormente dibattute: in primo luogo il riconoscimento del motore di ricerca quale responsabile del trattamento; in secondo luogo, la prevalenza, in linea di principio, che la Corte ha attribuito, nei casi di richieste di cancellazione, agli artt. 7 e 8 della Carta (rispettivamente il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali) sul diritto alla libertà di informazione, riconosciuto all'art. 11 della medesima; infine, il ruolo che i gestori di motori di ricerca hanno assunto a seguito del caso *Google Spain* nell'applicazione del diritto all'oblio, inteso quale diritto alla deindicizzazione.

La prima problematica riguarda la differenza che la CGUE ha constatato, nel caso *Google Spain,* tra il gestore del motore di ricerca e l'editore *web,* riconoscendo solo il primo come effettivo responsabile del trattamento e dunque attribuendo solo a quest'ultimo un obbligo di rimozione del *link.* Il riconoscimento del gestore di un motore di ricerca come responsabile del trattamento non risulta essere pienamente condivisibile se si considera che elemento principale che contraddistingue l'attività di un motore di ricerca è l'automatismo delle informazioni senza, di fatto, un'operazione di selezione tra i dati personali di un individuo e le altre informazioni. Al motore di ricerca sono forniti i riferimenti di base da utilizzare nei parametri della ricerca e di estrazione delle informazioni rilevanti, con la conseguenza che la scelta di quest'ultime avviene poi automaticamente; per cui risulta difficile configurare un'unica responsabilità ai gestori dei motori di ricerca dal momento che gli stessi non hanno un'effettiva conoscenza e un controllo sui dati in questione[51]. Differentemente dagli editori delle singole pagine *web,* il motore di ricerca non è responsabile del contenuto e della pubblicazione delle notizie, ma piuttosto è responsabile del reindirizzamento alle pagine dei siti *web* tramite una selezione delle pagine memorizzate dal motore di ricerca che contengono le parole ricercate dall'utente. Dunque, perché imporre un obbligo di cancellazione esclusivamente al gestore di un motore di ricerca che, differentemente dall'editore *web,* non ha il minimo controllo sull'informazione pubblicata oggetto dell'istanza di rimozione?

Ulteriore punto di discussione risulta essere il contrasto che si potrebbe verificare tra l'obbligo alla rimozione del *link* a carico del gestore di un motore di ricerca e la libertà di informazione e di essere informati, avendo la Corte riconosciuto in linea di principio la prevalenza degli artt. 7 e 8 della Carta sulla libertà di informazione. La critica mossa contro la

[51] IASSELLI M., I fondamenti e l'evoluzione del diritto all'oblio, in CASSANO G. (a cura di), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio,* Wolters Kluwer, Vicenza, 2017, pag. 231-337.

Corte nel caso *Google Spain* concerne la mancanza di attenzione e il peso che la CGUE ha attribuito alla libertà di espressione e di informazione[52]. La CGUE al fine di contemperare il diritto del soggetto interessato alla protezione dei dati personali con l'interesse pubblico all'informazione, ha stabilito che i diritti fondamentali derivanti dagli artt. 7 e 8 della Carta di Nizza consentono ad un individuo di ottenere la rimozione di informazioni da un certo elenco di risultati, ma che esistono "*ragioni particolari come il ruolo ricoperto da tale persona nella vita pubblica,* per le quali *l'ingerenza nei suoi diritti fondamentali, è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi*[53]*".* Risulta tutt'altro che agevole tradurre sul piano operativo quest'affermazione: cosa si intende per ragioni particolari? Chi è il soggetto legittimato a valutare la prevalenza del diritto alla protezione dei dati personali sull'interesse collettivo all'informazione?

Su questo punto sono intervenute, nel 2014, le Autorità europee per la *privacy,* le quali, riunitesi nel *Working Party 29*[54]*,* al fine di garantire un'attuazione uniforme della sentenza e fornire una risposta alle questioni lasciate insolute dalla Corte, hanno predisposto specifiche Linee Guida contenenti una serie di criteri comuni che le autorità di controllo sono chiamate ad utilizzare nella gestione dei reclami relativi alle richieste di cancellazione da parte di persone fisiche. Nelle *Guidelines* è comunque stabilito che le valutazioni devono essere effettuate caso per caso e tenendo talvolta conto di più criteri; pertanto, nessun criterio è di per sé determinante, atteso che ciascun indice deve essere interpretato alla luce del principio stabilito dalla Corte di Giustizia, in particolare tutelando "*l'interesse del pubblico ad avere accesso all'informazione"*.

Il problema principale è che tale valutazione "caso per caso", ossia l'onere di stabilire in quali casi la libertà di informazione debba soccombere rispetto all'interesse dell'individuo a proteggere i dati personali, è attribuita direttamente al gestore di un motore di ricerca, che conseguentemente assume un ruolo centrale nell'applicazione del *right to be forgotten.*

Come precedentemente sottolineato, infatti, la Corte ha riconosciuto i gestori di un motore di ricerca quali responsabili del trattamento, stabilendo il diritto di un individuo di richiedere direttamente ai gestori[55], in quanto responsabili, la rimozione dei dati personali e,

[52] KRANENBOURG H., *Google and the Right to Be Forgotten*, in *Protection Law Rev.*, 2015, Issue 1, pag. 74.
[53]CGUE, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [*GC*], 13 maggio 2014, punto 97.
[54] Il *Working Party 29* è il gruppo di lavoro consultivo e indipendente previsto dall'art. 29 della Direttiva 95/46/CE.
[55]Sentenza *Google Spain*, punto 77.

dunque, attribuendo *in primis* a *Google* il potere di valutare e decidere se soddisfare o meno la richiesta di cancellazione[56].

Nel 2015 l'azienda di *Mountain View,* al fine di uniformarsi alla pronuncia della CGUE e a seguito dell'aumento esponenziale delle richieste di cancellazione[57], ha pubblicato un rapporto (*Google Trasparency Report),* in cui ha predisposto un sistema *online* con cui gli utenti possono avanzare le proprie richieste di cancellazione dei propri dati personali dai risultati delle ricerche del *search engine.*

Allo scopo di garantire un corretto bilanciamento tra il diritto dell'individuo ad esercitare un controllo sui suoi dati e il diritto di tutti di conoscere e distribuire le informazioni, *Google* valuterà la richiesta esaminando (come previsto dalla sentenza della CGUE e dalla successive *Guidelines* del *Working Party 29)* se vi sia la presenza o meno di un interesse pubblico tale per cui la notizia debba permanere nei risultati del motore di ricerca, quali ad esempio frodi finanziarie, negligenza professionale, condanne penali, o la condotta pubblica in relazione al pubblico ufficio[58]. Solo in caso di mancato accoglimento della richiesta di deindicizzazione da parte di *Google,* il soggetto interessato potrà adire le autorità garanti o il giudice competente; le autorità pubbliche, pertanto, saranno protagoniste di quello che sembra essere un "secondo grado" di giudizio, reso del tutto ipotetico se si considerano i costi e i tempi della giustizia ordinaria, tanto che è legittimo credere che la maggior parte dei ricorsi si esauriscano con la procedura *online* di fronte a *Google*[59].

La minaccia più grave che si potrebbe presentare risulta più chiara se si considerano le finalità prettamente economiche insite nel gestore di un motore di ricerca; si intende dire che *Google* essendo un'azienda privata - mossa da interessi economici, quale la massimizzazione del proprio profitto, e non essendo pertanto un soggetto terzo in grado di agire imparzialmente - per evitare di subire i costi di una eventuale soccombenza in giudizio, potrebbe accogliere la maggior parte delle richieste di rimozione, minando ancor di più il già difficile equilibrio tra l'interesse generale all'informazione e il diritto di un individuo di esercitare un controllo sui propri dati personali[60].

---

[56] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement,* Springer, 2017, pag. 67.

[57] *Google Inc.* attualmente ha ottenuto 917.952 richieste di cancellazione dati da tutta Europa, accolte solo per il 46,3%. I dati sono disponibili all'indirizzo https://transparencyreport.google.com/eu-privacy/overview, (Data di ultimo accesso: 30/04/2020).

[58] Le informazioni sulle modalità di presentazione di una richiesta di deindicizzazione a *Google* sono reperibili sul sito: https://policies.google.com/faq?hl=it

[59] FAINI F., PIETROPAOLI S., *Scienza giuridica e tecnologie informatiche,* Giappichelli, 2017, pag. 61.

[60] *Ibidem.*

Il diritto all'oblio, dunque, così come interpretato dalla CGUE, ossia il diritto di un individuo di ottenere la deindicizzazione dei dati personali e di effettuare tale richiesta direttamente al motore di ricerca che, in quanto responsabile del trattamento, avrà il potere di valutare autonomamente il corretto bilanciamento tra il diritto dell'interessato di ottenere la cancellazione dei dati personali e il diritto della collettività di essere informata, ha suscitato non poche perplessità. Ad esempio, alcuni commentatori hanno ritenuto che dal momento che al diritto di una persona di essere dimenticata potrebbe parimenti corrispondere il diritto di un'altra a ricordare, il *right to be forgotten*, così come delineato dalla sentenza *Google Spain*, rappresenti un ostacolo al libero accesso degli individui alle informazioni, favorendo fenomeni di censura[61]. Altri commentatori hanno definito tale sentenza come un chiaro esempio di "censura privatizzata"[62]: la decisione della Corte, attribuendo a *Google* il potere di decidere autonomamente i risultati da rimuovere dalle ricerche effettuate dal suo motore di ricerca, ha affidato direttamente ad un'azienda privata il controllo sull'applicazione del diritto all'oblio e sulla ricerca del giusto equilibrio tra diritto all'informazione e diritto alla protezione dei dati personali, piuttosto che ad un tribunale[63].

Tuttavia, preme nuovamente sottolineare che la Corte ha affrontato tale caso alla luce delle norme dell'UE sulla protezione dei dati personali che risalivano al 1995, anno in cui *internet* e *smartphone* erano fenomeni ancora poco conosciuti. La Corte, pertanto, ha dovuto conciliare diversi diritti fondamentali, la cui importanza è cresciuta parallelamente allo sviluppo e alla crescita della società digitale[64]. Le "ombre" sul diritto all'oblio sorte a seguito del caso *Google Spain* hanno sicuramente contribuito a mettere in luce le lacune normative sulla disciplina del *right to be forgotten*, non espressamente previsto in una direttiva troppo lontana per comprendere l'evoluzione del rapporto tra *internet*, cancellazione dei dati e desiderio di oblio.

---

[61] Si legge in SOLON O., *EU "right to be forgotten" ruling paves way for censorship",* 2014, disponibile su: https://www.wired.co.uk/article/right-to-be-forgotten-blog: "*one person's right to be forgotten is another person's right to remember";* v. anche ROSEN J., *The right to be forgotten,* in Standford law review online, 64, 2012, pag. 88*: "The right to be forgotten […] represents the biggest threat to free speech on the internet in the coming decade";* v. inoltre TREGUER F., *Right to be forgotten: with free expression under threat, Europe needs a "Marco Civil Moment",* in Global Voices, 2014.

[62] Si legge in TREGUER F., *Right to be forgotten: with free expression under threat, Europe needs a "Marco Civil Moment",* in Global Voices, 2014: *"accordingly, the threshold for de-indexing content is higher for a public figure than for the average citizen. So the ruling effectively gives Google the task of drawing the boundaries of whom and what belongs to the public sphere. By doing so, it is reinforcing the dangerous trend toward privatized online censorship – a trend we've gotten used to in the context of copyright enforcement*".

[63] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 69.

