lacittadinanzaeuropea online
Rivista di studi e documentazione sull'integrazione europea
ISSN 2785-4183
lceonline 2/2023 (www.lceonline.eu) - numero speciale

Il diritto all'oblio. Un'analisi della sua evoluzione dall'adozione del GDPR(*)

Ramón M. ORZA LINARES*

Sommario: 1. Introduzione **2.** Sviluppi della normativa europea sulla protezione dei dati. *2.1.* Premessa *2.2.* Il Regolamento dell'Unione Europea sulla protezione dei dati *2.3.* Sviluppi successivi all'entrata in vigore del GDPR **3.** Alcuni esempi di applicazione giurisprudenziale del diritto all'oblio, dopo il GDPR *3.1.* Nella giurisprudenza europea *3.1.1.* CGUE del 9 marzo 2017, causa C-398/15 *3.1.2.* CEDU del 28 settembre 2018, cause 60798/10 e 65599/10 *3.1.2.* CEDU del 28 settembre 2018, cause 60798/10 e 65599/10 *3.1.3.* CGUE del 24 settembre 2019, causa C-507/17 *3.2.* Nella giurisprudenza costituzionale spagnola *3.2.1.* STC 58/2018, 4 giugno *3.2.2.* STC 23/2022, del 21 febbraio **4.** Conclusioni

1. Introduzione

Tim Bernes-Lee, il creatore del "World Wide Web", ha pubblicato una lettera sul Guardian[1] – in occasione del 28° anniversario della sua invenzione – in cui, tra le altre cose, afferma che "abbiamo perso il controllo dei nostri dati personali", consegnandoli a società private e governi. Questo ha portato, a suo avviso, a "non poter accedere ai nostri dati personali, né decidere cosa farne, a chi darli, quali di questi dati vogliamo condividere o per cosa vengono utilizzati". Inoltre, i governi possono perseguitare gli oppositori, spiare le opinioni e limitare la libertà di espressione[2].

La rilevanza del diritto all'oblio – il "diritto alla cancellazione" – deriva dal fatto che è uno dei pochi strumenti nelle mani dei cittadini per controllare le loro informazioni private, i loro dati, disponibili su Internet. Nelle pagine che seguono ci si limiterà a presentare alcuni dei testi normativi e giurisprudenziali più rilevanti relativi a questo diritto, apparsi dopo l'approvazione del "Regolamento generale sulla protezione dei dati" (RGPD/GDPR)[3].

(*) Traduzione dallo spagnolo di Rosa Iannaccone.

* Professore di Diritto costituzionale, Università di Granada. Questa pubblicazione fa parte del progetto di "R&S&I PID2019-106118GB-I00 finanziato da MCIN/ AEI/10.13039/501100011033".

[1] T. Bernes-Lee, *Tim Berners-Lee: I invented the web. Here are three things we need to change to save it*, in *The Guardian*, 12/03/2017.

[2] Sir Timothy ("Tim") John Bernes-Lee ha stabilito la prima comunicazione tra un *client* e un server utilizzando il protocollo HTTP nel novembre 1989. Nell'ottobre 1994 ha fondato il "World Wide Web Consortium" (WWW), con sede al MIT, per supervisionare e standardizzare lo sviluppo delle tecnologie alla base del Web e del funzionamento di Internet. Nel 2002 ha ricevuto il Premio Principe delle Asturie per la Ricerca Tecnica e Scientifica, insieme a Lawrence Roberts, Robert Kahn e Vinton Cerf, "per aver progettato e realizzato un sistema [Internet] che sta cambiando il mondo offrendo possibilità prima impensabili di progresso scientifico e sociale", secondo la motivazione della giuria.

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. [NdR: in italiano v. il testo del GDPR "Arricchito con riferimenti ai Considerando - Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018", disponibile sul sito del Grarante per la protezione dei dati personali].

2. Sviluppi della normativa europea sulla protezione dei dati

2.1. Premessa

Il primo organismo internazionale a parlare della necessità di regolamentare l'uso dei dati personali in via informatica è stato il Consiglio d'Europa. Così, già nel 1967, fu costituita una commissione per studiare il conflitto tra la privacy e l'uso dei computer[4].

Come sottolinea Garzón Clariana, "nel 1968, dopo aver ottenuto il parere del Comitato giuridico dell'Assemblea, i parlamentari decisero di raccomandare al Comitato dei Ministri di prestare attenzione alla possibilità di migliorare le norme di protezione per far fronte ai rischi derivanti dal progresso tecnico, soprattutto per quanto riguarda il diritto alla privacy". Si tratta della Raccomandazione 509 del 31 gennaio 1968 su "Human rights and modern scientific and technological developments"[5].

Nel 1973 e nel 1974 sono entrate in vigore altre due risoluzioni del Consiglio dei Ministri sulla protezione della privacy dalle banche dati[6].

Già nel 1981 era stata approvata la Convenzione del Consiglio d'Europa n. 108 (28 gennaio) "sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", il cui testo è entrato in vigore il 1° ottobre 1985, dopo cinque ratifiche[7].

Il suo preambolo esprime l'intenzione delle Parti contraenti di rafforzare la protezione dei diritti e delle libertà fondamentali, e in particolare del "diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica", riaffermando l'"impegno a favore della libertà d'informazione indipendentemente dalle frontiere" e riconoscendo quindi "la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli".

Per conciliare questi diritti, sono stati stabiliti dei criteri per l'utilizzo dei dati personali, quali:
- il requisito della veridicità e del corretto utilizzo dei dati (articolo 5): essi devono essere ottenuti e trattati "lealmente e lecitamente", registrati per "finalità determinate e legittime" e non utilizzati in modo incompatibile con tali finalità, "adeguati, pertinenti e non eccedenti" rispetto alle finalità registrate, "esatti e, se necessario, aggiornati" e, infine, conservati in una forma che consenta l'identificazione degli interessati e per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati registrati;
- il divieto di trattamento automatico delle informazioni relative all'origine razziale, alle opinioni politiche, alle convinzioni religiose o di altro tipo, alla salute sessuale e alle pene detentive (articolo 6);
- la sicurezza delle registrazioni dei dati (articolo 7);
- il riconoscimento del diritto degli interessati a conoscere l'esistenza di dati che li riguardano, la possibilità di cancellarli o correggerli (articolo 8);
- il diritto di ricorrere contro qualsiasi violazione dei diritti summenzionati (articolo 8);
- i limiti che la Convenzione pone all'esercizio del diritto alla libertà di informazione sono (articolo 9, paragrafo 1);
- la sicurezza dello Stato;
- la tutela di altri diritti fondamentali.

L'articolo 3.1 della Convenzione stabilisce che essa si applica "alle collezioni automatizzate di dati a carattere personale e all'elaborazione automatica di tali dati nei settori pubblico e privato".

---

[4] Va ricordato che la Seconda guerra mondiale ha dato un forte impulso alla ricerca su ciò che oggi conosciamo come computer, che ha portato alla costruzione di numerose macchine tra il 1945 e il 1951, distribuite tra Stati Uniti e Gran Bretagna, che seguivano i principi di base del computer moderno. Tuttavia, il termine informatica è relativamente recente. È stato coniato in Francia nel 1962. In realtà, solo alla fine degli anni '70 sono comparsi i microprocessori e le prime workstation e personal computer: X. Molero Prieto, *La génesis del ordenador moderno*, in *Un viaje a la historia de la informática*, Valenzia, 2016.

[5] G. Garzón Clariana, *La protección de los datos personales y la función normativa del Consejo de Europa*, in *Revista de Instituciones Europeas,* 1/1981, 11 (https://www.cepc.gob.es/sites/default/ files/2021-12/28020rie008001009.pdf).

[6] Resolution (73) 22, *On the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, adottata il 26 settembre 1973 (https://rm.coe.int/native/0900001680502830); Resolución (74) 29, *On the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, adottata il 20 settembre 1974 (Può essere consultato in: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804d1c51).

[7] Testo della Convenzione n. 108 (https://www.garanteprivacy.it/documents/10160/10704/1798208).

Nel 2018 questa convenzione è stata modificata. La nuova versione, nota come "Convenzione 108+", è stata aperta alla firma il 10 ottobre 2018, a Strasburgo, con grande successo tra gli Stati membri e con la partecipazione di Paesi terzi extraeuropei, come Argentina, Capo Verde, Mauritius, Messico, Marocco, Senegal, Tunisia e Uruguay[8].

Gli elementi chiave di questa modernizzazione sono i principi di trasparenza e proporzionalità nel trattamento dei dati, aumentando le garanzie da adottare insieme a garanzie adeguate, quali quelle di seguito elencate.

- Specificazione delle basi giuridiche in base alle quali i dati personali possono essere trattati (articolo 5).
- Catalogo dei dati sensibili è esteso alle informazioni genetiche, ai dati biometrici che identificano in modo univoco una persona, ai dati personali relativi a reati, procedimenti e condanne e alle relative misure di sicurezza, ai dati che rivelano l'origine razionale o l'origine etnica, all'appartenenza sindacale (articolo 6).
- Obbligo di notificare almeno alle autorità di vigilanza le violazioni della sicurezza che riguardano le persone (articolo 7).
- Diritti di accesso e di cancellazione sono garantiti ed estesi e devono essere trasmesse tutte le informazioni relative al trattamento da effettuare e alle finalità (articolo 9).
- Individuazione dei responsabili del trattamento e gli incaricati del trattamento devono adottare tutte le misure necessarie per garantire la conformità alle norme sulla protezione dei dati e il principio della responsabilità proattiva è stabilito in modo analogo (articolo 10).
- I trasferimenti di dati, sia tra membri che tra Stati terzi, sono facilitati, a condizione che siano rispettate le garanzie minime (articolo 14).
- L'importanza che le autorità di vigilanza, oltre al loro ruolo di strumento sanzionatorio, investano nella formazione e nella sensibilizzazione in questo settore (articolo 16).

D'altra parte, l'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico), il 23 settembre 1980, ha adottato le "Linee guida sulla protezione della privacy e dei flussi transfrontalieri di dati personali" ("Linee guida sulla privacy") come raccomandazione del Consiglio dell'OCSE a sostegno dei tre principi che accomunano i Paesi dell'OCSE: democrazia pluralistica, rispetto dei diritti umani ed economie di mercato aperte[9].

