ISSN 2384-9169
Fascicolo n. 3 - 2020
rivista.eurojus.it

La tutela dei dati personali e la portata territoriale dell'obbligo di deindicizzazione dei contenuti online.

DI ANGELA CORRERA*

Sommario: 1. Premessa. – 2. La portata territoriale e sostanziale del diritto all'oblio da *Google Spain* ad oggi. – 3. Il problema dell'estensione degli obblighi di rimozione dei contenuti illeciti dal *web*. – 4. Alcune considerazioni a margine dei recenti arresti della Corte di giustizia.

1. Premessa.

Le nuove forme della raccolta e del trattamento dei dati personali e la pervasività del controllo operato su di essi da parte di soggetti pubblici e privati hanno progressivamente moltiplicato l'esigenza di tutela, nella consapevolezza di non poter circoscrivere le relative problematiche nel quadro giuridico tradizionale di riferimento, divenuto inadeguato a contenere il carattere immateriale della realtà del *Web*.

In tale contesto, caratterizzato da un inarrestabile dinamismo e da un'incessante mutevolezza, la categoria dei diritti è stata proiettata in uno spazio nuovo e inesplorato, i cui confini si disperdono sfumando in un vero e proprio "villaggio globale"[1].

Invero, le difficoltà della progettazione politica e le lungaggini dei processi normativi hanno fatto sì che l'esperienza giuridica non rimanesse immune dalle tensioni provocate dalla rivoluzione digitale.

* Dottoranda di ricerca in Diritto dell'Unione europea – Università di Napoli 'Parthenope'.

[1] Così, N. BOBBIO, *L'età dei diritti,* Einaudi, Torino, 1990; S. RODOTÀ, *Apologia dei diritti*, disponibile online at: *http://it.scribd.com/doc/53206551/Apologia-dei-diritti-Stefano-Rodota-I-diritti-dell-uomo-oggi-Norberto-Bobbio*.

Sulla base delle pronunce rese nelle cause C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL),* e C-18/18*, Eva Glawischnig-Piesczek c. Facebook*, che, nello scorso anno, hanno interessato due giganti del Web, *Google e Facebook*[2], definendo ulteriormente i contorni del diritto all'oblio e la portata degli obblighi gravanti sugli *hosting providers*, il presente lavoro intende evidenziare il ruolo svolto dalla Corte di giustizia[3] per superare il disorientamento giuridico derivato dallo sviluppo di *Internet* e delle strutture ad esso connesse; nonché l'impatto di tali decisioni sulla legislazione UE e sugli equilibri tra gli attori coinvolti nella protezione della *privacy*[4].

Va subito ricordato che il regolamento europeo n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali (*General Data Protection Regulation*, individuato anche con l'acronimo «GDPR»)[5], costituisce una tappa fondamentale del percorso evolutivo che ha interessato i concetti di *data protection* e di *privacy* e in cui la Corte Ue ha assunto un ruolo di anticipazione politica delle scelte successivamente accolte in concreto dal legislatore europeo[6]. A dimostrazione di ciò, basti ricordare le pronunce che, negli anni immediatamente precedenti l'entrata in vigore del GDPR, hanno contribuito a disegnare un quadro normativo uniforme in materia di *data protection*[7] e a riformulare le categorie tradizionali della dignità della persona e dell'autodeterminazione individuale, messe in discussione dalle nuove sfide della realtà sociale.

---

[2] Corte giust. 24 settembre 2019, causa C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:772; 3 ottobre 2019, causa C-18/18*, Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, ECLI:EU:C:2019:821.

[3] Cfr. G. TESAURO, *Manuale di diritto dell'Unione europea* (a cura di) P. DE PASQUALE e F. FERRARO, Napoli, 2019, p. 108 ss.; M. CONDINANZI, R. MASTROIANNI, *Il contenzioso dell'Unione Europea*, Torino, 2009.

[4] Sul tema, v. M. PUGLIA, *La protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'UE*, in AA.VV. (a cura di), *Liber amicorum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, Torino, 2018, p. 788; F. ROSSI DAL POZZO*, La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *Annali AISDUE*, Vol. I, Bari, 2020, p. 71 ss.

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, in *GUUE* del 4.05.2016, L119/1. Per un primo commento, v. M. BOTTINO, *Approvato il nuovo regolamento generale per la protezione dei dati personali nell'UE*, in *Eurojus,* 26 aprile 2016.

[6] Per approfondimenti sulla giurisprudenza evolutiva della Corte di giustizia in materia di dati personali*, ex multis* v. G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, p. 9; F. BALDUCCI ROMANO, *Il diritto alla protezione dei dati personali nella giurisprudenza della Corte di giustizia,* in *Rivista italiana di diritto pubblico comunitario*, 2015, p. 1619.