[64] *Ibidem.*

L’art. 17 del GDPR, rubricato diritto alla cancellazione (“diritto all’oblio”), avrà l’obiettivo di rispondere alle esigenze di maggiore protezione dei dati personali all’interno della rete, prevedendo non solo un esplicito elenco di casi in cui l’interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali, ma anche situazioni in cui tale richiesta non può essere accolta dato il suo potenziale conflitto con altri diritti fondamentali, *in primis* la libertà di informazione e di espressione.

Dall’analisi dell’art. 17, nel successivo capitolo, si cercherà di rispondere a due quesiti: in primo luogo, se la nuova disciplina del diritto alla cancellazione e del diritto all’oblio possa considerarsi innovativa rispetto a quanto precedentemente disposto all’art. 12 della direttiva 95/46/CE; in secondo luogo, se il diritto all’oblio, così come configurato dal Regolamento, possa fornire una risposta concreta alle numerose critiche emerse a seguito del caso *Google Spain,* sancendo l’esistenza di un *right to be forgotten* autonomo ed efficace.

CAPITOLO II - IL DIRITTO ALL'OBLIO NEL REGOLAMENTO 2016/679

2.1. L'art. 17 del GDPR

Come preannunciato, il GDPR prevede all'art. 17, il "diritto alla cancellazione (diritto all'oblio)" ed inserisce esplicitamente per la prima volta in un testo normativo il *right to be forgotten.*

Il diritto alla cancellazione dei dati personali configura una pretesa vantabile dall'interessato solo in presenza di determinate circostanze, oggetto di una tassativa elencazione. L' art. 17, par. 1, infatti, stabilisce che l'interessato ha il diritto di ottenere dal titolare del trattamento[65] la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, al ricorrere di uno dei seguenti motivi:

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 e non sussiste altro fondamento giuridico per proseguire con il trattamento dei dati personali;

c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento per finalità di marketing diretto;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico 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 diretti a minori[66].

[65] L'art. 4, par. 1, n.7, GDPR, stabilisce che si intende per "titolare del trattamento": "*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 […]".*

[66] Al considerando n. 65 si afferma che il diritto alla cancellazione dei dati personali è particolarmente rilevante: "*se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore*."

Dalla sopra menzionata elencazione, si può osservare che il diritto alla cancellazione dei dati personali, nell'impianto del Regolamento, non è configurato come una pretesa esercitabile discrezionalmente dall'interessato, ma ha una portata ristretta. Sotto questo profilo, l'art. 17 si limita a replicare il contenuto essenziale del diritto alla cancellazione dei dati personali precedentemente disciplinato nell'ambito della direttiva 95/46/CE[67], individuando, tuttavia, rispetto alla direttiva citata, i casi di violazione della normativa tali da rendere lecita la richiesta di cancellazione di dati, come la revoca del consenso o il trattamento dei dati dei minori nella fornitura della società dell'informazione.

L'elemento assoluto di novità è contenuto nel par. 2 dell'art. 17, in base al quale se il titolare del trattamento ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi *link,* copia o riproduzione dei suoi dati personali.

In realtà tale paragrafo, che si presenta come l'aspetto più innovativo dell'articolo in esame, ha un predecessore nell'art. 12, lett. c) della "direttiva madre", che prevedeva il diritto della persona interessata di ottenere dal titolare del trattamento "la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione […]". Risulta evidente il divario tra le due disposizioni in esame: nella direttiva era richiesta esclusivamente una notificazione ai terzi a cui il titolare aveva "comunicato" i dati, nel GDPR è previsto un obbligo in capo al titolare che ha pubblicato i dati personali di informare della richiesta di cancellazione "tutti i titolari del trattamento che stanno trattando i dati". Tuttavia, l'art. 17, par. 2, sancisce in capo al titolare del trattamento esclusivamente un'obbligazione di mezzi e non di risultato[68], imponendo di adottare le misure, tecniche e organizzative, che ci si potrebbero ragionevolmente attendere considerando la tecnologia disponibile e i relativi costi di attuazione, per informare i terzi che stanno trattando i dati personali della richiesta dell'interessato di cancellazione. In sostanza, il titolare del trattamento ha l'obbligo di informare i terzi che stiano trattando i dati personali oggetto della richiesta di cancellazione, ma non ha l'onere di verificare il

[67] L'art. 12, lett. b) della Direttiva 1995/46/CE stabiliva che l'interessato ha: "*il diritto di ottenere dal titolare del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente Direttiva, in particolare a causa del carattere incompleto o inesatto dei dati".*

[68] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion of the European Data Protection Supervisor on the data protection reform package,* 2012, pag. 24.

comportamento adottato da quest'ultimi, ossia dell'avvenuta cancellazione anche da parte dei terzi.

Tuttavia, il diritto ad ottenere la cancellazione dei dati personali non è configurato dal Regolamento come una pretesa vantabile *ad nutum* dall'interessato, in ragione del suo potenziale conflitto con altri diritti fondamentali. Pertanto, l'art. 17, par. 3, prevede, in un'ottica di bilanciamento e limitazione dell'esercizio del diritto alla cancellazione, delle eccezioni al soddisfacimento della richiesta di rimozione dell'interessato consistenti nei casi in cui il trattamento dei dati personali è necessario per:

a) l'esercizio del diritto alla libertà di informazione;
b) l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è rivestito il titolare del trattamento;
c) motivi di interesse pubblico nel settore della sanità;
d) fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici;
e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

È lo stesso art. 17, dunque, a contenere un esplicito riferimento alla necessità di bilanciare il diritto alla cancellazione con gli altri diritti fondamentali, in particolare con l'esercizio della libertà di informazione. Tale importante eccezione si ricollega al considerando 153, secondo cui, "il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente Regolamento. Il trattamento dei dati effettuato unicamente a scopi giornalisti o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente Regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e d'informazione sancito nell'art. 11 della Carta […] È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali […] Per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo". Tale previsione normativa dovrebbe mettere a tacere le numerose

critiche mosse a seguito della sentenza *Google Spain*, che identificavano il diritto all'oblio quale possibile minaccia alla libertà di espressione o di informazione[69].

Può, dunque, l'art. 17 considerarsi una novità rispetto a quanto precedentemente previsto dall'art. 12 della direttiva 95/46/CE? La risposta risulta essere affermativa. La direttiva, infatti, oltre a non prevedere il diritto all'oblio, non aveva alcun articolo specificatamente dedicato al diritto alla cancellazione – l'art. 12 era infatti rubricato "Diritto di accesso" -. La direttiva non definiva i presupposti per l'esercizio del diritto alla cancellazione, che ora invece sono strettamente disciplinati al par. 1 dell'art. 17. Ancora, la direttiva prevedeva la possibilità di rivolgersi esclusivamente al titolare del trattamento per ottenere la cancellazione dei dati personali, non prendendo in considerazione il fatto che tali dati, quando pubblicati in rete, potessero essere trasmessi ad un numero illimitato di ulteriori titolari. Tale problematica è invece affrontata dal par. 2 dell'art. 17 che sancisce l'obbligo in capo al titolare di adottare misure ragionevoli per informare gli altri titolari della richiesta di cancellazione: il titolare, dunque, oltre a cancellare i dati personali, ha l'obbligo di trasmettere la richiesta di cancellazione anche a tutti coloro che utilizzano copie, *link* o riproduzioni di detti dati personali.

Se la portata innovativa dell'art. 17 è evidente, non sono pochi i dubbi che sorgono sulla reale applicazione di tale disposizione ed in particolare sulla disciplina del diritto all'oblio.

2.2. Un'analisi critica: l'ambiguità dell'art. 17

Se con l'introduzione del *right to be forgotten* all'interno del Regolamento ci si poteva aspettare una disciplina chiara del diritto in parola e in linea con l'interpretazione fornita dalla Corte nel caso *Google Spain*, l'analisi dell'art. 17 dimostra come tali ragionevoli supposizioni siano parzialmente errate.

Un primo punto di discussione emerge già dall'analisi della rubrica dell'art. 17: il termine oblio, infatti, figura esclusivamente nella *rubrica legis* dell'art. 17 e non all'interno del testo normativo. Di qui dunque una serie di interrogativi. Qual è il rapporto che sussiste tra il diritto alla cancellazione e diritto all'oblio? L'espressione "diritto all'oblio" è da intendersi quale ulteriore specificazione del diritto alla cancellazione? Cancellazione e oblio sono da intendersi quale sinonimi o sono due diritti distinti e autonomi[70]?

[69] JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017, pag. 72.
[70] MARKOU C., The Right to be Forgotten: Ten Reason Why It Should Be Forgotten, in GUTRWIRTH, LEENES, DE HERT (ed. by.), *Reforming European Protection Law*, Springer Netherlands, 2015, pag. 208

La difficoltà di individuare le differenze tra il diritto all'oblio e alla cancellazione è emersa sin dalla Proposta di Regolamento del Parlamento europeo e del Consiglio del 25 gennaio 2012, in cui l'art. 17 era rubricato "diritto all'oblio e alla cancellazione", suggerendo l'idea che si trattasse di due tematiche ben distinte[71]. Nonostante il diritto all'oblio figurasse nella rubrica dell'art. 17, la previsione normativa del medesimo articolo era formulata esclusivamente nei termini della "cancellazione", senza alcun riferimento all'oblio e senza fornire elementi costituitivi in grado di distinguere il "*right to be forgotten"* dal "*right to erasure"*[72]. Tale omissione, dunque, ha condotto la dottrina maggioritaria a ritenere che il diritto all'oblio, così come presentato nella Proposta di Regolamento, rendesse semplicemente più "brillante" la rubrica dell'art. 17[73].

Se la prima formulazione dell'art. 17 risultava ambigua, legittimando l'idea che cancellazione e oblio fossero oggetto di due distinti diritti in capo all'interessato, anche quella inserita nel testo definitivo non ha mancato di suscitare critiche. L'espressione "oblio", come sopra sottolineato, figura esclusivamente nella rubrica dell'art. 17 del testo definitivo, e si ripete tra parentesi, dovendosi notare un cambiamento tra la stesura dell'articolo in sede di Proposta di Regolamento e il testo finale.

L'ambiguità della *rubrica legis* può essere meglio compresa analizzando il par. 2 dell'art. 17 in cui viene affrontata la problematica legata alla diffusione delle informazioni di un individuo all'interno della Rete[74]. Il diritto all'oblio, così come disciplinato all'interno del GDPR, non si configura quale diritto autonomo, formalizzato dal GDPR, ma potrebbe essere piuttosto interpretato come un'estensione e un rafforzamento del diritto alla cancellazione[75]. Si legge, infatti, nel considerando n. 66 del Regolamento che "per rafforzare il diritto all'oblio nell'ambiente *online,* è opportuno che il diritto alla cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi *link* verso tali dati personali o copia o riproduzione di detti dati personali […]".

---

[71] *Ibidem*.
[72] XANTHOULIS N., *Conceptualizing a Right to Oblivium in the Digital World: a Human Rights-based Approach*, SSRN (ATT 2064503): 17, 2012.
[73] Si legge in XANTHOULIS N. *op. cit.: "it could be true that the right to be forgotten, as presented in the new EU proposed Regulation, does not in fact add much more than a shiny title to Article 17?";* v., inoltre, MARKOU C., *op. cit.*, pag. 208.
[74] BURKET H., GASSER U., HETTICH P., THOUVENIN F., *Remembering and Forgetting in the Digital Age,* Springer, 2018, pag. 50.
[75] XANTHOULIS N., *Conceptualizing a Right to Oblivium in the Digital World: a Human Rights-based Approach*, SSRN (ATT 2064503): 17, 2012.