Nelle Americhe, l'OSA (Organizzazione degli Stati Americani) ha approvato risoluzioni sul tema della protezione dei dati personali sin dal 1996 in occasione della sua Assemblea Generale. Nel 2012, il Comitato Giuridico Interamericano dell'OSA ha approvato una "Proposta di dichiarazione di principi sulla privacy e la protezione dei dati personali nelle Americhe", che contiene 12 principi in materia, e nel 2015 la "Guida legislativa sulla privacy e la protezione dei dati personali nelle Americhe".

Più di recente, l'Assemblea Generale dell'OSA ha chiesto al Comitato Giuridico Interamericano di iniziare ad aggiornare i Principi sulla Protezione dei Dati Personali, tenendo conto della loro evoluzione, compito che il Comitato sta attualmente svolgendo con il supporto del Dipartimento di Diritto Internazionale in qualità di Segreteria Tecnica[10]. Attualmente, molti Paesi americani hanno adottato proprie normative sulla protezione dei dati, tra cui Messico, Brasile[11], Cile, Colombia, Perù.

[8] Le ultime ratifiche approvate sono quelle dell'Andorra, il 18 ottobre 2022, dell'Austria, il 13 luglio 2022, dell'Albania, il 22 luglio 2022, della Romania, il 9 marzo 2022, e dell'Armenia, il 25 gennaio 2022. La Spagna ha firmato il 10 ottobre 2018 e ha ratificato il 28 gennaio 2021. L'Italia ha firmato il 5 marzo 2019 e ha ratificato l'8 luglio 2021. Significativamente, né la Svezia né la Svizzera, tra gli altri, l'hanno finora ratificata. Il testo della Convenzione e tutte le informazioni ad essa relative sono disponibili in rete.

[9] Le "Linee guida dell'OCSE sulla protezione della privacy e sui flussi transfrontalieri" sono disponibili in rete.

[10] Il documento originale in cui questi principi sono sviluppati in dettaglio è disponibile in rete (http://www.oas. org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_CJI-doc_541-17_corr1.pdf).

[11] In Brasile, dal 18 settembre 2020, l'articolo 18 della Legge generale sulla protezione dei dati riconosce il diritto dell'interessato a richiedere la cancellazione dei dati in determinate circostanze. Tuttavia, in questo Paese, una sentenza della Corte Superiore di Giustizia del 10 novembre 2016 ha concluso che il diritto all'oblio, concepito come facoltà di opporsi, a causa del trascorrere del tempo, alla divulgazione di fatti veritieri e legittimamente ottenuti pubblicati su supporti analogici o digitali, è incompatibile con la Costituzione brasiliana.

Negli Stati Uniti, la California ha approvato il "California Consumer Privacy Act", che entrerà in vigore all'inizio del 2020, che, ispirandosi alla normativa europea, prevede la protezione dei dati dei suoi residenti, con particolare attenzione alla tutela dei minori[12].

Per quanto riguarda le altre aree geografiche, la situazione è più diversificata e la regione Asia-Pacifico spicca per la sua crescente importanza economica. In questa regione, gli standard di protezione della privacy sono stati adottati già negli anni '70 e, dal 1992, è stato creato il forum APPA ("Asia Pacific Privacy Authorities") come spazio di condivisione e discussione delle Autorità per la privacy di questa regione, che comprende i rappresentanti di 19 Paesi (Australia, Canada, Colombia, Hong Kong, Giappone, Corea del Sud, Macao, Messico, Nuova Zelanda, Perù, Filippine, Singapore, Stati Uniti, tra gli altri), e le sue riunioni trattano aspetti riguardanti in particolare le nuove tecnologie, la gestione delle richieste e dei reclami in materia di privacy. Questo forum ha tenuto 56 riunioni, l'ultima delle quali si è svolta nella British Columbia (Canada) tra il 30 novembre e il 2 dicembre 2021. Nell'ambito di questo forum, sono state adottate una serie di regole sulla privacy transfrontaliera ("Cross Border Privacy Rules", CBPR) che contengono le basi per le leggi sulla privacy che devono essere adottate da ciascuno dei Paesi membri. Finora sono state accettate da Corea del Sud, Stati Uniti, Canada, Giappone e Messico. Le organizzazioni che desiderano partecipare a questo sistema devono sottoporre le proprie norme e politiche di protezione dei dati personali alla convalida di terzi per garantire la protezione dei dati personali[13].

In Africa, le norme sulla protezione dei dati esistono solo in 28 dei 55 Stati africani. Di questi, solo 15 hanno istituito autorità indipendenti per monitorare l'attuazione di tali normative[14].

2.2. Il Regolamento dell'Unione Europea sulla protezione dei dati

Per quanto riguarda l'Unione Europea, in particolare, la prima cosa da notare è che tutti i Paesi membri erano anche firmatari della Convenzione Europea dei Diritti dell'Uomo e quindi membri del Consiglio d'Europa. Pertanto, la protezione dei diritti umani, in generale, dei dati personali, non era un obiettivo iniziale delle istituzioni europee, ma, per ottenere questa protezione, l'attività di quella che oggi è l'Unione Europea poggiava sulle basi e sui principi difesi dal Consiglio d'Europa.

Tuttavia, già nel 1957, il Trattato sul funzionamento dell'Unione europea prevedeva all'articolo 16, paragrafo 1, che: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". Ci sono voluti alcuni decenni perché questa protezione si concretizzasse in norme più precise.

Nel frattempo, le Costituzioni dei Paesi europei del secondo dopoguerra includevano nei loro testi i diversi diritti umani, compresi quelli legati alla protezione della privacy e dell'intimità. Solo nel 1974 la Costituzione svedese ha inserito nell'articolo 3, nel secondo capitolo del catalogo dei diritti e delle libertà individuali, la garanzia di protezione dei cittadini "contro qualsiasi danno alla loro integrità personale derivante dall'archiviazione di dati che li riguardano attraverso l'elaborazione informatica".

Il primo atto legislativo specifico da evidenziare è la 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. Il mercato interno, nel quale è garantita la libera circolazione di beni, persone, servizi e capitali, implica anche la libera circolazione dei dati personali da uno Stato membro all'altro. L'uso del trattamento dei dati nel settore economico privato e nel campo della cooperazione amministrativa, scientifica e tecnica ha reso necessaria l'armonizzazione

---

[12] Sebbene negli Stati Uniti non esista una legislazione federale simile al GDPR, in California possiamo trovare una modifica nel *California Consumer Privacy Act* del 2018, entrato in vigore il 1° gennaio 2020, ai consumatori sono riconosciuti una serie di diritti sui propri dati, tra cui il "diritto alla cancellazione", ispirato alla legislazione europea, anche se solo sui dati che il datore di lavoro ha ottenuto direttamente dagli interessati. Anche in Russia vi è una normativa in materia nel 2020: si tratta della "Legge sul diritto all'oblio", approvata dalla Duma il 3 luglio 2015 e dal Consiglio della Federazione l'8 luglio, che ha sancito il diritto degli utenti di Internet a "richiedere la rimozione dai risultati di ricerca di informazioni inaffidabili o irrilevanti". Disposizioni simili sono contenute nella sezione 27 del Personal Data Protection Bill indiano del 2019. Per un'analisi più completa: E. Torralba, *Reflexiones sobre el alcance territorial del Derecho al Olvido*, in *Cuadernos de Derecho Transnacional,* 2/2021).

[13] Il sistema di regole sulla privacy transfrontaliera (CBPR) è disponibile in rete (https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf).

[14] Cfr. il sito web della Scuola africana sulla governance di Internet, AfriSIG (https://www.apc.org/en/project/african-school-internet-governance-afrisig) e il sito web della Dichiarazione africana sui diritti e le libertà di Internet (https://africaninternetrights.org/en).

delle leggi nazionali sulla protezione dei dati personali per evitare qualsiasi ostacolo al flusso transfrontaliero. L'articolo 32 della Direttiva 95/46/CE prevedeva un periodo di tre anni per il recepimento del contenuto della Direttiva nel diritto nazionale degli Stati membri.

Tuttavia, si è notato che le normative adottate dai Paesi dell'Unione mantengono differenze sostanziali nella regolamentazione della protezione dei dati. Si è quindi deciso che è necessaria una convergenza in questo settore così delicato per i diritti e le libertà dei cittadini[15].

Infine, nel 2016 è stato adottato il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, RGPD o General Data Protection Regulation, GDPR), entrato in vigore il 25 maggio 2018 (art. 99.2 GDPR). La sua disciplina è completata, oltre che da altre norme e tenendo presente il considerando 20 del GDPR, da Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 26 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Con specifico riferimento al diritto all'oblio[16] , o diritto alla cancellazione, questo è disciplinato dall'articolo 17 del GDPR, dove viene previsto il diritto da parte del soggetto interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano e il corrispondente obbligo del titolare del trattamento di dare seguito a tale richiesta, senza ingiustificato ritardo, qualora ricorra una delle seguenti circostanze:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo 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 di cui all'articolo 8, paragrafo 1.

Inoltre, ai sensi dell'articolo 17, paragrafo 2, qualora abbia reso pubblici dati personali e sia obbligato, ai sensi del paragrafo 1, a cancellarli, il responsabile del trattamento, tenuto conto della tecnologia disponibile e dei costi di attuazione: "adotta 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". Questo aspetto del diritto all'oblio è stato chiamato anche diritto alla deindicizzazione, in quanto si tratta non solo di "cancellare" i dati personali, ma anche di fare in modo che non vengano indicizzati dai motori di ricerca, in quanto anch'essi hanno lo status di "responsabili del trattamento" dopo la sentenza della Corte di giustizia dell'Unione europea del 13 maggio 2014[17].

Questo regolamento è stato completato in Spagna con la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (LOPD)[18], ferma restando la validità del GDPR in Spagna e nel resto dei Paesi dell'UE:

Questa legge dedica due articoli al diritto di cancellazione e al diritto all'oblio.

---

[15] Un'analisi dettagliata di questo processo decisionale si trova in R. M. Orza Linares, *La influencia regulatoria de la Unión Europea: El ejemplo del Reglamento General de Protección de Datos de la Unión Europea*, in E. Marín De Espinosa Ceballos (dir.), M. R. Moreno Torres Herrera, P. Esquinas Valverde (coord.), *El Derecho Penal en el Siglo XXI,* Valencia, 2021.
[16] Sugli sviluppi del diritto all'oblio, v. A. Moreno Bobadilla, *El derecho al olvido digital: una brecha entre Europa y los Estados Unidos*, in *Revista de Comunicación,* 18(1)/2019, in particolare pp. 261-264.
[17] CGUE del 13 maggio 2014, *Google c. CEDU e Mario Costeja*, ECLI:EU:C:2014:317.
[18] Testo disponibile in rete (https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673).