Ritenendo, dunque, il diritto all'oblio quale estensione del diritto alla cancellazione, analizzando l'art. 17, ed escludendo le disposizioni che si riferiscono all'obbligo del titolare del trattamento di cancellare i dati personali a seguito di una richiesta giustificata da parte di un utente, si può constatare che il "*right to be forgotten"* è sintetizzato nel GDPR all'interno del par. 2 dell'art. 17, il quale prevede che se il titolare del trattamento ha reso pubblici dati personali, sarà tenuto a prendere tutte le misure ragionevoli, per informare i terzi che effettuano il trattamento di tali dati, della richiesta dell'interessato di cancellare qualsiasi *link,* copia o riproduzione dei suoi dati personali[76].

Il fulcro del diritto all'oblio, così come disciplinato dal GDPR, risulta essere l'obbligo di informativa in capo al titolare del trattamento che ha pubblicato i dati personali. Tale obbligo determina di fatto un rafforzamento del diritto alla cancellazione di un individuo: infatti, se effettivamente la richiesta di cancellazione fosse estesa a tutti i titolari che stiano trattando *link,* copie o riproduzione dei dati personali oggetto dell'istanza di cancellazione e se, conseguentemente, anche quest'ultimi provvedessero ad accogliere tale richiesta, il diritto di un interessato ad ottenere la cancellazione dei propri dati personali all'interno della rete risulterebbe essere assolutamente rafforzato e l'oblio, inteso come sinonimo di dimenticanza, si potrebbe configurare quale possibile effetto derivante dalla cancellazione generalizzata dei dati personali all'interno del *web*. Al contrario, se l'obbligo di cancellazione incorresse esclusivamente nel titolare del trattamento che ha pubblicato i dati nella rete, il diritto di un individuo di ottenere la cancellazione dei dati personali risulterebbe alquanto debole, dato che detti dati, nel momento in cui vengono diffusi nel *web,* risultano essere oggetto di trattamento da parte di altri titolari. In conclusione, il *right to be forgotten,* così come previsto dal GDPR, non si configura come un diritto autonomo, ma piuttosto quale diritto alla cancellazione in forma rafforzata.

Ma il diritto all'oblio, così come disciplinato dall'art. 17, par. 2, può ritenersi effettivamente un diritto applicabile e in grado di innalzare il livello di protezione dei dati

[76] Si legge in XANTHOULIS N., *op. cit.*: "*[…] one possibility would be to interpret the right to be forgotten as a mere extension to the right to erasure. Under this approach the right to be forgotten would logically constitute what is left of Article 17 when we exclude the provisions that relate to the obligation of the data controller to delete personal data following a justified claim by a user. In that case, the right to be forgotten is summarised in Article 17(2) which provides that, in case the data controller has made the personal data public, it will be obliged to take all reasonable steps, including technical measures, to inform third parties which are processing such data of the erasure request made by the individual";* v. inoltre BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag 196: "*Article 17 Sec. 2 GDPR provides for* the right to be forgotten, *which is a legal consequence of the right to erasure under Art. 17 Sec. 1 GDPR".*

personali di un individuo? I dubbi al riguardo non sono pochi. La previsione pur essendo di grande impatto, nella pratica rischia di divenire sterile o foriera di confusione.

In primo luogo, l'obbligo di informativa in capo al titolare del trattamento, che come sottolineato rappresenta il fulcro del diritto all'oblio previsto dal GDPR, comporta esclusivamente un'obbligazione di mezzi e non di risultato[77]. Il par. 2 dell'art. 17, in sostanza, impone in capo al titolare del trattamento che ha reso pubblici i dati personali un mero dovere di segnalazione, senza l'onere di dover verificare il comportamento dei soggetti terzi informati della richiesta di cancellazione, che rimangono di fatto liberi circa la possibilità di accettare o meno l'istanza di cancellazione.

Tuttavia, anche la sola configurazione di un mero obbligo di mezzi presenta alcuni aspetti non poco problematici, individuati peraltro dalla stessa European Union Agency for Cybersecurity (ENISA)[78], ossia l'Agenzia europea per la sicurezza delle reti e dell'informazione che ha il compito di assistere la Commissione europea nei testi di legge afferenti alla sicurezza informatica e le reti di comunicazione. L'ENISA ha mostrato come in un sistema aperto, quale il *world wide web,* sia impossibile, una volta che le informazioni siano state pubblicate, individuare qualunque copia o riproduzione di dati personali trattati da terzi. Risulta, dunque, improbabile che il titolare del trattamento possa comunicare facilmente della richiesta di cancellazione tutti coloro che stiano trattando a loro volta i dati personali su cui è stata presentata la richiesta di cancellazione[79]. E già questo punto, a parere di chi scrive, risulta essere un grande limite per l'effettiva applicazione del diritto all'oblio, quale estensione del diritto alla cancellazione.

Peraltro, oltre alla difficoltà concernente l'individuazione dei soggetti che devono essere informati circa la richiesta di cancellazione, ulteriore elemento vago risulta essere l'oggetto d'informativa. L'art. 17, par. 2, di fatti, non chiarisce se il titolare del trattamento debba rendere edotti i terzi che stanno trattando i dati, di qualsiasi richiesta presentata o soltanto delle istanze

[77] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion of the European Data Protection Supervisor on the data protection reform package,* 2012, pag. 24.
[78] ENISA, *The Right to Be Forgotten: Between Expectations and Practice,* 20 novembre 2012.
[79] ENISA, *The Right to Be Forgotten: Between Expectations and Practice,* 20 novembre 2012, pag. 8: *"In a completely open system like the (vast) public portion of today's world-wide web, anyone can make copies of a public data item and store them at arbitrary locations. Moreover, the system does not account for the number, owner or location of such copies. In such an open system it is not generally possible for a person to locate all personal data items (exact or derived) stored about them; it is difficult to determine whether a person has the right to request removal of a particular data item; nor does any single person or entity have the authority or jurisdiction to effect the deletion of all copies. Therefore, enforcing the right to be forgotten is impossible in an open, global system, in general".*

che risultino fondate oppure se debba limitarsi a comunicare di avere effettivamente rimosso le informazioni in questione[80].

Inoltre, la disciplina del diritto all'oblio prevista dal GDPR risulta non prendere minimamente in considerazione quanto stabilito dalla Corte di Giustizia nel caso *Google Spain.* Esaminando, infatti, l'art. 17, in combinato disposto con il considerando 66, nulla si dice circa il ruolo che rispetto al trattamento di dati *online* svolgono i motori di ricerca o i *provider* gestori dei siti *internet,* diversi dai siti fonte, su cui i dati personali sono ugualmente disponibili *online* in quanto copiati da quelli. E ancora, nulla si dice riguardo il tema della deindicizzazione dei contenuti in *internet* da parte dei gestori dei motori di ricerca, da cui discende la nuova interpretazione fornita dalla CGUE nel caso *Google Spain* sul diritto all'oblio.

Al tal riguardo, risultano essere illuminanti le nuove *Guidelines* 5/2019[81], pubblicate il 2 dicembre 2019, dall'European Data Protection Board (EDPB)[82], che oltre a costituire un aggiornamento delle precedenti Linee Guida disposte dal *Working Party 29* a seguito del caso *Google Spain,* consentono di chiarire le funzioni che i gestori di un motore di ricerca sono tenuti ad assolvere in relazione all'art. 17 del GDPR, e dunque il ruolo che quest'ultimi assumono nei casi di richieste di cancellazione.

Nelle Linee Guida viene sottolineata l'essenziale differenza che intercorre nella gestione delle richieste di cancellazione tra il gestore di un motore di ricerca e gli editori di siti *web.* Le istanze di cancellazione avanzate ai primi comportano la deindicizzazione dei *link* oggetto della richiesta di cancellazione, con la conseguenza che l'informazione continuerà a rimanere disponibile all'interno del sito originario[83]. Dunque, le *Guidelines* confermano l'interpretazione

---

[80] Si legge in SARTOR G, *The right to be forgotten in the Draft Data Protection Regulation,* International Data Protection Law, 2015, vol. 5, N. 1, pag. 69: "*According to Article 17 (2), the controller who has made the data public should inform the third parties who 'are processing the data'. The content of this obligation is far from clear, with regard to both the object of this initiative and its addressees. In fact, should the controller inform third parties about any removal request by a data subject, even unfounded, or only about justified removal requests, or only about the fact that he has effectively removed the information?"*

[81] Le Linee Guida 5/2019 sono disponibili al sito https://www.garanteprivacy.it/.

[82] L'European Data Protection Board, o Comitato europeo per la protezione dei dati, è l'organismo che ha sostituito il *Working Party artcicle 29,* ed è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

[83] EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1),* 2 dicembre 2019, pag. 5: "*There are some considerations when applying Article 17 GDPR in respect of a search engine provider's data processing. In this regard, it is necessary to state that the processing of personal data carried out in the context of the activity of the search engine provider must be distinguished from processing that is carried out by the publishers of the third-party websites such as media outlets that provide online newspaper content. If a data subject obtains the delisting of a particular content, this will result in the deletion of that specific content from the list of search results concerning the data subject when the search is, as a main rule, based on his or her name. This content will however still be available using other search criteria".*

del diritto all'oblio fornita dalla CGUE nel caso *Google Spain:* le richieste di cancellazione presentate, ai sensi dell'art. 17 del GDPR, direttamente al gestore di un motore di ricerca comportano esclusivamente la deindicizzazione dei dati oggetto dell'istanza di rimozione.

Tuttavia, anche le nuove *Guidelines* risultano essere ancora incomplete: il documento tratta esclusivamente del ruolo che i gestori di un motore di ricerca sono tenuti ad assolvere in relazione al par. 1 e 3 dell'art. 17. L' EDPB, infatti, sottolinea che le Linee Guida oggetto di analisi non si applicano al gestore di un motore di ricerca al secondo comma dell'art. 17 in cui viene disciplinato l'obbligo di informativa circa la richiesta di cancellazione in capo al titolare del trattamento che ha reso pubblici i dati personali. Per tale disposizione sono previste Linee Guida specifiche separate, ma non ancora pubblicate. Ad oggi, dunque, sembrerebbe che i gestori di un motore di ricerca non abbiano l'onere di informare i siti sorgente della richiesta di deindicizzazione da parte del soggetto interessato[84]. Si attendono, tuttavia, le *Guidelines* per comprendere effettivamente la portata di tale obbligo di informativa, elemento chiave per definire l'efficacia del diritto all'oblio, quale estensione del diritto alla cancellazione.

Ma ulteriore problematica risulta essere il rapporto tra il diritto all'oblio e il diritto all'informazione, che si ricorda essere una delle questioni maggiormente dibattute a seguito del caso *Google Spain,* ove il *right to be forgotten* è stato additato come una possibile minaccia al diritto all'informazione della collettività. L'art. 17, par. 3, menziona tra le eccezioni dell'esercizio del diritto alla cancellazione ("diritto all'oblio") l'esercizio del diritto alla libertà di espressione e di informazione, che rappresentano pertanto un interesse ostativo alla richiesta di cancellazione. La problematica scaturisce dal fatto che il GDPR non prevede sanzioni nel caso di una ultrattività del responsabile del trattamento in caso di rimozione eccessiva dei contenuti, mentre è prevista una sanzione particolarmente gravosa nel caso di mancato rispetto della richiesta di cancellazione[85]. La minaccia più grave che si potrebbe verificare, data la presenza di sanzioni solo in caso di ingiustificata inottemperanza da parte del titolare del trattamento, è la possibilità che i titolari accolgano qualsiasi istanza di

[84] EUROPEAN DATA PROTECION BOARD (EDPB), *op. cit.*, pag. 6: "*This paper does not address Article 17.2 GDPR. Indeed, this Article requires data controllers who have made the personal data public to inform controllers who have then reused those personal data through links, copies or replications. Such obligation of information does not apply to search engine providers when they find information containing personal data published or placed on the internet by third parties, index it automatically, store it temporarily and make it available to internet users according to a particular order of preference7 . In addition, it does not require search engine providers, who have received a data subject's delisting request, to inform the third party which made public that information on the internet. Such obligation seeks to give greater responsibility to original controllers and try to prevent from multiplying data subjects' initiatives [...] It is also planned to have separate specific guidelines in respect of Article 17.2 GDPR".*

[85] v. art. 83 GDPR.

cancellazione che sia ritenuta fondata, senza di fatto procedere ad un'analisi approfondita circa il ricorrere di elementi validi per respingere la richiesta di cancellazione, stabiliti al par. 3 dell'art. 17[86]. Peraltro, la disposizione omette di fornire dei parametri orientativi sul bilanciamento del diritto alla cancellazione ("diritto all'oblio") e del diritto alla libertà di informazione: l'art. 85[87] del Regolamento affida tale questione al diritto degli Stati membri. Il rinvio alle legislazioni nazionali, tuttavia, potrebbe minare completamente l'obiettivo di armonizzazione alla base dell'intera riforma UE in materia di protezione dei dati personali, potendone derivare un quadro normativo estremamente frammentato all'interno dell'Unione[88].

In conclusione, l'analisi dell'art. 17 dimostra come l'attesa normativizzazione del diritto all'oblio ad opera del legislatore europeo non sia riuscita effettivamente a risolvere i numerosi quesiti sorti a seguito del caso *Google Spain,* e come l'enigmaticità della disposizione – soprattutto il vago obbligo di informativa in capo ai titolari del trattamento che hanno reso pubblici i dati personali e il bilanciamento tra il diritto all'oblio e il diritto alla libertà di informazione – aumenti la difficoltà di comprenderne la reale efficacia e portata. L'art. 17 risulta foriero di una serie di ambiguità che invece di essere definite in sede legislativa saranno sicuramente rimesse alla giurisprudenza della CGUE.

Non a caso, il diritto all'oblio sarà oggetto di ulteriore dibattito in dottrina a seguito della recentissima sentenza della Corte di Giustizia nel caso C-507/17[89] emessa il 24 settembre 2019, ove la Corte è stata chiamata ad affrontare la tematica circa l'applicabilità territoriale del *right to be forgotten* (non disciplinata nell'art. 17), che sarà di fondamentale importanza per comprendere definitivamente se il diritto all'oblio, così come previsto dal GDPR, possa considerarsi un diritto effettivamente realizzabile e in grado di innalzare il livello di protezione degli individui all'interno e al di fuori dell'Unione.

---

[86] KELLER D., *The final draft of Europe's right to be forgotten law,* in http://cyberlaw.stanford.edu/blog/, 2015.
[87] L'art. 85 del GDPR prevede che: 1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria. 2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 2 e comunica senza ritardo ogni successiva modifica.
[88] KELLER D., *op. cit.*
[89] CGUE, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)***,** 24 settembre 2019

CAPITOLO 3 - IL DIRITTO ALL'OBLIO: NON UN DIRITTO A PORTATA UNIVERSALE

3.1. L'ambito di applicazione territoriale del GDPR

Il 24 settembre 2019, a cinque anni di distanza dalla sentenza *Google Spain,* la CGUE è stata chiamata a precisare, nel caso C-507/17 (*Google Cnil)*, la portata territoriale dell'obbligo di cancellazione, chiarendo se la deindicizzazione da parte dei gestori di un motore di ricerca operi solo a livello nazionale o europeo, oppure se si estenda a livello globale.

Per comprendere, tuttavia, le motivazioni che hanno condotto la dottrina maggioritaria a ritenere che la sentenza della CGUE rappresenti un limite al diritto all'oblio, così come disciplinato dall'art. 17, è necessario soffermarsi su una delle principali novità introdotte dal GDPR, ossia l'ambito territoriale di applicabilità del Regolamento. Infatti, nonostante il GDPR sia un Regolamento europeo, il suo scopo territoriale non si limita ai confini degli Stati membri. In un'economia globale con gruppi multinazionali e trasferimenti transfrontalieri di dati, gli aspetti internazionali sono stati presi in considerazione al momento della riforma dell'Unione in tema di protezione dei dati personali[90]. L'analisi dell'ambito di applicazione territoriale del Regolamento sarà funzionale per evidenziare gli elementi di criticità rinvenuti nel caso *Google Cnil* ove l'applicazione del diritto all'oblio è stata limitata esclusivamente ai confini dell'Unione, rendendo ancor più debole la sua effettiva realizzazione.

L'art. 3 del GDPR definisce l'ambito di applicazione territoriale delle disposizioni. Si tratta di un ambito di applicazione molto ampio, che interessa diverse entità situate sia all'interno che all'esterno dell'Unione.

L'art. 3, par. 1, prevede che la normativa si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento[91] nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. Pertanto, il comma 2 dell'art. 3 estende l'applicazione al trattamento di dati personali di interessati che si trovano nell'Unione effettuato da un responsabile del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di

[90] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 22.
[91] L'art. 4, par. 8, del GDPR, definisce "responsabile del trattamento" come: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".*

servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nell'Unione.

La previsione in esame si rivela alquanto innovativa per quanto riguarda l'applicabilità territoriale del GDPR, introducendo due criteri precisi per la definizione dell'ambito di applicazione del Regolamento, tali da estendere gli effetti oltre i confini dell'Unione: il principio di stabilimento e il criterio del *target.*

Il principio di stabilimento, noto anche come *establishment criterion*, viene sancito all'interno dell'art. 3, par. 1 del GDPR[92]. In base a tale principio, il luogo geografico in cui viene effettuato il trattamento di dati è irrilevante nel determinare se tale trattamento rientri o meno nell'ambito di applicazione del GDPR: ciò che conta è, invece, che il trattamento dei dati avvenga nel contesto delle attività di uno stabilimento che si trovi nell'Unione[93]. La definizione di "stabilimento" non è contenuta all'interno della disposizione, ma il considerando 22 chiarisce che con il termine "stabilimento" si fa riferimento a qualsiasi attività effettiva e reale esercitata da un titolare o responsabile del trattamento, per mezzo di una organizzazione stabile.

Bisogna considerare che la definizione di stabilimento fornita al considerando 22 ha origine dalla giurisprudenza della Corte di Giustizia Europea nelle sentenze *Google Spain* e *Weltimmo*[94], in cui la Corte ha ampliato l'ambito di applicazione territoriale della direttiva 95/46/CE. Infatti, ai sensi dell'art. 4, par. 1, lett. a), della "direttiva madre", le norme nazionali di recepimento erano destinate ai trattamenti effettuati "nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro". In tal senso, l'applicabilità del quadro normativo dipendeva dallo svolgimento di un'attività realizzata da un'impresa stabilmente presente all'interno di uno degli Stati membri. Nel caso di soggetti extra-europei, le regole operavano solo nel caso in cui il responsabile disponesse di "strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro". Tale impostazione con l'incremento dell'utilizzo della rete e dei *social network*, strumenti

[92] *Ibidem.*
[93] EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3),* 16 novembre 2018, pag. 8: *"The text of the GDPR specifies that the Regulation applies to processing in the context of the activities of an establishment in the EU "regardless of whether the processing takes place in the Union or not". It is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR".*
[94] Corte di Giustizia, sentenza del 1ottobre 2015, causa C-230/14, *Weltimmo.*

caratterizzati dall'assenza di confini, è divenuta sempre meno efficace. In particolare, dal campo di applicazione della normativa sfuggivano proprio le grandi imprese exta-europee che dominano il panorama mondiale del mercato delle comunicazioni, come *Google.* La CGUE, pertanto, ha preceduto quando disposto nell'art. 3 del GDPR, estendendo l'ambito di applicazione della direttiva, tramite il progressivo allargamento della nozione di "stabilimento".

Nel famoso caso *Google Spain,* la Corte è stata interrogata sulla qualificabilità come stabilimento della società *Google Spain,* aperta in Spagna da *Google Inc.,* per la promozione e la vendita degli spazi pubblicitari proposti dal motore di ricerca agli abitanti di tale Stato membro. Secondo *Google* non poteva parlarsi di stabilimento in senso tecnico, dal momento che il trattamento di dati personali[95] veniva effettuato esclusivamente da *Google Inc.,* quale gestore *Google Search,* senza alcun intervento da parte di *Google Spain,* la cui attività era limitata alla fornitura di un sostegno all'attività pubblicitaria del gruppo *Google.*

Tuttavia, la Corte rileva che il concetto di stabilimento non pretende che il trattamento di dati personali venga effettuato proprio dallo stabilimento interessato, essendo sufficiente che sia effettuato nel "contesto delle attività" di quest'ultimo. D'altronde, nella specie, il fatto che ci sia una inscindibile connessione tra le attività delle due società, *Google Spain* e *Google Inc.,* è incontestabile, dato che la vendita degli spazi pubblicitari costituisce l'unico mezzo idoneo a rendere economicamente redditizia l'attività del motore di ricerca, che è offerta gratuitamente agli utenti del *web.* Nel caso *Google Spain,* dunque, risulta evidente lo sforzo della CGUE di ampliare l'ambito di applicazione territoriale della "direttiva madre", tramite un'interpretazione estensiva dell'art.4, al fine di garantire agli individui un livello elevato di protezione anche per trattamenti di dati effettuati al di fuori dell'Unione. In particolare, nell'individuare il luogo al quale collegare l'applicazione della direttiva, la Corte ritiene rilevante non tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui la società che opera il trattamento esercita la propria attività, basata sul trattamento[96].

Di pochi mesi successiva alla sentenza *Google Spain* è la sentenza *Weltimmo,* in cui la CGUE ha ulteriormente precisato la nozione di stabilimento. La domanda di pronuncia

---

[95] Si ricorda che l'art. 1, lett. b), della direttiva 95/46/CE, definiva il "trattamento di dati personali" come *qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il rafforzamento o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione".*

[96] FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, in *Dir. Inf.*, 2015, pag. 122.

pregiudiziale verteva sull'interpretazione degli artt. 4, par. 1, lett. a) e 28, paragrafi 1, 2 e 6, della direttiva 95/46/CE. Nel caso di specie, la Weltimmo, società registrata in Slovacchia, gestiva un sito *internet* di annunci immobiliari riguardanti beni situati in Ungheria. Nell'ambito di tale attività, essa trattava i dati personali degli inserzionisti. A seguito di un'ipotesi di trattamento illecito di dati, gli inserzionisti presentavano reclamo all'autorità ungherese preposta alla tutela dei dati personali, che comminava alla Weltimmo un'ammenda per aver violato la legge ungherese di attuazione della Direttiva 95/46/CE. La Weltimmo contestava la decisione dell'autorità ungherese adducendo che non avrebbe potuto irrogare l'ammenda giacché, ai sensi dell'art. 4, par.1, lett. a)[97], della citata direttiva, l'autorità ungherese di controllo non era competente e non poteva applicare il diritto ungherese nei confronti di un fornitore di servizi stabilito in un altro Stato membro, ma piuttosto, ai sensi dell'art. 28, par. 6, della citata Direttiva, detta autorità avrebbe dovuto invitare la sua omologa slovacca ad agire al suo posto. Chiamata a dirimere la controversia, la Corte suprema adiva la CGUE per chiarire se, nel caso di specie, la direttiva consentisse all'autorità ungherese di controllo di applicare la legge ungherese adottata sulla base della Direttiva e di imporre l'ammenda prevista da tale legge.