L'articolo 15 stabilisce che:

> 1. Il diritto di cancellazione è esercitato ai sensi dell'articolo 17 del Regolamento (UE) 2016/679.
> 2. Qualora la cancellazione derivi dall'esercizio del diritto di opposizione ai sensi dell'articolo 21, paragrafo 2, del regolamento (UE) 2016/679, il titolare del trattamento può conservare i dati identificativi dell'interessato necessari a impedire futuri trattamenti per finalità di marketing diretto.

L'articolo 93, che fa riferimento al diritto all'oblio nelle ricerche su Internet-stabilisce che:

> 3. Ogni persona ha il diritto di ottenere che i motori di ricerca su Internet rimuovano dagli elenchi di risultati ottenuti a seguito di una ricerca sulla base del proprio nome i link pubblicati contenenti informazioni relative alla persona stessa che siano inappropriate, inesatte, irrilevanti, non pertinenti, obsolete o eccessive o che lo siano diventate nel corso del tempo, tenendo conto delle finalità per le quali sono state raccolte o elaborate, del tempo trascorso e della natura e dell'interesse pubblico delle informazioni. Lo stesso vale nel caso in cui le circostanze personali addotte dall'interessato nel suo caso dimostrino che i suoi diritti prevalgono sul mantenimento dei link da parte del servizio di ricerca su Internet. Tale diritto sussiste anche se le informazioni pubblicate sul sito web collegato sono legittimamente conservate e non vengono cancellate dal sito web collegato prima o allo stesso tempo.
> 4. L'esercizio del diritto di cui al presente articolo non impedisce l'accesso alle informazioni pubblicate sul sito web mediante l'uso di criteri di ricerca diversi dal nome della persona che esercita il diritto.

In sintesi, e seguendo la sistematizzazione proposta da María Solange Maqueo, il diritto all'oblio presenta due aspetti principali.

Da un lato, "i riferimenti al diritto all'oblio digitale riguardano genericamente la rimozione delle informazioni disponibili su Internet". Ciò include "dalla rimozione delle informazioni personali da parte dell'editore del contenuto della pagina web di partenza alla loro rimozione dalle piattaforme su cui sono ospitate le informazioni create da terzi".

D'altra parte, il diritto all'oblio si riferisce alla "possibilità per le persone fisiche di chiedere direttamente ai motori di ricerca di deindicizzare determinati link a pagine web ottenuti tramite ricerche basate sul nome". In questo caso, non si tratta di eliminare le informazioni disponibili su Internet, ma di "limitarne la disponibilità o renderne più difficile l'accesso"[19].

2.3. Sviluppi successivi all'entrata in vigore del GDPR

L'articolo 97 del Regolamento generale sulla protezione dei dati prevede che la Commissione europea presenti, entro il 25 maggio 2020 e successivamente ogni quattro anni, una relazione sulla valutazione e sul riesame del regolamento. Tali relazioni, che saranno rese pubbliche, conterranno anche, se del caso, proposte di modifica del regolamento alla luce degli "sviluppi delle tecnologie dell'informazione e alla luce dei progressi della società dell'informazione".

In ottemperanza a tale obbligo, la Commissione ha finora preparato e presentato due relazioni: una il 24 luglio 2019 e l'altra il 24 giugno 2020.

Nella prima di queste relazioni[20], per quanto riguarda l'influenza internazionale del regolamento[21], la Commissione osserva che "un numero crescente di imprese ha promosso il rispetto dei dati personali come elemento di differenziazione concorrenziale e punto di forza nelle vendite. Questi sviluppi non si limitano all'UE, ma riguardano anche economie estere molto innovative". Per quanto riguarda l'influenza del regolamento sulle normative di altri Paesi, la relazione osserva che "poiché i Paesi di tutto il mondo si trovano sempre più spesso ad affrontare sfide analoghe", stanno adottando nuove norme sulla protezione dei dati o modernizzando quelle esistenti. Nel farlo, "Spesso tali leggi

[19] M. S. Maqueo Ramírez, *El derecho al olvido digital desde la perspectiva de la Unión Europea y la viabilidad de su extrapolación al caso de México*, in *Latin American Law Review*, 03/2019, p. 83.

[20] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Bilancio delle norme sulla protezione dei dati come catalizzatore della fiducia nell'UE e oltre* (COM/2019/374 finale), 24/07/2019 (https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=COM%3A2019%3A374%3AFIN).

[21] Sezione VI: *La convergenza verso l'alto sta progredendo a livello internazionale*. Le citazioni selezionate sono tutte tratte da questa sezione.

presentano una serie di caratteristiche comuni condivise dal regime di protezione dei dati dell'UE, come una legislazione di ampia portata piuttosto che norme settoriali, diritti individuali applicabili e un'autorità di controllo indipendente". Per la Commissione, quindi, "questa tendenza è veramente globale, dalla Corea del Sud al Brasile, dal Cile alla Thailandia, dall'India all'Indonesia. La partecipazione sempre più universale alla "Convenzione 108" del Consiglio d'Europa, recentemente modernizzata con un contributo significativo della Commissione, è un altro evidente indizio di questa tendenza alla convergenza verso l'alto".

Come sottolinea Jorge Pérez, "l'influenza internazionale del pacchetto normativo europeo è innegabile". E porta come esempio la Decisione di esecuzione (UE) 2019/419 della Commissione, del 23 gennaio 2019, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguatezza della protezione dei dati personali da parte del Giappone ai sensi della legge sulla protezione dei dati personali, che – a suo avviso – "evidenzia questa influenza in questo periodo di applicazione del Regolamento generale"[22].

La relazione sottolinea inoltre, per quanto riguarda il flusso di dati, che "altri Paesi che hanno messo in atto strumenti di trasferimento simili all'adeguatezza del Regolamento hanno riconosciuto che l'UE, così come i Paesi riconosciuti dall'UE come "adeguati", garantiscono il necessario livello di protezione", citando in particolare Argentina, Colombia, Israele e Svizzera.

Questa fiducia reciproca "può creare una rete di paesi nel contesto della quale i dati possono circolare liberamente". Inoltre, la Commissione osserva che "è in corso un intenso lavoro con altri Paesi terzi, quali il Canada, la Nuova Zelanda, l'Argentina e Israele che mira a garantire la continuità, ai sensi del regolamento, delle decisioni di adeguatezza adottate sulla base della direttiva sulla protezione dei dati del 1995". Inoltre, "lo scudo UE-USA per la privacy si è dimostrato uno strumento utile per garantire flussi di dati transatlantici basati su un livello elevato di protezione, con oltre 4 700 imprese partecipanti".

Infine, la Commissione rileva il desiderio di incrementare il dialogo con le organizzazioni e le reti regionali "quali l'Associazione delle nazioni del sud-est asiatico (ASEAN), l'Unione africana, il forum delle autorità di protezione dei dati Asia-Pacifico (APPA, Asia Pacific Privacy Authorities forum) o la rete per la protezione dei dati ibero-americana (Ibero-American Data Protection Network)", in quanto il loro ruolo è sempre più importante nella formulazione di standard comuni di protezione dei dati, nel favorire lo scambio di migliori pratiche e nel promuovere la cooperazione tra le autorità preposte alla protezione dei dati. Si mostra altresì interessato a collaborare con "l'Organizzazione per la cooperazione e lo sviluppo economico e la Cooperazione economica Asia-Pacifico", per sviluppare la convergenza verso un alto livello di protezione dei dati.

Un anno dopo, la Commissione ha presentato la seconda delle relazioni (COM/2020/264 definitivo) che, significativamente, si intitola "La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati"[23]. In questo senso, e con riferimento all'argomento di queste pagine, la Commissione osserva che "la necessità di garantire la fiducia e la domanda di protezione dei dati personali non sono certamente aspetti limitati all'UE" e che "le e persone fisiche di tutto il mondo conferiscono un'importanza sempre maggiore alla tutela della vita privata e alla sicurezza dei loro dati"[24].

La Commissione fa riferimento a uno studio, che ha coinvolto 2.600 consumatori in tutto il mondo, da cui è emerso che un numero significativo di consumatori ha già preso provvedimenti per proteggere la propria privacy, ad esempio cambiando società o provider a causa delle loro politiche sui dati o delle pratiche di condivisione delle informazioni[25].

Per quanto riguarda l'influenza internazionale del Regolamento, la relazione osserva che: "l'adozione del regolamento generale sulla protezione dei dati ha spinto altri paesi in numerose

[22] J. Pérez Miras, *Il bilancio del primo anno di applicazione del Regolamento generale sulla protezione dei dati della Commissione europea*, in *EnRed@2.0 Revista Digital por y para emplead@s de la Junta de Andalucía*, 6/02/2020.

[23] Comunicazione della Commissione al Parlamento europeo e al Consiglio, "La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati" (Bruxelles, 24.6.2020 COM(2020) 264 finale) (https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=COM%3°2020%3A264%3AFIN).

[24] *Ibid*.

[25] CISCO, *Indagine sulla privacy dei consumatori,* 2019.

regioni del mondo a prendere in considerazione la possibilità di seguire l'esempio". La relazione rileva che questa tendenza è "realmente universale", e va "dal Cile alla Corea del Sud, dal Brasile al Giappone, dal Kenya all'India e dalla California all'Indonesia"[26]. Ciò sottolinea la leadership dell'UE nella protezione dei dati e la sua capacità di "fungere da punto di riferimento a livello mondiale per la regolamentazione dell'economia digitale". Lo stesso Segretario generale delle Nazioni Unite António Guterres ha osservato che il GDPR ha "costituito un esempio ispiratore [...] per misure analoghe altrove" e ha "esortato l'UE e i suoi Stati membri a continuare a svolgere un ruolo di guida nel plasmare l'era digitale e ad essere all'avanguardia nell'innovazione tecnologica e nella regolamentazione"[27].