Elemento cruciale nella decisione della CGUE è stata l'interpretazione della nozione di "stabilimento". L' Avvocato Generale aveva evidenziato la necessità di un'interpretazione flessibile di tale nozione, ed in particolare, facendo esplicito riferimento al considerando 19 della Direttiva citata, ha sostenuto che "detto considerando suggerisce una concezione flessibile della nozione in parola, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata"[98]. La CGUE ha ripreso quanto affermato dall'Avvocato Generale pronunciandosi a favore di una "concezione flessibile della nozione di stabilimento […][99]". Infatti, "per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva 95/46/CE, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle

[97] L'art. 4, comma 1, lett. a), stabiliva che ciascuno Stato membro dovesse applicare le disposizioni adottate per l'attuazione della Direttiva al trattamento di dati personali: "*effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto internazionale applicabile".*

[98] Conclusioni dell'Avvocato Generale nella causa C-230/14, punto 28.

[99] Punto 29 della causa C-230/14, *Weltimmo*.

prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite *internet"*[100]. Dunque, secondo la CGUE, l'art. 4, par. 1, lett. a), della direttiva citata, deve essere interpretato nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge il trattamento.

L'interpretazione estensiva fornita dalla CGUE sulla nozione di stabilimento è confluita all'interno del Regolamento, il quale recita al considerando 22, facendo da contrappunto all'art. 3, par. 1: "lo stabilimento implica l'effettivo e reale svolgimento di attività del quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica". Dunque, il concetto di stabilimento si estende a qualsiasi attività effettiva e reale esercitata da un titolare o responsabile del trattamento, per mezzo di una stabile organizzazione. Per rientrare nell'ambito di applicazione territoriale del GDPR è sufficiente che lo stabilimento supporti economicamente il trattamento dei dati effettuato dalla società madre[101]. Ad esempio, rientra nell'ambito di applicazione del GDPR, l'attività di un'azienda automobilistica con sede legale negli Stati Uniti e una filiale di proprietà con ufficio situato a Bruxelles, avente il compito di supervisionare tutte le operazioni in Europa, compresi il marketing e le pubblicità[102]. Alla luce dell'art. 3, par. 1, del GDPR, la filiale belga potrebbe essere considerata un'organizzazione stabile che svolge attività reali ed effettive, pertanto uno "stabilimento" soggetto all'applicazione del Regolamento.

Il Regolamento opera, inoltre, un'ulteriore estensione della tutela in quanto nell'ambito di applicazione territoriale vengono fatti rientrare anche quei trattamenti di dati di soggetti che si trovano nel territorio dell'Unione, effettuati da un titolare o da un responsabile del trattamento che non siano stabiliti al suo interno, quando le attività di trattamento riguardino l'offerta di beni, la prestazione di servizi o il loro monitoraggio che abbia luogo nel territorio dell'Unione (art. 3, par. 2).

Il principio emergente dall'art. 3, comma 2, noto come criterio del target o *targeting criterion,* costituisce l'aspetto più innovativo in materia di applicazione territoriale del GDPR.

---

[100] *Ibidem.*
[101] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 24.
[102] EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3),* 16 novembre 2018.

Esso si focalizza sulla collocazione fisica degli interessati e di tutti i soggetti destinatari del trattamento dei dati, piuttosto che sul luogo in cui avviene il trattamento stesso[103]. In base a tale criterio, l'assenza di un'attività stabile nell'Unione non implica che il titolare del trattamento sia da considerarsi esonerato dall'ambito di applicazione del Regolamento[104], qualora il trattamento dei dati abbia come destinatari soggetti che si trovino nell'Unione Europea e che tale trattamento si concretizzi nell'offerta di beni o servizi, indipendentemente dal fatto che vi sia un pagamento correlato[105], o nel monitoraggio del comportamento di soggetti interessati nell'UE[106]. Tale disposizione andrà sicuramente a colpire le società internazionali che offrono servizi via *internet*[107].

Per determinare se il titolare o il responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione[108]. Fattori determinanti per definire tale intenzione sono, per esempio, l'utilizzo nell'attività di offerta di beni e prestazione di servizi di una lingua o di una valuta di utilizzo comune in uno o più Stati membri. Mentre la semplice accessibilità del sito *web,* un indirizzo di posta elettronica o l'uso della lingua abitualmente utilizzata nel paese terzo in cui è stabilita la società non sono sufficienti per accertale tale intenzione[109].

Pertanto, il servizio *online* di stampa e consegna di album fotografici personalizzabili, offerto e gestito da una compagnia turca, è soggetto alle disposizioni del GDPR nel momento in cui il sito sia disponibile in inglese, francese e tedesco, permetta il pagamento in euro e

[103] Cfr. BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 28: *"Given a global economy, characteristics like nationality or place of residence become less important for the scope of data protection and the place where a person stays becomes decisive".*
[104] EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3*), 16 novembre 2018, pag. 13: "*The absence of an establishment in the Union does not necessarily mean that processing activities by a data controller or processor established in a third country will be excluded from the scope of the GDPR, since Article 3(2) sets out the circumstances in which the GDPR applies to a controller or processor not established in the Union, depending on their processing activities".*
[105] Considerando 23, GDPR.
[106] EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3*), 16 novembre 2018, pag. 14: "*In assessing the conditions for the application of the targeting criterion, the EDPB therefore recommends a twofold approach, in order to determine first that the processing relates to personal data of data subjects who are in the Union, and second whether processing relates to the offering of goods or services or to the monitoring of data subjects' behaviour in the Union".*
[107] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 26.
[108] Considerando 23, GDPR.
[109] *Ibidem.*

garantisca la spedizione in Francia e Germania: in questo caso, risulta evidente che il servizio sia rivolto a soggetti che si trovano nell'Unione[110].

L'art. 3, par. 2, lett. b), prevede che il trattamento di dati relativo al monitoraggio del comportamento dei clienti dell'UE, nella misura in cui il loro comportamento si svolge all'interno dell'Unione, rientra nell'ambito di applicazione territoriale del GDPR. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche siano monitorate su *internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento di dati personali che consistono nella profilazione[111] della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali[112]. In breve, qualsiasi forma di *web tracking* sarà considerata monitoraggio: gli strumenti *web* di monitoraggio consentono ai *provider* dei siti *web* di analizzare il comportamento degli utenti del sito *web*, ad esempio misurando, attraverso un motore di ricerca o una pubblicità *online*, quanto tempo e quanto spesso il sito *web* è stato visitato dall'utente[113].

L'art. 3 amplia notevolmente l'ambito di applicazione territoriale del GDPR, disciplinando una tutela adeguata non solo nel caso di trattamenti all'interno dell'Unione, ma anche al di fuori dei suoi confini, data l'a-territorialità della rete. Tuttavia, l'ampliamento della tutela dei dati personali al di fuori delle frontiere dell'Unione, non verrà riconosciuto per le richieste di deindicizzazione: nel caso C-507/17 (*Google Cnil)* emergerà che il diritto all'oblio, così come disciplinato dal Regolamento, risulti essere un diritto tutto "europeo", che non possiede, almeno per il momento, una portata universale, potendosi legittimamente applicare esclusivamente all'interno dei confini dell'Unione.

[110] EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3),* 16 novembre 2018, pag. 25.
[111] In base all'art. 4, par. 4, GDPR, si intende per "profilazione": "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".*
[112] v. considerando 24, GDPR.
[113] BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR),* Springer, 2017, pag. 26.

3.2. Il caso C-507/17

Con sentenza del 24 ottobre 2019[114], la CGUE si è pronunciata sulla questione della portata territoriale del diritto alla deindicizzazione, ossia la pretesa dell'interessato, nei confronti di un gestore di un motore di ricerca, di ottenere la cancellazione di uno o più risultati dall'elenco che compare all'esito di una ricerca effettuata mediante il proprio nome.

Con decisione del 21 maggio 2015[115], la Presidente della *Commission nationale de l'informatique et des libertés (*CNIL**),** autorità francese di garanzia della *privacy,* ingiungeva a *Google* di procedere, entro il termine di quindici giorni, alla cancellazione di alcuni dei risultati visualizzati in esito alla ricerca effettuata a partire dai nomi di ventuno persone, e ciò su tutte le estensioni del nome di dominio del motore di ricerca, ossia non solo da quella principale (*google.com)* e quelle collegate agli Stati membri (es. *google.fr, .it,* etc.), ma anche quelle relative a Paesi terzi. L'azienda di Mountain View, tuttavia, rifiutava di ottemperare, limitando l'esecuzione del provvedimento alle sole declinazioni corrispondenti agli Stati membri dell'Unione, ed offrendo di applicare un "blocco geografico", consistente nell'inibizione della visualizzazione – su tutte le estensioni di *Google* – dei *link* oggetto del provvedimento, per le sole ricerche effettuate a partire da un indirizzo IP localizzato nello stato di residenza dell'interessato.

La CNIL, prendendo atto dell'inottemperanza di *Google* alla propria decisione del 21 maggio 2015, con deliberazione del 10 marzo 2016[116], irrogava a tale società la sanzione pecuniaria di 100.000 euro. Il provvedimento sanzionatorio, tuttavia, veniva impugnato da *Google* dinanzi al Conseil d'État, che sollevava il rinvio pregiudiziale, ai sensi dell'art. 267 TFUE, rivolgendo alla CGUE i seguenti quesiti interpretativi: se il diritto alla deindicizzazione, sancito dalla sentenza *Google Spain,* comporti la necessità che tale operazione sia eseguita su tutti i nomi di dominio del motore di ricerca, in modo che i risultati meritevoli di rimozione non possano più essere visualizzati; in caso di risposta negativa al primo quesito, se il citato diritto alla deindicizzazione comporti l'obbligo di *Google* di rimuovere i risultati controversi sul solo sito corrispondente allo Stato in cui si ritiene che sia stata effettuata la ricerca, ovvero, più in generale, su tutti i nomi di dominio corrispondenti alle estensioni del motore di ricerca negli

[114] CGUE, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)***,** 24 settembre 2019.
[115] Decision n. 2015-047 du 21 mai 2015 mettant en demeure la société X, disponibile sul sito *internet Legifrance*, https://www.legifrance.gouv.fr/
[116] Délibération de la formation restreinte n. 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X, disponibile sul sito https://www.legifrance.gouv.fr/

Stati membri; se, sempre in caso di risposta negativa al primo quesito, ed in aggiunta alla rimozione dei risultati solo a livello nazionale o europeo, siano obbligatorie misure tecniche ulteriori, a carico del gestore di un motore di ricerca, quali un "blocco geografico", ossia un accorgimento che impedisca la visualizzazione dei risultati controversi allorché la ricerca venga effettuata su un indirizzo IP localizzato nella Stato di residenza dell'interessato.

Sebbene alla data di presentazione della domanda di pronuncia pregiudiziale fosse vigente la direttiva 95/46/CE, la Corte ha esaminato le questioni sollevate tanto alla luce di tale direttiva quanto del Regolamento 2016/679.

Nella sentenza la Corte, che ha trattato le tre questioni pregiudiziali congiuntamente, rileva in via preliminare che lo stabilimento di *Google* sul territorio francese svolge delle attività, in particolari commerciali e pubblicitarie, che sono inscindibilmente connesse al trattamento dei dati personali effettuato per le esigenze del motore di ricerca; e che pertanto il motore di ricerca menzionato – alla luce dell'esistenza di applicazioni ponte (*gateway)* tra le sue diverse versioni nazionali – non può che essere considerato un soggetto che svolge un singolo trattamento di dati personali nel contesto delle attività del suddetto stabilimento francese[117]. La situazione sotto esame rientra pertanto nell'ambito di applicazione territoriale della legislazione dell'Unione in materia di protezione dei dati personali.