La relazione fa inoltre riferimento alla necessità di garantire l'applicazione del regolamento alle attività di trattamento "degli operatori stranieri attivi sul mercato dell'UE". A tal fine, è essenziale "che tale ampliamento di portata si rifletta adeguatamente nelle azioni di esecuzione attuate dalle autorità di protezione dei dati.". In particolare, esse "dovrebbero garantire il coinvolgimento, ove necessario, del rappresentante nell'UE del responsabile del trattamento o dell'incaricato del trattamento, e dovrebbe essere possibile rivolgersi a tale rappresentante in aggiunta o in sostituzione della società stabilita al di fuori dell'UE". Questo approccio dovrebbe essere perseguito "con maggior vigore" per chiarire che "mancanza di uno stabilimento nell'UE non esonera gli operatori stranieri dalle loro responsabilità ai sensi del regolamento generale sulla protezione dei dati".

E per promuovere la convergenza globale nel campo della protezione dei dati, la Commissione "a intensificato il proprio dialogo in una serie di consessi bilaterali, regionali e multilaterali al fine di promuovere una cultura globale di rispetto della vita privata e di sviluppare elementi di convergenza tra sistemi diversi di tutela della vita privata". Nel portare avanti questi sforzi, la Commissione si è affidata – e continuerà a farlo – al sostegno attivo del Servizio europeo per l'azione esterna, della rete di delegazioni dell'UE nei Paesi terzi e delle missioni presso le organizzazioni internazionali. Ciò ha permesso anche una maggiore coerenza e complementarietà tra i diversi aspetti della dimensione esterna delle politiche dell'UE, dal commercio al nuovo partenariato Africa-UE. Anche il G20 e il G7 hanno recentemente riconosciuto il contributo della protezione dei dati alla fiducia nell'economia digitale e ai flussi di dati, in particolare attraverso il concetto di "flusso transfrontaliero di dati", proposto per la prima volta dalla presidenza giapponese del G20. La strategia sui dati sottolinea l'intenzione della Commissione di promuovere ulteriormente lo scambio di dati con partner fidati, combattendo al contempo gli abusi, come l'accesso sproporzionato ai dati personali da parte di autorità pubbliche (straniere).

In definitiva, la Commissione è impegnata a promuovere la diffusione internazionale della cultura della protezione dei dati, in particolare:

- sostenere i processi di riforma in corso nei Paesi terzi per quanto riguarda le norme di protezione dei dati nuove o aggiornate, attraverso lo scambio di esperienze e di buone pratiche;
- collaborare con i partner africani per promuovere la convergenza normativa e sostenere lo sviluppo delle capacità delle autorità di vigilanza nell'ambito del capitolo digitale del nuovo partenariato Africa-UE;
- valutare come facilitare la cooperazione tra gli operatori privati e le autorità di contrasto, in particolare negoziando quadri bilaterali e multilaterali per il trasferimento dei dati nel contesto dell'accesso delle autorità di contrasto straniere alle prove elettroniche, al fine di evitare conflitti normativi, garantendo al contempo la presenza di adeguate garanzie di protezione dei dati;
- collaborare con organizzazioni internazionali e regionali come l'OCSE, l'ASEAN o il G20 per promuovere flussi di dati affidabili basati su standard elevati di protezione dei dati, anche nel contesto dell'iniziativa "free flow of data with confidence";
- istituire una "Accademia della protezione dei dati" come piattaforma in cui le autorità di protezione dei dati dell'UE e dei Paesi terzi possano condividere conoscenze, esperienze e migliori pratiche per facilitare e sostenere la cooperazione tra le autorità per la privacy e per facilitare e sostenere gli scambi tra le autorità di regolamentazione europee e internazionali;

[26] Un "successo" normativo, quello del GDPR, che il Parlamento europeo vuole ora ripetere approvando un apposito regolamento sull'intelligenza artificiale ("Artificial Intelligence Act"). E. Pérez, *"Aspiramos a que incluso China nos explique sus algoritmos": tres eurodiputados españoles nos cuentan qué se juega Europa con la AI*, in *Xakata*, 9/05/2022.

[27] A. Guterres, *Secretary-General, Addressing Italian Senate, Warns of 'Great Fracture' amid Rising Great-Power Rivalry, Asymmetric Conflicts, Climate Crisis*, 18/12/2019 (https://press.un.org/en/2019/sgsm19916.doc.htm).

- promuovere la cooperazione internazionale tra le autorità di vigilanza, anche attraverso la negoziazione di accordi di cooperazione e assistenza reciproca.

Per quanto riguarda specificamente il diritto all'oblio (o diritto alla cancellazione), la Commissione osserva che, secondo i risultati di un'indagine sui diritti fondamentali del 2019, "il 69% della popolazione dell'UE di età superiore ai 16 anni ha sentito parlare del GDPR e il 71% delle persone nell'UE conosce la propria autorità nazionale per la protezione dei dati", il che dimostra che "le persone sono sempre più consapevoli dei loro diritti: diritti di accesso, rettifica, cancellazione e portabilità dei dati personali, diritto di opposizione al trattamento dei dati personali e maggiore trasparenza"[28]. Tuttavia, la Commissione rileva la necessità di "adottare ulteriori orientamenti pratici, di facile comprensione, e che forniscano risposte chiare nonché ad evitare ambiguità sulle questioni relative all'applicazione del regolamento generale sulla protezione dei dati, ad esempio in materia di trattamento di dati di minori e di diritti degli interessati, compreso l'esercizio del diritto di accesso e del diritto di cancellazione, consultando le parti interessate nel processo"[29].

Anche la risposta dell'Unione Europea all'epidemia di coronavirus è stata molto importante, anche se la sua analisi esula dallo scopo di queste pagine, nonostante l'indubbio legame di molte delle misure adottate con la protezione dei dati personali (confinamento, registrazione dei vaccinati, controllo dei passeggeri, passaporto covid, controllo dell'accesso a imprese o stabilimenti legati al turismo, ecc.).

Particolarmente degni di nota sono gli strumenti digitali che l'Unione europea ha promosso in relazione a questa pandemia. Attraverso la sua "Strategia digitale" (2019-2024), ha cercato di "garantire che gli europei possano rimanere connessi e sicuri online". Da notare anche la collaborazione instaurata con Google, Facebook, Twitter e Microsoft per garantire che queste aziende promuovano attivamente fonti di informazione autorevoli sul coronavirus, oltre a limitare i contenuti falsi o fuorvianti. Più precisamente, Google Search si è impegnato a dare risalto agli articoli pubblicati dalle organizzazioni di "fact-checking" dell'UE, Facebook e Instagram hanno indirizzato più di 2 miliardi di persone in tutto il mondo verso le risorse dell'OMS e di altre autorità sanitarie attraverso un "Information Hub", Twitter ha raccolto gli ultimi tweet da una serie di fonti autorevoli e affidabili nelle lingue locali, YouTube ha pubblicato pannelli informativi con link a funzionari sanitari globali e locali, sia sulla sua homepage che nei video e nelle ricerche del COVID 19, e la pagina TikTok del COVID-19 ha ricevuto più di 52 milioni di visite nei cinque maggiori mercati europei (Regno Unito, Germania, Francia, Italia e Spagna) .

Inoltre, la Commissione europea e la Rete di cooperazione per la tutela dei consumatori, istituita dal Regolamento (CE) 2006/2004 sulla cooperazione per la tutela dei consumatori, sono state in costante contatto con le principali piattaforme online: Allegro, Amazon, Alibaba/ AliExpress, CDiscount, Ebay, Facebook, Google, Microsoft/Bing, Rakuten, Verizon Media/Yahoo e Wish, per condividere informazioni su possibili frodi e truffe. Come risultato di questa cooperazione, queste piattaforme hanno rimosso centinaia di milioni di offerte e pubblicità relative al coronavirus, dichiarando al contempo il loro forte impegno nella protezione dei consumatori e contro le pubblicità che potrebbero offrire "virtù miracolose" contro il virus.

3. Alcuni esempi di applicazione giurisprudenziale del diritto all'oblio, dopo il GDPR.

3.1. Nella giurisprudenza europea.

3.1.1. CGUE del 9 marzo 2017, causa C-398/15.

Nel 2017, la Corte di giustizia dell'Unione europea ha dovuto pronunciarsi in via pregiudiziale sulla possibilità per l'amministratore unico di una società che in passato era stata sottoposta a una procedura di insolvenza e alla successiva liquidazione di chiedere la cancellazione dello "storico" dal registro pubblico delle imprese, sostenendo che tali informazioni, che le società di rating utilizzano

[28] Comunicazione della Commissione al Parlamento Europeo e al Consiglio, *La protezione dei dati come pilastro dell'autonomia dei cittadini*, cit.
[29] *Ibid*.

per redigere i rapporti, gli avevano causato un grave danno reputazionale o economico, dissuadendo i potenziali acquirenti di immobili da una nuova società di cui era amministratore unico[30].

In una prima decisione, il Tribunale di Lecce, in data 1° agosto 2011, ha accolto le domande dell'attore e ha condannato la Camera di Commercio di Lecce "all'anonimizzazione dei dati che collegano il sig. Manni alla liquidazione dell'Immobiliare Salentina e la condanna al risarcimento del danno subito dall'attore, fissato in 2000 euro, oltre interessi e spese"[31]. Il Tribunale di Lecce ha quindi ritenuto che "le annotazioni che collegano il nome di una persona fisica a una fase critica della vita dell'impresa (quale la procedura concorsuale) non possono essere indeterminate, in assenza di uno specifico interesse generale alla loro conservazione e divulgazione". Poiché il Codice Civile non prevede una durata massima dell'iscrizione, ha ritenuto che, "trascorso un congruo periodo di tempo dalla chiusura della procedura concorsuale della società in questione e dalla cancellazione delle sue iscrizioni nel registro delle imprese, la necessità e l'utilità, ai sensi del D.Lgs. n. 196, dell'indicazione del nome della persona fisica della società nella ragione sociale non può essere indefinita, in assenza di uno specifico interesse generale alla sua conservazione e divulgazione". "L'indicazione del nome dell'ex amministratore unico di tale società al momento della sua liquidazione viene meno, in quanto l'interesse pubblico di una "memoria storica" dell'esistenza della società e delle difficoltà da essa attraversate [può] essere soddisfatto in larga misura anche attraverso dati anonimi"[32] .

In risposta al ricorso presentato dalla Camera di Commercio, la Corte di Cassazione ha deciso di sottoporre una questione pregiudiziale alla Corte di Giustizia dell'Unione Europea.

La CGUE ha ritenuto che il trattamento di tali dati, che erano illegittimi, fosse coperto dal diritto comunitario, in quanto lo scopo del sistema di pubblicità che esso stabilisce è quello di tutelare, in particolare, gli interessi dei terzi in relazione alle società per azioni e alle società a responsabilità limitata, in quanto, come garanzia nei confronti dei terzi, esse offrono solo il loro patrimonio e le loro passività. A tal fine, la pubblicità deve consentire ai terzi di conoscere gli atti essenziali della società e alcune informazioni che la riguardano, in particolare l'identità delle persone che hanno il potere di vincolarla[33]. Inoltre, da questo punto di vista, è importante che chiunque desideri instaurare e mantenere relazioni commerciali con società stabilite in altri Stati membri possa facilmente venire a conoscenza degli elementi essenziali relativi alla costituzione delle società commerciali e dei poteri delle persone autorizzate a rappresentarle, il che richiede che tutte le informazioni pertinenti siano esplicitamente riportate nel registro[34]. Inoltre, "possono sorgere questioni che richiedono che questi dati siano disponibili molti anni dopo che una società ha cessato di esistere"[35]. Pertanto, "sembra giustificato che le persone fisiche che decidono di partecipare a scambi economici attraverso una società di questo tipo siano obbligate a rendere pubblici i dati relativi alla loro identità e alle loro funzioni all'interno di essa, a maggior ragione se sono consapevoli di tale obbligo nel momento in cui decidono di intraprendere tale attività"[36]. Tuttavia, data "la notevole eterogeneità dei termini di prescrizione previsti dalle varie normative nazionali nei diversi settori del diritto, come evidenziato dalla Commissione, è attualmente impossibile individuare un termine unico a partire dallo scioglimento di una società, allo scadere del quale l'iscrizione di questi dati nel registro e la loro divulgazione non sono più necessari"[37].

3.1.2. CEDU del 28 settembre 2018, cause 60798/10 e 65599/10

Per quanto riguarda la Corte europea dei diritti dell'uomo, in una sentenza del 2018[38], essa applica anche la giurisprudenza sul diritto all'oblio stabilita dalla Corte di giustizia dell'Unione europea.

---

[30] CGUE del 9 marzo 2017, causa C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*. Un'analisi di questa sentenza si trova in E. Guichot, *El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español*, in *Revista de Administración Pública,* 2009.
[31] *CGUE del 9 marzo 2017*, para. 27.
[32] *Ibid.*, para. 28.
[33] *Ibid.*, para. 49.
[34] *Ibid.*, para. 50.
[35] *Ibid.*, para. 54.
[36] *Ibid.*, para. 59.
[37] *Ibid.*, para. 55.
[38] CEDU del 28 settembre 2018, cause 60798/10 e 65599/10, *M. L. e W. W. c. Germania*.

In questo caso, due fratelli sono stati condannati nel 1993 in Germania all'ergastolo per l'omicidio di un attore tedesco. Sono stati rilasciati con la condizionale nel 2007 e nel 2008. La vicenda è stata riportata e analizzata da diversi media, sia nelle loro edizioni cartacee che sui rispettivi siti web. Dopo il loro rilascio, i fratelli hanno cercato di ottenere l'anonimizzazione di tutte le informazioni che li riguardavano e, non riuscendoci, si sono rivolti al tribunale. Nei primi giudizi hanno ottenuto sentenze a favore delle loro richieste, ma, infine, la Corte federale di giustizia ha respinto le loro richieste in quanto, come sottolinea E. Guichot, "sarebbe un modo per cancellare la storia a vantaggio di chi ha commesso il reato e avrebbe un effetto dissuasivo sulla libertà di informazione, obbligando a controllare regolarmente tutti i loro archivi, con il conseguente [sforzo] in termini di tempo e personale"[39].

Nel loro ricorso alla Corte europea dei diritti dell'uomo, i ricorrenti hanno sostenuto di essere stati nuovamente confrontati con il loro reato quando, dopo aver scontato la loro pena di oltre quindici anni, si stavano preparando per il loro reinserimento nella società. Il mantenimento su Internet dei fascicoli che li riguardano li stigmatizza ancora una volta. Ritengono che, finché le informazioni su una condanna pronunciata anni fa sono disponibili su un portale Internet, saranno lette allo stesso modo da un vicino di casa o da un datore di lavoro, indipendentemente dal fatto che siano state scritte di recente o all'epoca della condanna. In entrambi i casi la persona bersaglio verrebbe marchiata con il timbro di un assassino[40].

Inoltre, i ricorrenti imputano alla Corte Federale di Giustizia di non aver riconosciuto i pericoli specifici dell'era di Internet. Secondo i ricorrenti, che si basano su una sentenza del 1973 della Corte costituzionale tedesca nel caso Lebach, un programma televisivo cade nell'oblio dopo un certo periodo di tempo, mentre i motori di ricerca su Internet consentono di ottenere informazioni su un evento specifico in qualsiasi momento, gratuitamente, rapidamente, ovunque e continuamente. La diffusione su Internet costituirebbe quindi una violazione duratura del diritto al rispetto della vita privata[41]. Per quanto riguarda il rifiuto della Corte Federale di obbligare i media a controllare sistematicamente tutti i loro archivi, i ricorrenti fanno riferimento al fatto che ciò non sarebbe necessario, ma solo in caso di espressa richiesta di anonimato da parte della persona interessata in un rapporto e che i costi relativi alla richiesta potrebbero essere sostenuti dal richiedente al fine di ridurre ogni possibile effetto deterrente sulla stampa[42]. I ricorrenti si chiedono se, vent'anni dopo la loro condanna, esista ancora un particolare interesse pubblico a essere informati sull'evento in questione. Essi ritengono che tale interesse sarebbe soddisfatto anche se potessero apparire in forma anonima nelle notizie, cosa che, sostengono, richiederebbe un intervento tecnico minimo[43]. Sottolineano che, anche se l'anonimizzazione al 100% non è possibile, non si tratta di rinunciare a tutte le forme di anonimizzazione. Sostengono che, con i mezzi ora disponibili negli archivi di Internet, dovrebbero essere obbligati a fare tutto il possibile per limitare la diffusione di informazioni per le quali è stata richiesta l'anonimizzazione[44] .

Pur ribadendo la sua dottrina sull'autodeterminazione informativa, che considera inclusa nel rispetto della vita privata sancito dall'articolo 8 della Convenzione europea dei diritti dell'uomo, la Corte ritiene che l'attacco alla reputazione personale debba comportare un certo livello di gravità ed essere stato attuato in modo tale da compromettere il godimento personale del diritto al rispetto della vita privata. Inoltre, "questa disposizione non può essere invocata per lamentarsi di un danno alla reputazione che deriverebbe prevedibilmente da azioni proprie, come un reato"[45]. Per E. Guichot, il requisito che il danno sia di una certa gravità segnerebbe un allontanamento dalla giurisprudenza della Corte di giustizia dell'Unione europea[46].

A ciò si aggiunge la visione coerente della Corte sul ruolo essenziale della stampa in una società democratica, che comprende la cronaca e il commento dei procedimenti giudiziari. La Corte osserva che "è inconcepibile che le questioni trattate dai tribunali non possano, prima o allo stesso tempo, dare

[39] E. Guichot, *Il riconoscimento e lo sviluppo del diritto all'oblio*, cit., pp. 62-63.
[40] CEDU del 28 settembre 2018, cause 60798/10 e 65599/10, *M. L. e W. W. c. Germania*, para. 68.
[41] *Ibid.*, para. 69.
[42] *Ibid.*, para. 71.
[43] *Ibid.*, para. 72.
[44] *Ibid.*, para. 73.
[45] *Ibid.*, para. 88.
[46] E. Guichot, *Il riconoscimento e lo sviluppo del diritto all'oblio*, cit., p. 63.

luogo a discussioni altrove, sia nelle riviste specializzate, sia nella stampa tradizionale o tra il pubblico in generale". Oltre al ruolo dei media nel diffondere tali informazioni e idee, esiste "il diritto del pubblico di riceverle". Altrimenti, "la stampa non sarebbe in grado di svolgere il suo indispensabile ruolo di "cane da guardia". Inoltre, non spetta alla Corte, né ai tribunali nazionali, sostituirsi alla stampa nella scelta della modalità di informazione da adottare in un determinato caso..."[47]. A ciò si aggiunge una funzione accessoria, ma di indubbia importanza, che consiste nel costituire archivi di informazioni già pubblicate e nel metterli a disposizione del pubblico, contribuendo notevolmente alla conservazione e all'accessibilità delle notizie e delle informazioni; sono una fonte preziosa per la didattica e la ricerca storica, soprattutto perché sono immediatamente accessibili al pubblico e generalmente gratuiti[48].

Dopo aver ribadito il rispetto del margine di apprezzamento dei tribunali nazionali, la Corte ribadisce i principi rilevanti per risolvere i conflitti tra la libertà di espressione o di informazione e i diritti alla vita privata e alla privacy, ossia il contributo a un dibattito di interesse generale, la notorietà della persona e dell'oggetto del reportage, la condotta precedente della persona, il contenuto, la forma e l'impatto della pubblicazione e, se del caso, le circostanze in cui sono state scattate le fotografie[49].

In ogni caso, la Corte ritiene che la comparsa dei motori di ricerca su Internet abbia facilitato la ricerca di informazioni da parte degli interessati, cosicché gli obblighi di tali motori di ricerca nei confronti degli interessati possono essere diversi da quelli dell'editore che origina le informazioni. Il bilanciamento degli interessi in gioco può quindi portare a risultati diversi a seconda che l'azione di cancellazione sia diretta contro l'editore iniziale delle informazioni, la cui attività è generalmente al centro di ciò che la libertà di espressione cerca di proteggere, o contro un motore di ricerca il cui interesse principale non è quello di pubblicare le informazioni iniziali sulla persona interessata, ma in particolare di rendere possibile, da un lato, la localizzazione di tutte le informazioni disponibili su tale persona e, dall'altro, di stabilire così un profilo di tale persona[50].

Per tutte queste ragioni, e dopo aver analizzato i criteri stabiliti per stabilire il conflitto tra libertà di informazione e privacy, ha concluso all'unanimità che non c'è stata alcuna violazione dell'articolo 8 della Convenzione[51].

3.1.3. CGUE del 24 settembre 2019, causa C-507/17

In relazione all'ambito di applicazione del diritto europeo, è di grande interesse la sentenza della Corte di giustizia dell'Unione europea (Grande Camera) nella causa C-507/17 del 24 settembre 2019, *Google* c. *Commission nationale de l'informatique et des libertés* (CNIL)[52].