La Corte osserva che, alla luce dell'obiettivo proprio della direttiva e del GDPR di garantire un livello elevato di protezione dei dati personali in tutta l'Unione[118] e tenuto conto delle caratteristiche di *internet*, sarebbe in linea di principio giustificato prevedere che la deindicizzazione debba essere effettuata su tutte le versioni di un motore di ricerca[119]. La Corte, quindi, deduce che l'Unione dispone certamente della competenza legislativa per prevedere un obbligo, a carico del gestore di un motore di ricerca, di procedere alla deindicizzazione su tutte le versioni del suo motore di ricerca[120].

A tali premesse, lineari e coerenti segue, tuttavia, uno sviluppo della motivazione meno convincente.

La Corte, soffermandosi sull'art. 17 del GDPR, sostiene che detta disposizione, pur effettuando nell'art. 17, par. 3, lett. a), un bilanciamento tra diritto all'oblio e libertà di

[117] CGUE, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)***,** 24 settembre 2019, punto 52.
[118] *Ivi*, punto 54.
[119] *Ivi*, punto 55.
[120] *Ivi*, punto 58.

informazione degli utenti in rete, non ha proceduto a tale bilanciamento per quanto riguarda la portata territoriale di una deindicizzazione al di fuori dell'Unione[121]. Anzi, osserva la Corte, né l'art. 17, né le altre norme del GDPR, relative ai poteri attribuiti alle autorità di controllo nazionali, contemplano strumenti e meccanismi per estendere la portata di una deindicizzazione al di fuori dell'Unione[122]. In sostanza dunque, la Corte afferma che il gestore di un motore di ricerca non possa essere obbligato, né in base alla direttiva né in base al Regolamento, a rimuovere a livello mondiale i risultati deindicizzati[123]. Di conseguenza, il diritto alla deindicizzazione, sentenzia la Corte, si arresta alle frontiere dell'Unione Europea. All'interno dello spazio europeo i gestori di un motore di ricerca devono, qualora necessario, adottare misure atte ad "impedire agli utenti di *internet,* che effettuano una ricerca sulla base del nome dell'interessato a partire da uno degli Stati membri, di avere accesso, attraverso l'elenco dei risultati visualizzato in seguito a tale ricerca, ai *link* oggetto di tale domanda, o quantomeno di scoraggiare seriamente tali utenti"[124]

Tuttavia, nel penultimo paragrafo della decisione la Corte ridimensiona le conseguenze del dispositivo lasciando un certo spazio a soluzioni diverse. La CGUE, infatti, pur affermando che la deindicizzazione deve avere estensione europea, ossia i risultati devono essere cancellati da tutte le versioni del motore di ricerca, corrispondenti agli Stati membri, afferma che tale principio potrebbe prestarsi a soluzioni variabili. La Corte, infatti, osserva che il diritto dell'Unione, pur non imponendo, allo stato attuale, che la deindicizzazione verta su tutte le versioni di un motore di ricerca neppure lo vieta[125]. Pertanto, le autorità nazionali, giurisdizionali e di controllo, restano competenti ad effettuare, conformemente agli *standard* nazionali di protezione dei diritti fondamentali, un bilanciamento tra, da un lato, il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali, e dall'altro il diritto alla libertà di informazione e, al termine di tale bilanciamento, a richiedere, se del caso, che il gestore di tale motore di ricerca effettui una deindicizzazione su tutte le versioni del motore di ricerca.

La nuova pronuncia della CGUE sul diritto all'oblio non appare del tutto chiara, né risolutiva. Anzi, pur dovendosi limitare a precisare l'estensione della portata territoriale del *right to be forgotten,* la sentenza non sembra sciogliere in modo definitivo la questione.

[121] *Ivi*, punto 61.
[122] *Ivi*, punti 62 e 63.
[123] *Ivi*, punto 64.
[124] *Ivi*, punto 73.
[125] *Ivi*, punto 72.

Di fatto, la previsione di un diritto all'oblio delimitato esclusivamente al territorio dell'Unione, determina una tutela debole, e per certi aspetti, poco efficace. Non si comprende il motivo per cui i risultati di una ricerca effettuata a partire del nome di un individuo, debbano essere rimossi esclusivamente da una parte della rete, e rimanere invece disponibili, in un'altra parte della rete, ove la stessa ricerca sia effettuata da un *computer* connessosi al di fuori dell'Unione. Peraltro, l'applicazione del diritto all'oblio circoscritta di confini virtuali di singoli Stati membri può essere facilmente aggirata da qualunque utente di *internet,* che può eseguire la sua ricerca ricorrendo a un diverso nome di dominio. In pratica, l'utente, anche se si trova in Italia, può sempre utilizzare *Google.com,* invece che *Google.it*[126]. Anche la tecnica del "blocco geografico" – tecnica proposta da *Google*[127] e accolta sia dall'Avvocato Generale[128] che dalla Corte[129] – risulta facilmente aggirabile. Tale tecnica consente di escludere l'accesso alle informazioni ricercate, quando la ricerca viene eseguita all'interno di uno specifico territorio, indipendentemente dal nome di dominio utilizzato e, dunque, anche qualora venga utilizzato *Google.com.* La ricerca dell'utente di *internet,* tuttavia, potrebbe essere egualmente eseguita o in un altro paese al di fuori dell'UE o, ancor più comodamente, tramite l'utilizzo di un indirizzo IP straniero.

Peraltro, anche nelle stesse *Guidelines* pubblicate dal *Working Party 29* a seguito del caso *Google Spain,* le Autorità europee avevano sottolineato che, pur considerando che gli utenti accedono usualmente a tali piattaforme mediante i propri domini nazionali, una soluzione basata su una limitazione "europea" degli interventi dei motori di ricerca dovesse ritenersi comunque non soddisfacente[130]. Per garantire, dunque, una tutela effettiva dei soggetti interessati, le Autorità europee, nel 2014, suggerivano che "*in any case de-listing should also be effective on all relevant domains, including .com"*[131]. La decisione della Corte, tuttavia, non sembra prendere minimamente in considerazione le conclusioni, non vincolanti, a cui era giunto il *Working Party 29* e, in sostanza, la strada percorsa dalla CGUE risulta concretamente irrealizzabile in uno spazio virtuale come *internet,* assolutamente privo di frontiere.

---

[126] BEVILACQUA G., *La dimensione territoriale dell'oblio in uno spazio globale e universale,* in Federalismi.it, , ISSN1826-3534, n. 23/2019, 18 dicembre 2019, pag. 14.
[127] Dopo la scadenza del termine fissato nel provvedimento della CNIL, *Google* ha presentato una proposta complementare di "blocco geografico", che tuttavia l'Autorità francese ha ritenuto insufficiente.
[128] Conclusioni dell'Avvocato Generale nella causa C-507/17, punto 78.
[129] Si veda la sentenza in esame, punto 43.
[130] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain" and Inc V Agencia Española de Protecciòn de Datos (AEDP) and Mario Costeja Gonzalez" C-131/12*- adottate il 26 novembre 2016, pag. 3.
[131] v. punto 7 delle *Guidelines.*

Spostando, invece, il campo di analisi al di là dei confini europei, la riflessione risulta essere ancor più controversa. Alla base, infatti, della riforma attuata dal legislatore europeo in materia di protezione dei dati personali vi è la necessità di riconsegnare ai cittadini europei il potere di controllo sui propri dati personali; controllo che con l'avvento della nuova era digitale e del fluire incessante delle informazioni personali si stava disperdendo[132]. La novità principale del GDPR, come si è precedentemente analizzato, risulta essere l'ampliamento dell'applicazione territoriale della normativa, al fine di garantire un livello elevato di protezione dei dati personali non solo all'interno dell'UE, ma anche al di fuori dei suoi confini. Infatti, ai sensi dell'art. 3 e dei considerando 22) 23) 24) la tutela, deve essere accordata non solo ai casi in cui il titolare o il responsabile del trattamento siano stabiliti nell'Unione, "indipendentemente dal fatto che il trattamento sia effettuato o meno all'interno dei confini europei", ma anche a tutte quelle attività che coinvolgono i dati personali relativi a soggetti che si trovano nell'Unione ed il cui titolare o responsabile del trattamento non sia stabilito in uno degli Stati membri. La *ratio* è quella di garantire, all'interno del mondo del *web* in cui le informazioni circolano senza la presenza di confini, una piena tutela dell'individuo ogni qualvolta i propri dati siano oggetto di trattamento, indipendentemente dal luogo in cui la prestazione o il servizio si sia materialmente compiuta.

Dal momento che il GDPR amplia l'orizzonte di riferimento della normativa, non si comprende per quale ragione il diritto all'oblio non possa trovare la medesima estensione applicativa, disciplinata all'art. 3 del Regolamento. Per quale motivo, di fronte ad una legittima richiesta di cancellazione, i risultati del motore di ricerca devono permanere nei domini extraeuropei, vanificando completamente il controllo dei propri dati personali all'interno della rete?

L'analisi della sentenza C-507/17, pertanto, mette in luce l'ambiguità della disciplina del diritto all'oblio prevista dall'art. 17, dimostrando che la relativa piena realizzazione del *right to be forgotten,* presenta ad oggi notevoli difficoltà.

In particolare, il *right to be forgotten* si scontra attualmente con il carattere a-territoriale della rete, caratteristica che pone di fronte a nuove sfide di non immediata soluzione. Tale problematica emerge pienamente all'interno della sentenza dal momento che la Corte, se da un

[132] Si veda il considerando 7, in cui si afferma che l'evoluzione digitale "richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche".

lato afferma che allo stato attuale non sussiste l'obbligo per un gestore di un motore di ricerca di effettuare un intervento di deindicizzazione su tutte le versioni del proprio motore, al contempo, nella consapevolezza della debolezza di tale soluzione, lascia comunque ai singoli Stati membri la possibilità di obbligare un motore di ricerca di procedere ad una deindicizzazione a livello globale. Sembrerebbe, dunque, che nella sentenza in commento la Corte evochi l'esistenza di più diritti all'oblio, tra loro diversi: "*quello europeo, avrebbe un'estensione coincidente con il territorio dell'Unione; gli altri, di stampo nazionale, sarebbero a "geometria variabile", allargando o restringendo il proprio perimetro in misura inversamente proporzionale alle plurime libertà di informazione nazionale, anch'esse puntiformi e variabili"*[133].

Di certo, la decisione della Corte dimostra come nella realtà digitale il futuro della tutela e del bilanciamento dei diritti fondamentali necessiterà di approcci di tipo multilivello e globale, soprattutto per quanto riguarda le procedure di deindicizzazione. Effettivamente, come spiega anche la Corte, molti Stati terzi non riconoscono il diritto alla deindicizzazione o comunque adottano un approccio differente per tale diritto[134], ed inoltre, l'equilibrio tra il diritto alla protezione dei dati personali e al diritto al rispetto della vita privata, da un lato, e la libertà di informazione degli utenti di *internet,* dall'altro, può variare notevolmente nel mondo[135]: quindi, risulta ragionevole ritenere che qualsiasi conclusione inerente ad istanze di cancellazione all'interno della rete, dovrà comunque prendere in considerazione tali differenze di approccio a livello internazionale.