La sentenza verte su una questione preliminare sollevata dal *Conseil d'État* (Consiglio di Stato francese, che agisce come Corte amministrativa suprema) con decisione del 19 luglio 2017.

La questione pregiudiziale è stata sollevata da Google contro una decisione della Presidenza del CNIL del 24 maggio 2015, che aveva accolto la richiesta di una persona fisica di rimuovere dall'elenco dei risultati ottenuti a seguito di una ricerca basata sul suo nome, i link che conducevano a una serie di pagine web, e di applicare tale rimozione a tutte le estensioni dei nomi di dominio del suo motore di ricerca[53].

A seguito di tale ingiunzione, Google ha semplicemente rimosso i link relativi a questa persona, esclusivamente dai risultati ottenuti in risposta alle ricerche effettuate da nomi di dominio corrispondenti alle estensioni del suo motore di ricerca negli Stati membri. La risposta di Google è stata considerata insufficiente dalla CNIL, che ha imposto alla società una sanzione di 100.000 euro con una decisione del 10 marzo 2016. Questa sanzione è stata impugnata da Google davanti al Consiglio di Stato francese, sostenendo che la rimozione dei link indicati nei risultati di ricerca non significava che dovessero essere rimossi, senza limitazioni geografiche, da tutti i nomi di dominio del

[47] CEDU del 28 settembre 2018, para. 89.
[48] *Ibid.*, para. 90.
[49] *Ibid.*, para. 95.
[50] *Ibid.*, para. 97.
[51] *Ibid.*, para. 116 e decisione finale.
[52] ECLI:EU:C:2019:772 (https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:62017CJ0507)
[53] *Ibid.*, para. 30.

suo motore. Inoltre, adottando tale interpretazione, il CNIL ha violato i principi di *comitas* e di non ingerenza riconosciuti dal diritto pubblico internazionale e ha violato in modo sproporzionato le libertà di espressione, informazione, comunicazione e stampa, garantite, tra l'altro, dall'articolo 11 della Carta.

Il Consiglio di Stato francese, prima di emettere una decisione definitiva, ha deciso di sospendere il procedimento e di sottoporre una questione pregiudiziale alla CGUE. Sebbene l'oggetto di questo rinvio pregiudiziale fosse incentrato sull'interpretazione da dare all'obbligo di rimozione dei link da parte del motore di ricerca, ci concentreremo sull'analisi della sentenza che è dedicata a risolvere la portata territoriale della normativa europea.

Così, per quanto riguarda l'obbligo di Google di rispettare il diritto europeo, la Corte afferma che il "trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro"[54]. In tali circostanze, "e attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività"[55]. Pertanto, il fatto che tale motore di ricerca sia gestito da un'impresa di un paese terzo non può significare che il trattamento dei dati personali effettuato sia soggetto agli obblighi e alle garanzie di cui alla direttiva 95/46 e al regolamento 2016/679[56].

Si potrebbe quindi intendere che "una deindicizzazione effettuata su tutte le versioni di un motore di ricerca è idonea a soddisfare pienamente tale obiettivo" di garantire un elevato livello di protezione dei dati personali dei cittadini dell'UE[57]. Per la Corte, sembra chiaro che in un mondo globalizzato, l'accesso degli utenti di Internet, in particolare di quelli al di fuori dell'Unione, a un link "che rinvia a informazioni concernenti una persona il cui centro di interessi si trova nell'Unione, può quindi produrre effetti immediati e sostanziali sulla persona in questione anche all'interno dell'Unione"[58].

Ciò potrebbe giustificare che il legislatore dell'UE "a prevedere un obbligo, per il gestore di un motore di ricerca, di procedere, quando accoglie una richiesta di deindicizzazione formulata da una persona siffatta, alla deindicizzazione su tutte le versioni del suo motore di ricerca"[59]. Ma "va sottolineato che molti Stati terzi non riconoscono il diritto alla deindicizzazione o comunque adottano un approccio diverso per tale diritto"[60] e va tenuto presente che "il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità", inoltre "che l'equilibrio tra il diritto al rispetto della vita privata e alla protezione dei dati personali, da un lato, e la libertà di informazione degli utenti di Internet, dall'altro, può variare notevolmente nel mondo"[61].

E, secondo la sentenza, il legislatore dell'UE non ha scelto "di attribuire ai diritti sanciti da tali disposizioni una portata che vada oltre il territorio degli Stati membri e che abbia inteso imporre a un operatore che, come Google, rientra nell'ambito di applicazione della direttiva o del regolamento suddetti, un obbligo di deindicizzazione riguardante anche le versioni nazionali del suo motore di ricerca che non corrispondono agli Stati membri"[62]. Di conseguenza, "il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente, a seguito di

[54] Ibid., para. 49. In questo paragrafo, si fa riferimento alla sentenza del 13 maggio 2014, *Google Spain SL e Google Inc.* c. *Agencia Española de Protección de Datos (AEPD) e Mario Costeja, C-131/12, EU:C:2014:317*, para. 60.
[55] *Ibid.*, para. 56.
[56] *Ibid.*, para. 51.
[57] *Ibid.*, para.. 55.
[58] *Ibid.*, para. 57.
[59] *Ibid.*, para. 58.
[60] *Ibid.*, para. 59.
[61] *Ibid.*, para. 60.
[62] *Ibid.*, para. 62.

un'ingiunzione di un'autorità di controllo o di un'autorità giudiziaria di uno Stato membro, un obbligo, derivante dal diritto dell'Unione, di effettuare tale deindicizzazione su tutte le versioni del suo motore"[63].

In breve, "che il gestore di un motore di ricerca, quando accoglie una domanda di deindicizzazione in applicazione delle suddette disposizioni, è tenuto ad effettuare tale deindicizzazione non in tutte le versioni del suo motore di ricerca, ma nelle versioni di tale motore corrispondenti a tutti gli Stati membri, e ciò, se necessario, in combinazione con misure che, tenendo nel contempo conto delle prescrizioni di legge, permettono effettivamente di 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"[64].

Tuttavia, la sentenza fa riferimento a due eccezioni. Come sottolinea E. Torralba, "non è escluso che, in virtù del bilanciamento dei diritti effettuato in base agli standard nazionali di protezione, uno Stato membro possa imporre al gestore del motore di ricerca di rimuovere i link da tutte le versioni di tale motore", poiché il GDPR "non impone, ma nemmeno vieta". In secondo luogo, "sebbene la rimozione dei link debba, in linea di principio, essere verificata in tutti gli Stati membri, l'interesse del pubblico ad accedere alle informazioni può variare da uno Stato all'altro, cosicché, proprio in virtù del bilanciamento nazionale, l'obbligo di rimuovere i link può talvolta essere limitato al territorio di uno o più Stati"[65].

In relazione a questo aspetto, è significativo che la Corte contraddica in modo molto chiaro l'opinione del Gruppo di lavoro "Articolo 29", che nelle sue linee guida sull'attuazione della sentenza della CGUE nella causa C-131/12, già citata, aveva indicato che in ogni caso la deindicizzazione dovrebbe essere efficace per tutti i domini rilevanti, compresi i ".com"[66].

Pertanto, la Corte riconosce che, accanto al modello europeo, che è più protettivo, possono coesistere modelli diversi che possono essere applicabili quando si tratta di proteggere i dati personali dei cittadini.

3.2. Nella giurisprudenza costituzionale spagnola

Sul diritto all'oblio, la Corte costituzionale spagnola ha emesso due sentenze, una nel 2018 e l'altra nel 2022, che commentiamo di seguito.

3.2.1. STC 58/2018, 4 giugno

Il primo di questi riguarda una denuncia relativa a informazioni pubblicate dal quotidiano "El País" negli anni '80 sullo smantellamento di una rete di narcotraffico che coinvolgeva il parente di un importante funzionario pubblico e altri membri dell'alta società di una determinata località. La notizia – che identificava le persone coinvolte con nome, cognome e professione – descriveva il *modus operandi* della rete, la detenzione dei partecipanti e lo stato di tossicodipendenza delle persone ricorrenti che, secondo la notizia, avevano sofferto di crisi di astinenza durante la loro permanenza in carcere.

Vent'anni dopo, nel 2007, "El País" ha creato un accesso gratuito al suo archivio digitale sul sito web "www.elpais.com". Da quel momento, quando i nomi e i cognomi dei ricorrenti venivano inseriti nel motore di ricerca Google, la notizia e un suo estratto apparivano come primo risultato.

---

[63] *Ibid.*, para. 64.
[64] *Ibid.*, para. 73.
[65] E. Torralba, *Reflexiones sobre el alcance*, cit., p. 590.
[66] Gruppo di lavoro Articolo 29, *Orientamenti sull'esecuzione della sentenza della Corte di giustizia dell'Unione europea su "Google Spain e Inc contro Agenzia spagnola per la protezione dei dati (AEPD) e Mario Costeja González*", C-131/12, WG 225 del 26 novembre 2014. In questa Guida, il Gruppo di lavoro Articolo 29 ha affermato che nonostante le soluzioni concrete possano variare a seconda dell'organizzazione interna e della struttura dei motori di ricerca, le decisioni di *delisting* devono essere attuate in modo da garantire una protezione efficace e completa di tali diritti e impedire che il diritto dell'Unione possa essere facilmente eluso. In questo senso – secondo la sentenza – limitare il *delisting* ai domini dell'UE, adducendo come motivazione che gli utenti tendono ad accedere ai motori di ricerca attraverso i loro domini nazionali, non può essere considerato un mezzo sufficiente a garantire in modo soddisfacente i diritti degli interessati. In pratica, ciò significa che, in ogni caso, il *delisting* deve essere efficace anche per tutti i domini pertinenti, compreso (para. 20).

Quando è stato presentato un reclamo al giornale per anonimizzare la storia o impedirne l'indicizzazione, il giornale ha rifiutato adducendo il diritto fondamentale alla libertà di informazione e l'impossibilità di impedire l'indicizzazione da parte dei motori di ricerca.

Gli interessati si sono rivolti al Tribunale di primo grado che, con sentenza del 4 ottobre 2012, ha accolto integralmente il ricorso, ritenendo provato che "El País" non avesse adottato meccanismi di controllo per impedire la diffusione indiscriminata della notizia. La notizia, inoltre, non era più vera perché i ricorrenti erano stati condannati in via definitiva, non per traffico di droga, ma per contrabbando e la pena era già stata scontata. Inoltre, l'interesse pubblico della notizia, essendo trascorsi oltre vent'anni e data la mancanza di rilevanza pubblica dei querelanti, era anch'esso venuto meno, e il giornale è stato pertanto condannato a pagare un risarcimento, a cessare immediatamente la diffusione della notizia e a mettere in atto misure tecnologiche adeguate per evitare che l'informazione fosse trovata qualora i nomi e cognomi dei querelanti fossero stati inseriti su Google[67].

Su ricorso del quotidiano "El País", il Tribunale provinciale di Barcellona, l'11 ottobre 2013, ha emesso una sentenza di rigetto del ricorso, ordinando anche la cessazione dell'utilizzo dei dati personali nel codice sorgente che conteneva la notizia.

In sede di ricorso in cassazione, il ricorso è stato parzialmente accolto dalla sentenza della Corte di Cassazione del 15 ottobre 2015[68]. Pertanto, la Suprema Corte non ha ritenuto che il giornale avesse violato il requisito della veridicità nella pubblicazione di quei fatti. Il problema, secondo la Camera, non era che il trattamento dei dati fosse non veritiero, ma piuttosto che fosse inadeguato allo scopo per cui i dati erano stati inizialmente raccolti e trattati. Il fattore tempo è di fondamentale importanza in questa materia, poiché il trattamento dei dati personali deve essere conforme ai principi di qualità dei dati non solo al momento della raccolta e del trattamento iniziale, ma per tutto il tempo in cui avviene il trattamento. Un trattamento che inizialmente poteva essere idoneo allo scopo che lo giustificava può, col tempo, diventare inadeguato a tale scopo, e il danno che provoca ai diritti personali, come l'onore e la privacy, sproporzionato rispetto al diritto tutelato dal trattamento dei dati[69]. Infine, ha accolto parzialmente il ricorso nel senso di dichiarare prive di valore e di effetto le decisioni relative alla cancellazione dei dati personali dei ricorrenti nel codice sorgente della pagina web contenente le informazioni e dei loro nomi, cognomi o anche iniziali, e al divieto di indicizzazione dei dati personali per l'utilizzo da parte del motore di ricerca interno dell'emeroteca digitale gestita dalla convenuta, decisioni che lasciamo senza effetto, mantenendo il resto delle decisioni della sentenza impugnata[70].

A seguito del ricorso di amparo dei ricorrenti, la Corte Costituzionale ha confermato la totalità della sentenza della Corte Suprema, ad eccezione del divieto di indicizzazione dei nomi dei ricorrenti da parte del motore di ricerca interno del giornale. Così, nella motivazione in diritto, al punto n. 8, si afferma che: "il divieto di indicizzare i dati personali, nello specifico i nomi e i cognomi dei ricorrenti, per l'utilizzo da parte del motore di ricerca interno di "El País" deve essere considerato una misura restrittiva della libertà di informazione idonea, necessaria e proporzionata al fine di impedire la diffusione di notizie lesive dei diritti invocati". Pertanto, "la misura richiesta è necessaria perché la sua adozione, e solo la sua adozione, limiterà la ricerca e la localizzazione della notizia nell'emeroteca digitale sulla base di dati personali che identificano inequivocabilmente i ricorrenti". Sicché: "va tenuto presente che i motori di ricerca interni ai siti web svolgono la funzione di consentire il reperimento e la diffusione delle notizie, e che tale funzione è garantita anche se si elimina la possibilità di effettuare la ricerca utilizzando il nome e il cognome delle persone in questione, che non hanno alcuna rilevanza pubblica". "Se la ricerca di informazioni ha uno scopo investigativo lontano dal mero interesse giornalistico per la persona 'indagata'", sarà sempre possibile localizzare la notizia "attraverso una ricerca tematica, temporale, geografica o di qualsiasi altro tipo". Per la Corte Costituzionale, "una persona che fa parte di quello che la Corte Suprema chiama nella sua sentenza 'il pubblico più attivo' può accedere alle notizie in molteplici modi, se è motivata dall'interesse pubblico che l'informazione può avere in un determinato contesto". Tuttavia, "la disposizione richiesta dai ricorrenti impedisce il monitoraggio *ad*

[67] *STC 58/2018*, 4 giugno,

[68] Camera Civile, *STS 4132/2015*, 15 ottobre. Un'analisi di questa sentenza della Corte Suprema si trova in A. Chicharro, *Medios de comunicación digital y derecho al olvido en la Unión Europea*, in J. Herrero, M. Trenta, (coord.) *El fin de un modelo de política*, in *La Laguna, Cuadernos Artesanos de Comunicación*, 140/2017, pp. 1470-1473.

[69] Base giuridica, Parágrafo 6.

[70] Sentenza *STS 4132/2015*, para. 2.

personam del passato di un determinato soggetto, insistiamo, senza alcuna proiezione pubblica, attraverso uno strumento la cui finalità è diversa, ed è volta ad assicurare la formazione di un'opinione pubblica plurale, non a soddisfare curiosità individuali e mirate"[71].

3.2.2. STC 23/2022, del 21 febbraio

Più di recente, la sentenza della Corte costituzionale 23/2022 del 21 febbraio ha respinto la richiesta di un ricorrente che chiedeva l'annullamento di una sanzione imposta dalla Commissione nazionale per il mercato dei valori mobiliari, pubblicata nella Gazzetta ufficiale dello Stato, in quanto contraria al principio di proporzionalità delle sanzioni e al diritto fondamentale alla protezione dei dati personali.

A prescindere da tutte le questioni relative alla sanzione, la presunta violazione del diritto alla protezione dei dati personali deriva dalla pubblicazione nel BOE del nome completo del ricorrente e del tipo e della natura della violazione, come previsto all'epoca dall'articolo 275.3 del Regio Decreto Legislativo 4/2015 che approva il Testo Unico della Legge sul mercato mobiliare.

Secondo il parere della Corte, il rinvio da parte della CNMV al BOE della decisione di "pubblicare la sanzione per un'infrazione molto grave inflitta al ricorrente... è effettuato per adempiere a finalità direttamente connesse alle legittime funzioni degli enti cedente e cessionario ed è espressamente autorizzato dalla legge (art. 304 TRLMV), e pertanto non richiede il consenso dell'interessato [art. 11, par. 2, lett. a), LOPD]"[72]. Questa misura risponde a una finalità costituzionale legittima, adeguata, necessaria e proporzionata, in quanto ha "lo scopo primario di assicurare la trasparenza dei mercati mobiliari, la corretta formazione dei prezzi su di essi e la tutela degli investitori", che risponde anche a un interesse generale dell'intera Unione Europea, come evidenziato dal Regolamento UE sugli abusi di mercato[73]. Inoltre, tenendo conto che i documenti pubblicati nel BOE hanno lo status di inalterabili, gli interessati possono "esercitare il diritto di chiedere ai motori di ricerca su Internet di rimuovere dagli elenchi di risultati ottenuti, a seguito di una ricerca basata sul loro nome, i link pubblicati contenenti informazioni che li riguardano una volta che non sono più necessari o pertinenti, tenendo conto delle finalità per cui i dati personali sono stati trattati, del tempo trascorso dalla pubblicazione e della natura e dell'interesse pubblico delle informazioni"[74].

In sintesi, esiste quindi "una base giuridica che legittima il trattamento dei dati, sia la comunicazione della decisione che impone una sanzione all'organo che pubblica il "BOE", sia la sua successiva pubblicazione nel BOE". Una pubblicazione che, inoltre, "non viola i principi di proporzionalità e temporalità che regolano la protezione dei dati personali". E "la misura prevista dal legislatore nell'art. 304 TRLMV e la sua applicazione da parte della CNMV non possono essere considerate sproporzionate per il raggiungimento di tale scopo". Non risulta neppure che "sia stato violato il principio di temporalità nel trattamento dei dati personali che compaiono nella delibera sanzionatoria pubblicata in via definitiva sul "BOE", in quanto il titolare può esercitare il diritto alla soppressione e all'oblio al momento opportuno"[75].

4. Conclusioni

Appare chiaro, dopo le pagine precedenti, che in Europa si sta radicando una vera e propria cultura della protezione dei dati e un consolidamento nella giurisprudenza delle principali linee normative che l'Unione Europea ha promosso.

[71] *STC 58/2018*, del 4 giugno. F.J. 8.
[72] *STC 23/2022*, del 21 febbraio, F.J. 3 C).
[73] Parlamento Europeo e Consiglio, *Regolamento (UE) N. 596/2014 del 16 aprile 2014 relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione*.
[74] *STC 23/2022*, 21 febbraio, F.J. 3.
[75] *STC 23/2022*, del 21 febbraio, F.J. 4.

Come si legge nel considerando 2 del Regolamento, l'obiettivo di "contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche", attraverso una normativa in cui il trattamento dei dati personali deve essere "al servizio dell'uomo" (considerando 4), sembra essere una realtà sempre più palpabile.

L'obiettivo è stabilire norme che "rispettino tutti i diritti fondamentali e osservino le libertà e i principi riconosciuti dalla Carta e sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e di informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale e la diversità culturale, religiosa e linguistica" (considerando 4).

Tuttavia, per quanto i legislatori dell'UE possano avere buone intenzioni, sono anche soggetti a limiti, come è stato sottolineato dalla CGUE. Pertanto, le autorità di controllo europee e degli Stati membri dell'UE non possono aspirare a un'applicazione universale della propria legislazione. Accanto al modello europeo, possono coesistere altri modelli di protezione dei dati.

Inoltre, in un'economia sempre più basata sul trattamento dei dati, compresi quelli personali, e in una società globale, sembra essenziale che le persone abbiano un maggiore controllo sui propri dati personali e che questi vengano trattati per scopi legittimi, in modo lecito, equo e trasparente e nel rispetto dei diritti umani.

In ogni caso, al di là di circostanze eccezionali come l'epidemia di COVID-19, che ha messo in discussione molte delle disposizioni giuridiche dell'Unione Europea sotto molteplici aspetti, comprese quelle sulla protezione dei dati – che richiederebbero una trattazione più dettagliata –, la normativa europea presenta anche alcuni punti deboli[76].