In particolare, risulta condivisibile quanto sostenuto dall'Avvocato Generale nella Conclusioni rese il 10 gennaio 2019 sulla vicenda *Google Cnil:* l'Avvocato Generale spiega nel dettaglio che l'applicazione extraterritoriale del diritto all'oblio da parte di un'autorità europea rischia di influenzare il comportamento di altre autorità nazionali presenti in paesi meno inclini al rispetto del diritto alla vita privata e alla protezione dei dati personali. In altri termini, ciò che l'Avvocato chiaramente teme è che dalla deindicizzazione su tutti i nomi di dominio di un motore di ricerca derivi una sorta di censura globale, dal momento che, alla luce del precedente europeo, anche le altre autorità straniere potrebbero sentirsi legittimate ed autorizzate delle ingerenti misure di deindicizzazione dei risultati di ricerca in *internet*[136]. Pertanto, un ipotetico

[133] BALDUCCI ROMANO F., *La Corte di giustizia "resetta" il diritto all'oblio,* in Federalismi.it, ISSN 1826-3534, n. 3/2020, 5 febbraio 2020, pag. 39.
[134] Si veda la sentenza in esame, punto 59.
[135] *Ivi*, punto 60.
[136] Conclusioni dell'Avvocato Generale nella causa C-507/17, punto 61.

obbligo di deindicizzazione a livello globale imposto dalle autorità nazionali nei confronti dei motori di ricerca, dovrà tener conto in maniera prospettica delle possibili ripercussioni indirette di tale decisione.

CONCLUSIONE

L'analisi effettuata evidenzia l'estrema complessità del fenomeno del diritto all'oblio, un diritto in continua evoluzione. Il *right to be forgotten,* che nasce in ambito giornalistico come diritto alla non ripubblicazione di fatti remoti sui quali si è ormai sopito l'interesse pubblico, evolve notevolmente con l'affermazione della società digitale.

Nell'ambito del diritto dell'Unione è stato proprio in relazione ad una controversia nata nell'ambito della digitalizzazione e dell'utilizzo dei motori di ricerca per la diffusione e il reperimento di notizie e informazioni, che la CGUE ha fornito un'interpretazione del diritto all'oblio alquanto innovativa, ossia quale diritto di ottenere direttamente dal gestore di un motore di ricerca, in quanto responsabile del trattamento, la deindicizzazione di informazioni personali.

Nonostante la portata innovativa di tale nuova declinazione del *right to be forgotten,* la decisione della CGUE ha messo in luce una serie di problematiche inerenti all'applicazione del diritto all'oblio, soprattutto in relazione al ruolo che i gestori di un motore di ricerca assumono nell'applicazione del *right to be forgotten* e nel bilanciamento tra il diritto alla protezione dei dati personali e il diritto della collettività ad essere informata. Dalle critiche emerse a seguito del caso *Google Spain* deriva l'introduzione del *right to be forgotten* all'interno dell'art. 17 del GDPR, ove il diritto all'oblio si configura quale diritto alla cancellazione in forma rafforzata.

Il nuovo Regolamento europeo sulla protezione dei dati personali, tuttavia, non appare risolutorio circa l'applicazione del *right to be forgotten,* anzi risulta foriero di una serie di ambiguità dovute non tanto ad una formulazione del testo normativo non del tutto chiara, ma piuttosto dalla netta difficoltà di poter risolvere le problematiche individuate nel corso del presente lavoro di ricerca (quale ad esempio l'obbligo di informativa a capo dei titolari del trattamento che hanno reso pubblici i dati personali o il ruolo dei gestori dei motori di ricerca nelle procedure di deindicizzazione) ricorrendo ad un singolo articolo all'interno dell'intero Regolamento. In definitiva, il risultato ottenuto in materia di diritto all'oblio dal Regolamento (UE) 2016/679, nel suo complesso, appare, tutto sommato, deludente.

L'art 17 non fornisce una risposta esaustiva al bilanciamento tra il diritto all'oblio e il diritto alla libertà di informazione, principale problematica rinvenuta a seguito del caso *Google Spain:* il par. 3, lett. a, dell'art. 17, in estrema sintesi, afferma che il diritto alla cancellazione non può essere riconosciuto all'interessato quando il trattamento dei dati personali sia necessario per l'esercizio del diritto alla libertà di informazione ed espressione. Problematica

principale è che il considerando 153 e l'art. 85, affidano agli stessi Stati membri il compito di conciliare la protezione dei dati personali ai sensi del Regolamento con il diritto alla libertà di espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria. Tale previsione potrebbe risultare alquanto pericolosa dal momento che potrebbe produrre discipline nazionali dissimili su un tema importante quale il rapporto tra il diritto dell'individuo alla protezione dei dati personali e la libertà di informazione della collettività.

Peraltro, l'art. 17 prevede una disciplina del diritto all'oblio che si scontra con una tecnologia non concepita per rispondere alle esigenze di tale norma. Appare infatti complesso, se non impossibile, che a seguito di una domanda di cancellazione da parte di un individuo, il titolare del trattamento che ha pubblicato i dati personali possa informare di tale richiesta tutti gli altri titolari del trattamento che stanno trattando qualsiasi *link,* copia o riproduzione dei dati oggetto dell'istanza di rimozione.

Inoltre, l'effettiva realizzazione del diritto all'oblio non trova un limite solo a livello tecnologico, ma anche a livello territoriale: mentre l'art. 3 del GDPR amplia notevolmente l'orizzonte di applicazione della normativa, estendendola anche al di fuori dei confini dell'UE, nel caso C- 507/17 la CGUE ha stabilito che non sussiste l'obbligo per un gestore di effettuare un intervento di deindicizzazione su tutte le versioni del proprio motore di ricerca. Il diritto all'oblio, così come stabilito dalla CGUE, si arresta alle frontiere dell'Unione. Tuttavia, nella consapevolezza della verosimile debolezza di tale soluzione, la CGUE lascia comunque agli Stati membri la possibilità di adottare al proprio interno decisioni più severe. Al punto 72 della sentenza, infatti, sottolineando che il diritto dell'Unione "pur se […] non impone [una deindicizzazione totale], neppure lo vieta", la Corte riconosce alle autorità di controllo o giudiziarie la competenza a richiedere ai motori di ricerca, nel rispetto delle normative interne, l'eliminazione dei *link* su tutti i domini a disposizione.

Tale apertura a soluzioni diverse e di carattere nazionale, mette in evidenza, da un lato, il livello di complessità che sottende ogni decisione di cancellazione destinata al mondo della Rete, privo di confini territoriali, e dall'altro suggerisce la necessità di affrontare le criticità che emergono nel panorama digitale non solo a livello europeo, ma anche a livello mondiale. Il *right to be forgotten*, di fatto, limitato esclusivamente ai confini degli Stati membri, non offre all'individuo una tutela adeguata dei propri dati personali.

Dunque, quali possibili soluzioni al fine di garantire la piena realizzazione del *right to be forgotten* senza limiti territoriali? Alla luce dell'analisi effettuata, seppur nella consapevolezza della reale difficoltà insita in tale soluzione, in mondo sempre più digitalmente interconnesso, ove principale caratteristica della reta risulta essere la sua a-territorialità, al fine di aumentare il livello di protezione dei dati personali e di garantire un'effettiva applicazione del diritto all'oblio, così come interpretato dal GDPR e dalla sentenza *Google Spain*, è auspicabile un rafforzamento delle misure di coordinamento e collaborazione, non solo tra le autorità di controllo europee, ma anche a livello internazionale. Di fatto, il mondo della rete, non prendendo in considerazione il trascorrere del tempo e l'esistenza dei confini territoriali, interferisce con il libero godimento di un individuo del diritto al rispetto della vita privata e del diritto alla protezione dei dati personali, e pertanto solo il riconoscimento di una tutela omogenea a livello internazionale dei dati circolanti in rete consentirebbe di garantire a tutti gli individui un livello di protezione particolarmente elevato, assicurando quel difficile desiderio di oblio, che ad oggi non risulta essere tecnicamente e universalmente possibile.

ABSTRACT

More than 20 years ago, the European Community (now the EU) felt a need to align data protection standards within the Member States in order to facilitate EU-internal, cross border data transfers. At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty, neither for individuals nor for data controllers and processors. For that reason, in 1995, the European Community adopted directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data in order to harmonise the protection of fundamental rights of individuals with regard to data processing activities and to ensure free flow of personal data between Member States.

European directives are not directly applicable in EU Member States but must be transposed into national law, so they require implementation measures in each EU Member State. Even though the directive was meant to provide complete harmonisation and a full level of protection, in practice it was transposed differently in the Member States. This resulted in the establishment of diverse data protection rules across the EU, with definitions and rules interpreted differently in national laws. Moreover, there were significant changes in information technology since the drafting of the directive in the mid-1990s. Taken together, these reasons prompted the reform of EU data protection legislation. The reform led to the adoption of the General Data Protection Regulation (Regulation (EU) 2016/679) in 2016, which became fully applicable on 25 May 2018, when the Data Protection Directive was repealed.

In contrast to the Data Protection Directive, the Regulation directly applies to its addressees. By equalising the rules for data protection, the GDPR lead to more legal certainty and removed potential obstacles to the free flow of personal data. The EU aims at regaining the people’s trust in the responsible treatment of their personal data in order to boost digital economy across the EU internal market.

One of the main innovations introduced by the GDPR is the so called “right to be forgotten”: it is the first time that this right is explicitly provided by European legislation. This dissertation aims to understand whether the right to be forgotten, as currently provided by art. 17 of the GDPR, turns out to be a new, autonomous and effective right, capable of raising the level of protection of users' personal data inside the articulated world of the net.

The right to be forgotten is, in fact, one of the most controversially discussed recent issues in data protection law: in particular, the doctrinal and jurisprudential debate on the right

to be forgotten has been strongly affected by the peculiar evolution, which in recent years, characterized the informative activity of modern societies. The right to be forgotten has taken on, in fact, different shades and connotations depending on the platforms used for the diffusion of news. This right was born in relation to the exercise of journalistic reporting, in particular, prior to the advent of the internet, this right was to be understood as the right of an individual not to see republished information lawfully published in the past, which as a result of the passage of a significant amount of time, were forgotten or unknown to the majority of the society.

Subsequently, with the development of digital society the right to be forgotten has developed as the right of a person to obtain the deletion of personal information that, otherwise, would be accessible for an indefinite period of time on the internet.

The relationship between the internet and the right to be forgotten was brought to a greater attention of the public and of the European regulator by the Court of Justice of the European Union's *Google Spain* decision in 2014, whereas the meaning of this right took on a further and innovative declination. The first Chapter of this dissertation is hence dedicated to the analysis of the new interpretation of the right to be forgotten given by the CJEU in the *Google Spain* case and the major problems that emerged after this decision.

The judgment of the CJEU on the *Google Spain* involves Mario Costeja Gonzalez, a Spanish national: in 2010 Mr. González, sought a remedy from the Spanish Data Protection Agency (Agencia Española de Protección de Datos, "the AEPD") against a Spanish newspaper company called Vanguardia, Google Spain and Google Inc. González claimed that when his name is "Googled", an article published in the newspaper of the Vanguardia from 1998 is shown. The article concerned the seizure and the auction of his property for non-payment of social security premiums. González claimed that the problem had been settled long before and that the article should have been deleted from the website in order to maintain his honour. The AEDP rejected the claim of González against the Vanguardia because the article had been published lawfully. However, the AEDP ordered Google Spain and Google Inc. to delete the information in question from their indexing database. Unsurprisingly, Google appealed the ruling to the national high court (Audencia Nacional), which referred several questions to the CJEU asking for clarification as to the application of the Data Protection Directive. Simply, the question is whether search engines should be considered data controllers and therefore whether they should provide users with instruments to modify or remove listing to inaccurate personal data.

The CJEU decided that search engines, as a data controller, have an obligation "*to remove from the list of result displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person*", even if the information displayed in that page is lawful. When analysing a data subject's request to remove links to a search result, search engine should therefore balance the interest of the subject in accordance to her right to protection of personal data and the public's interest to have access to the information.

The CJEU decision in the *Google Spain* case, therefore, provides a new interpretation of the right to be forgotten as a right to deindexing: the search engine is required to delete the links in which the information subject to the request for removal is contained, while the news continues to remain on the source site that published the information.

Commentators around the world have criticised such decision. Many scholars, in fact, believed that the judgment may interfere with free access to information and could favour censorship: the Court recognizing *Google* as a data controller has given to a private company the power to determine which result should be removed and the correct balance between the right to be forgotten and the right to be informed.

The criticisms emerged following the *Google Spain* case contributed to the introduction of the right to be forgotten in art. 17 of the GDPR titled as "right to erasure (right to be forgotten)".

The second Chapter of the thesis is dedicated to the analysis of art. 17 of the GDPR, analysing on the one hand the main innovation introduced by art. 17 on the discipline of the right to erasure and the right to be forgotten with respect to the respective provisions of directive 95/46/EC and, on the other hand, the most controversial aspects of the newly introduced regulatory framework.

In particular, according to art. 17(1), individuals have the right to request from the "data controller" the erasure of personal data relating to them in specifically provided cases such as in case the data are no longer necessary in relation to the purpose for which they were initially processed or if the consent on which the processing was based has been withdrawn.

The right to erasure is not however introduced as an absolute right, as certain exceptions to its application are provided. More specifically, art. 17(3) states that the retention of the data might be considered necessary if the protection of other interests prevail such as the exercise of the right of freedom of expression or the protection of public health.

The main problem with art. 17 is that it does not provide any clear or descriptive definition of what might constitute the right to be forgotten, and how it potentially differs from the right to erasure. The right to be forgotten is mentioned exclusively in the title of art. 17, while there is no trace of it within the legislative text. This is because GDPR does not create an independent right to be forgotten but interprets it as an extension of the right to erasure.

Under this approach the right to be forgotten would logically constitute what is left of art. 17 when we exclude the provisions that relate to the obligation of the data controller to delete personal data following a justified request by a user. The right to be forgotten is summarised in art. 17(2) which provides that, in case the data controller has made the personal data public, it will be under an obligation to take all reasonable steps, including technical measures, to inform third parties which are processing such data of the erasure request made by the individual.

The right to be forgotten, as foreseen by the GDPR, is thus enclosed in such obligation imposed on the data controller that made the personal data public to communicate the erasure demand to all other data controllers which process the personal data of the person that has requested the removal. But can the right to be forgotten, as provided by art. 17(2), be considered as a right capable of raising the level of protection of an individual's personal data? There are many doubts about that.

Firstly, the obligation of the data controller to provide information to all other data controllers that are processing personal data is quite impossible to be effectively observed in an open system, such as the world wide web: it is in fact unlikely that the data controller could easily communicate the erasure request to all those which are in turn processing the personal data relating to the relevant request for deletion.

Secondly, art. 17 does not seem to take into account the interpretation of the right to be forgotten provided by the CJEU in the *Google Spain* case: such provision, in fact, does not regulate the role of search engine operators and/or the deindexing procedure. The European Data Protection Board (EDPB) in the new Guidelines 5/2019, published on December 2, 2019, clarified the role search engines assume in case of erasure request. The erasure request made to the search engine will result in the deindexing of the links, with the consequence that the information will continue to remain available inside the original site.

Furthermore, art. 17 does not provide any reference to the territorial scope of the right to be forgotten. The article does not clarify if the personal information should be deleted from the data processor exclusively in European domains or even in the rest of the world.

The third chapter of the thesis analyses therefore the territorial application of the GDPR, regulated by art. 3., and the new judgment of the CJEU (case C- 507/17) on the territorial scope of the right to be forgotten.

Despite art. 17 nothing says about the territorial scope of the right to be forgotten, art. 3 of the GDPR perfectly regulates the territorial scope of the Regulation, providing that, although the GDPR is a European Regulation, its territorial scope does not stop at European boundaries. In fact, if neither controller nor processor is established within the EU, the GDPR can apply nevertheless: the absence of an establishment in the Union does not necessarily mean that processing activities by a data controller or processor establishment in a third country will be excluded from the scope of the GDPR, since art. 3(2) states that data processing that is related to the offering of goods or services in the EU, irrespective of whether a payment by the latter is required, falls within the territorial scope of application of the GDPR.

While art. 3 of the GDPR significantly widens the territorial scope of the Regulation, extending it also beyond the borders of the EU, the decision of CJEU in the case C-507/17, on 29 September 2019, limited the application of the right to be forgotten to the territory of Member States. The events leading to this ruling began on May 21, 2015, when the President of the *Commission national de l'informatique et des libertès* ("CNIL"), the French data protection authority served formal notice on Google that, when implementing a request to de-list search results, the company must apply the removal globally, rather than just to the domain of the requester's residence. Google refused, and limited the removal only to the EU Member States. Google proposed a "geo-blocking technique" that would prevent a user in an EU Member State from accessing links delisted in the EU. CNIL found this procedure inadequate and imposed a fine of €100.000. For this reason, Google appealed to the Conseil d'Etat for an annulment of CNIL's adjudication. The Conseil, in turn, asked the Court how to interpret the territorial scope of deindexing.

In deciding the case, the Court considered both the EU Data Protection directive of 1995 and the EU General Data Protection Regulation of 2016. The Court first established that Google fell within the territorial scope of the directive and the GDPR, given its activities in French territories. It then considered the goal of the relevant EU law: guaranteeing a "high level of

protection of personal data throughout the European Union". Nonetheless, the Court stated that the right to protection of personal data is not absolute and must be balanced against other fundamental rights and public interest in having access to information.

Given the global nature of the internet, and countries differing attitudes toward balancing the right to be forgotten and the right to information, the Court determined that it could not impose to operator to carry out de-listing on all version of its search engines, but only on the version of that search engine corresponding to all the Member States. Therefore, the right to be forgotten of an individual stops at the borders of the European Union. However, while the Court found EU law does not require de-listing on all of search engine's domain, it left open the possibility for Member States to order global removal.

The new CJEU ruling on the right to be forgotten does not appear entirely clear. Although, it should be limited to clarifying the territorial scope of the right to be forgotten, the judgement does not seem to definitively resolve the issue. The provision of a right to be forgotten confined exclusively to the territory of the EU *de facto* weakens the level of protection of personal data. It is difficult to understand why the results of search engine carried out on the basis of an individual's name should be removed exclusively from one part of the network and remain available in another part of the web where the same search is carried out by a computer connected outside EU.

In conclusion, the analysis of the *Google Cnil* case highlights the ambiguity of the right to be forgotten provided by art. 17 of GDPR, showing that the full implementation of this right, confined exclusively to the territory of the Member States, is extremely challenging.

A possible solution to guarantee the full realization of the right to be forgotten without territorial limits, could be a strengthening of coordination and cooperation measure in data protection law, not only between the European supervisory authorities, but also at international level. In fact, only the recognition of an internationally uniform protection of personal data would make it possible to guarantee all users a particularly high level of protection, giving the possibility for individuals to be effectively forgotten by the web, which to date is not technically and universally possible.

BIBLIOGRAFIA

AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI (FRA), "*Manuale sul diritto europeo in materia di protezione dei dati*", Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain" and Inc V Agencia Española de Protecciòn de Datos (AEDP) and Mario Costeja Gonzalez" C-131/12*- adottate il 26 novembre 2016.

BALDUCCI ROMANO F., *La Corte di giustizia "resetta" il diritto all'oblio*, in Federalismi.it, ISSN 1826-3534, n. 3/2020, 5 febbraio 2020, pag. 39.

BARATTA R., "*Lezioni di diritto dell'Unione Europea*", Luiss University Press, Roma, 2019.

BEVILACQUA G., *La dimensione territoriale dell'oblio in uno spazio globale e universale,* in Federalismi.it, ISSN1826-3534, n. 23/2019, 18 dicembre 2019, pag. 14.

BURKET H., GASSER U., HETTICH P., THOUVENIN F., *Remembering and Forgetting in the Digital Age*, Springer, 2018, pag. 49.

BUSSCHE A., VOIGT P., *The EU General Data Protection Regulation (GDPR)*, Springer, 2017, pag. 156.

CORRALES M, FENWICK M., FORGÓ N., *New technology, Big Data and the Law,* Springer, 2017.

ENISA, *The Right to Be Forgotten: Between Expectations and Practice,* 20 novembre 2012.

EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 3/3018 on the territorial scope of the GDPR (Article 3),* 16 novembre 2018.

EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1),* 2 dicembre 2019.

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion of the European Data Protection Supervisor on the data protection reform package,* 2012, pag. 24.

FAINI F., PIETROPAOLI S., *Scienza giuridica e tecnologie informatiche,* Giappichelli, 2017, pag. 61.

FINOCCHIARO G., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali, Zanichelli,* 2017, pag. 7.

FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in Dir. Inf., 2015, pag. 117.

FINOCCHIARO G., *La memoria della rete, in Il diritto dell'informazione e dell'informatica*", A. XXVI, Fasc. 3, 2010, pag. 391 e ss, 2014.

GUTWIRTH S., LEENES R., De HERT P., *Data protection on the move: current development in ICT and privacy/data protection,* Springer, 2016.

IASSELLI M., I fondamenti e l'evoluzione del diritto all'oblio, in CASSANO G. (a cura di), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio*, Wolters Kluwer, Vicenza, 2017, pag. 231-337.

IT GOVERNANCE PRIVACY TEAM, *Eu General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, It Governance Publishing*, 2017, pag. 197.

JOUGLEUX P., MARKOU C., PRASTITOU T., SYNODINOU T., *EU Internet Law: regulation and enforcement*, Springer, 2017.

KELLER D., *The final draft of Europe's right to be forgotten law*, in http://cyberlaw.stanford.edu/blog/, 2015.

KRANENBOURG H., *Google and the Right to Be Forgotten*, in Protection Law Rev., 2015, 1.

MARKOU C., The Right to be Forgotten: Ten Reason Why It Should Be Forgotten, in GUTRWIRTH, LEENES, DE HERT (ed. by.), *Reforming European Protection Law*, Springer Netherlands, 2015.

RICCI A., I diritti dell'interessato, in FINOCCHIARO G. (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017, pag. 179-250.

ROSEN J., *The right to be forgotten*, Standford law review online, 64, 2012, pag. 88.

ROSSI E., *Forget me…or not? La Corte di Giustizia torna sul diritto di farsi dimenticare. Prima lettura di due recenti pronunce sul "diritto all'oblio*", in http://www.sidiblog.org/, 2019.

SARTOR G, *The right to be forgotten in the Draft Data Protection Regulation*, International Data Protection Law, vol. 5, N. 1., 2015.

SOLON O., *EU "right to be forgotten" ruling paves way for censorship"*, 2014, disponibile su: https://www.wired.co.uk/article/right-to-be-forgotten-blog.

TREGUER F., *Right to be forgotten : with free expression under threat, Europe needs a "Marco Civil Moment*", in Global Voices, 2014.

XANTHOULIS N., *Conceptualizing a Right to Oblivium in the Digital World: a Human Rights-based Approach*, SSRN (ATT 2064503): 17, 2012.

GIURISPRUDENZA

Conclusioni dell'Avvocato Generale nella causa C-131/12, *Google Spain,* presentate il 25 giugno 2013.

CGUE, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [*GC*], 13 maggio 2014.

Conclusioni dell'Avvocato Generale nella causa C-230/14, *Weltimmo,* presentate il 25 giugno 2015.

CGUE, C-230/14, *Weltimmo s. r. o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság,* 1 ottobre 2015.

Conclusioni dell'Avvocato Generale nella causa C-507/17, presentate il 10 gennaio 2019.

CGUE, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL),* 24 settembre 2019.