Quello che consideriamo il principale è che l'efficacia del diritto all'oblio è lasciata alla discrezione di società private, la maggior parte delle quali ha sede negli Stati Uniti, e con un certo livello di resistenza al controllo. In effetti, i motori di ricerca Google, Bing e Yahoo hanno predisposto dei moduli online per consentire ai cittadini di richiedere che i loro dati personali non vengano proposti nei risultati delle ricerche. Ma non sono gli unici motori di ricerca disponibili su Internet[77]. Inoltre, la natura dei dati richiesti e la necessità di fornire una documentazione che ne garantisca la veridicità, conferiscono a queste aziende una posizione di forza le cui conseguenze future potrebbero essere molto preoccupanti.

Al momento, con l'attuale guerra di invasione dell'Ucraina da parte della Federazione Russa, la cui fine è ancora lontana, le normative dell'Unione Europea incontreranno nuove resistenze al loro rispetto al di fuori dei confini strettamente comunitari[78]. In effetti, il motore di ricerca russo per eccellenza, Yandex, per ora è ancora accessibile, ma non sappiamo come potrà evolvere in futuro. In ogni caso, per il momento non è disponibile alcun modulo per esercitare il diritto di cancellazione sul suo motore di ricerca[79].

Infatti, come ha giustamente sottolineato Alice Pease, "sebbene i motori di ricerca operino sotto la supervisione delle autorità nazionali per la protezione dei dati, in pratica l'azienda ha spesso l'ultima parola sull'opportunità di scollegare o meno le informazioni dal nome di un individuo, senza alcuna responsabilità o controllo pubblico". Per l'autore, infatti, "la valutazione dei diritti alla privacy e della

---

[76] Un'analisi più dettagliata è stata discussa qualche tempo fa in R. M. Orza Linares, *La regulación del "derecho al olvido" en la Unión Europea. Aspectos críticos*, in F.J. Durán Ruíz (dir.), *Desafíos de la protección de minores en la sociedad digital. Internet, redes sociales y comunicación*, Valencia, 2018, pp. 125-160.

[77] Sebbene questi siano i più utilizzati, altri motori di ricerca includono "Baidu.com" – il più usato in Cina –, "Yandex.ru" – il più usato in Russia –, "Naver.com" – il più usato in Corea del Sud –, "DuckDuckGo.com", "Archive.org", "Ask.com", "Ecosia.com!, "Qwant.com", ecc.

[78] Recentemente, la Federazione Russa ha approvato un "Piano di azioni prioritarie per garantire lo sviluppo dell'economia russa in condizioni di pressione da parte delle sanzioni esterne", secondo quanto riferito dal Ministero dello Sviluppo Economico russo, che include, tra le altre misure, la "Cancellazione della responsabilità per l'uso di software (SW) senza licenza nella Federazione Russa, di proprietà di un detentore di copyright proveniente da Paesi che hanno sostenuto le sanzioni".

[79] Non va dimenticato che il motore di ricerca Yandex ha il suo sito principale in Russia (www.yandex.ru), anche se al momento della stesura di questo articolo è operativo almeno anche su www.yandex.eu e www.yandex.com. D'altra parte, Yandex è il motore di ricerca più popolare in Russia, addirittura davanti a Google.ru, essendo il quarto motore di ricerca più utilizzato al mondo, secondo NetMarketShare, con dati del settembre 2021.

libertà di informazione non è un compito facile" e "richiedere a un'azienda a scopo di lucro di intraprendere la valutazione dei valori legali ed etici è per molti versi problematico"[80]. Questo ci costringe a ridefinire sostanzialmente il ruolo di tali motori di ricerca, da "mero intermediario" nella comunicazione al di fuori delle norme sulla protezione dei dati, a "ruolo attivo nel garantire il controllo delle persone sui loro diritti digitali"[81] e a soppesare gli interessi contrastanti in ogni caso.

Inoltre, va notato che la richiesta non dovrebbe essere ammissibile in tutti i casi. Secondo le linee guida dell'Agenzia spagnola per la protezione dei dati, dovrebbe essere accolta solo quando:
a) c'è un motivo legittimo e fondato;
b) che il suddetto motivo si riferiva a alla sua specifica situazione personale;
c) che il motivo invocato giustifica il diritto di opposizione richiesto;
d) che, nel caso di informazioni di rilevanza pubblica, i dati sono imprecisi obsoleti[82] .

Google, nella sezione "Privacy e termini" alla voce "Domande frequenti", afferma che, in relazione al diritto all'oblio, dopo la presentazione della richiesta, "ogni richiesta deve essere valutata individualmente e i diritti dell'individuo di controllare i propri dati personali devono essere soppesati con il diritto del pubblico di conoscere e distribuire le informazioni". E nel valutarla, i criteri utilizzati per accettarla o rifiutarla saranno "se i risultati includono informazioni obsolete sulla vostra vita privata, così come se c'è un interesse pubblico nel fatto che le informazioni rimangano nei risultati di ricerca di Google (ad esempio se si riferiscono a truffe finanziarie, negligenza professionale, condanne o altri reati), negligenza professionale, condanne penali o la vostra condotta in qualità di pubblici ufficiali, eletti o nominati)" e in ogni caso, trattandosi di "decisioni difficili" e di una "organizzazione privata", potrebbero non essere nella "posizione giusta" per valutare il caso. Pertanto, "se non siete d'accordo con la nostra decisione, potete contattare l'autorità locale per la protezione dei dati".

Più estesamente, nel suo documento "Come bilanciare il diritto all'oblio di un individuo con il diritto del pubblico all'informazione?", il Consiglio consultivo distingue tre categorie o ruoli in base alla rilevanza sociale dell'individuo:

Nel primo gruppo troviamo figure pubbliche come politici, leader religiosi, amministratori delegati e grandi uomini d'affari, personalità della cultura o dello sport. In questi casi, le richieste più alte saranno fatte al momento di valutare l'eventuale rimozione di un link.

Un criterio meno rigido è previsto per i privati cittadini e il terzo gruppo comprende le persone con un "ruolo pubblico in un contesto specifico o limitato". Questa categoria comprende i dipendenti pubblici o chiunque abbia un ruolo sociale nella propria professione orientato verso una particolare comunità. Un gruppo che rientra in un criterio intermedio e in cui la decisione di rimuovere o meno un link dipenderà dalle informazioni specifiche.

Per quanto riguarda il tipo di informazioni, si afferma che sarà più favorevole soddisfare la richiesta quando si tratta di informazioni personali (salute, vita sessuale, ecc.). Il rapporto afferma chiaramente che non devono essere soppressi i risultati relativi a dichiarazioni di politici o leader religiosi, articoli di opinione su dibattiti rilevanti, informazioni di attualità che non compromettono i diritti fondamentali di alcun individuo o informazioni relative a questioni generali di salute o di consumo.

Il link deve essere rimosso in caso di richiesta di informazioni sensibili da parte di governi, aziende o privati (documenti di identità, indirizzi personali, password, ecc.). Sarà rimosso anche quando le informazioni pubblicate o diffuse sono false.

Pertanto, i criteri di base che Google dovrà prendere in considerazione saranno i seguenti:
a) se l'interessato è una persona pubblica o meno;
b) la natura stessa delle informazioni da deindicizzare;

---

[80] A. Pease, *Il "diritto all'oblio": affermare il controllo sulla nostra identità digitale o riscrivere la storia?*, in *IRPPS Working Papes,*, 8/2015, p. 9.
[81] *Ibid*., p. 8.
[82] Il Comitato europeo per la protezione dei dati ha pubblicato nel 2019 le *Linee guida 5/2019 sui criteri per il diritto all'oblio nei casi di motori di ricerca ai sensi del GDPR*. Tali linee guida hanno aggiornato le raccomandazioni del Gruppo di lavoro articolo 29 adottate nel 2014, a seguito della sentenza della CGUE nella causa C-131/12 "Google Spain, v. AEPD e Mario Costeja", cit.

c) l'entità della fonte originale che pubblica le informazioni;
d) il tempo trascorso dalla pubblicazione.

Non si può fare a meno di sottolineare che con le domande presentate ai motori di ricerca, queste società private potrebbero costruire una grande banca dati – la cui veridicità è accreditata dagli stessi interessati – e il cui sfruttamento potrebbe essere molto redditizio per loro in futuro. Se la possibilità di realizzare applicazioni redditizie per l'analisi di dati massivi, utilizzando in misura maggiore o minore l'intelligenza artificiale (*big data*), è già importante, è perfettamente immaginabile quanto queste aziende possano essere redditizie per i dati che i cittadini offrono loro volontariamente e che godono di un altissimo grado di veridicità.

Per avere un'idea dell'importanza delle informazioni personali che stiamo offrendo a Google, possiamo considerare il numero di richieste presentate finora in relazione alla cancellazione dei dati personali. In particolare, dal 29 maggio 2014 al 18 maggio 2022, sono state presentate 1.274.387 richieste di rimozione o mascheramento di 4.970.215 pagine web. Di queste richieste, il 49,0% è stato accettato e il 51,0% è stato rifiutato. In particolare, la Spagna ha ricevuto 112.454 richieste, che hanno portato all'analisi di 376.783 pagine. Di queste, solo il 39,9% è stato accettato, mentre il 60,1% è stato rifiutato.

Infine, sebbene non vi siano dubbi sugli sforzi, sia legislativi che giurisprudenziali, compiuti nell'Unione europea per difendere la privacy e controllare i dati personali dei cittadini, non solo le minacce non stanno scomparendo, ma ne stanno emergendo di nuove. Infatti, insieme all'indiscutibile avanzata dei *big data* e dell'intelligenza artificiale, i gravi conflitti che si stanno attualmente svolgendo in Europa pongono minacce significative alla privacy e alla libertà dei cittadini e ci obbligano a essere vigili, affinché possano continuare a essere efficaci e validi.

Abstract

Il contributo presenta una rassegna di alcuni dei più importanti testi giuridici e giurisprudenziali europei sul diritto all'oblio, dopo l'entrata in vigore del Regolamento UE sulla protezione dei dati. La rilevanza di questo diritto risiede nel fatto che è uno dei pochi strumenti a disposizione dei cittadini per controllare l'uso dei propri dati su Internet.

Parole chiave: diritto all'oblio, privacy, GDPR

*

The paper presents a review of some of the most relevant European legal and jurisprudential texts on the right to be forgotten, following the entry into force of the EU Data Protection Regulation. The importance of this right lies in the fact that it is one of the few tools available to citizens to control the use of their data on the Internet.

Key words: right to be forgotten, privacy, GDPR