[7] Corte giust. 8 aprile 2014, cause riunite C-293/12 e C-594/12*, Digital Rights Ireland e Seitlinger e a.,* ECLI:EU:C:2014:238;13 maggio 2014, causa C-131/12, *Google Spain, Google Inc. e Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* ECLI:EU:C:2014:317; 17 luglio 2014, cause riunite C-141/12 e C-372/12, *Y.S. e a*., ECLI:EU:C:2014:2081; 2 ottobre 2014, causa C-127/13, *Strack c.Commissione,* ECLI:EU:C:2014:2250; 11 dicembre 2014, causa C-212/13, *Ryneš,* ECLI:EU:C:2014:2428; 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a*., ECLI:EU:C:2015:238; 16 luglio 2015, causa C-615/13 P, *ClientEarth e PAN Europe/EFSA,* ECLI:EU:C:2015:489; 16 luglio 2015, causa C-580/13, *Coty Germany,* ECLI:EU:C:2015:485; 1 ottobre 2015, causa C-201/14*, Bara e a.,* ECLI:EU:C:2015:638; 1 ottobre 2015, causa C-230/14, *Weltimmo,* ECLI:EU:C:2015:639; 6 ottobre 2015, causa C-362/14, *Schrems,* ECLI:EU:C:2015:650. Sembra, inoltre, opportuno ricordare alcune pronunce successive al biennio esaminato, ma che si pongono in continuità con esse: Corte giust. 21 dicembre 2016, causa C-203/15, *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.,* ECLI:EU:C:2016:970; 26 luglio 2017, Parere 1/15 *sul progetto di Accordo PNR UE/Canada,* ECLI:EU:C:2017:592.

Com'è noto, il diritto alla protezione dei dati personali trova ormai espressa enunciazione all'art. 16 del TFUE[8] e all'art. 8 della Carta dei diritti fondamentali dell'Unione europea[9], come diritto autonomo rispetto alla *privacy*, tutelato all'art. 7 della medesima Carta. Il riconoscimento di quest'ultima come fonte vincolante di rango primario ai sensi dell'art. 6 TUE ha peraltro contribuito a rendere effettiva la tutela dei diritti in esame[10]. Preme evidenziare che la tutela è declinata all'interno della Carta in due diverse disposizioni che fotografano l'aspetto negativo e quello positivo del diritto, rispettivamente, alla *privacy* e alla protezione dei dati personali. Difatti, muovendo dall'ampia nozione di "dato personale" deve ritenersi che il diritto alla protezione dei dati personali si configuri quale prerogativa del soggetto di "controllare" tutte le informazioni che a lui si riferiscono e che, in quanto tali, costituiscono la sua proiezione e il suo essere nella società dell'informazione.

In tal senso, il diritto alla protezione dei dati personali, diversamente dal diritto alla riservatezza, che trova la sua essenza nella libertà "negativa" di non subire interferenze nella propria vita privata, rappresenta il fondamento della libertà "positiva" di esercitare un controllo sul flusso di informazioni e di dati che al soggetto si riferiscono[11]. Si tratta, a ben riflettere, della manifestazione più pregnante del *right to be let alone*, derivato dal passaggio del modello di tutela statica e negativa della riservatezza - che, costruita sul prototipo della proprietà privata, si esaurisce nell'esclusione delle ingerenze altrui nella protezione dei dati personali - ad un modello di tutela dinamica, fatta di regole rigorose da cui discendono, non solo le modalità del

---

[8] V. il commento di B. CORTESE, *Art. 16*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 444.

[9] Per un approfondimento, v. F. PICOD, S. VAN DROOGHENBROECK, *Charte des droits fondamentaux de l'Union européenne: Commentaire article par article*, Bruxelles, 2018; O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdfUE*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di)*, Carta dei diritti fondamentali dell'Unione europea*, 2017, p. 132; F. DONATI, *Protezione dei dati personali*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea,* Bologna, 2001, p. 83; J. RIDEAU, *Droit institutionnel de l'Union et des Communauteés européenne*, Parigi, 2006, p. 349; G. GONZÀLEZ FUSTER e R. GELLER, *The fundamental right of data protection in the European Union: in search of an uncharted right, in International Review of Law Computers and Technology*, n. 1, vol. 26, 2012, p. 73; J. VEDSTED-HANSEN*, Commentary on Article 7* e di H. KRANENBORG, *Commentary on Article 8*, entrambi in S. PEERS-T. HERVEY-J. KENNER-A. WARD (a cura di), *The EU Charter of Fundamental Rights – A Commentary*, Oxford, 2014, rispettivamente 153 ss. e 223 ss..

[10] V. B. NASCIMBENE, *Quale strumento giuridico per la Carta dei diritti fondamentali dell'Unione europea?*, in *Giur. It.,* 2001, p. 659 ss.; L.S. ROSSI (a cura di), *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, Milano 2002; G. STROZZI, J. RIDEAU, *La protection des droits fondamentaux dans l'Union européenne. Perspectives ouvertes par le Traité de Lisbonne*, in *Rev. aff. eur*., 2007, p. 185 ss.; I. PINGEL*, Les références a la Charte des droits fondamentaux dans le Traité établissant une Union européenne: Mélanges en l'honneur du professeur Philippe Manin*, Paris, 2010, p. 795 ss.; F. BESTAGNO, *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia, in Diritti umani e diritto internazionale*, 2015, p. 259 ss. e ID., *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Il Diritto dell'Unione europea*, 2015, p. 21; A. VON BOGDANDY*, Comunità di diritti fondamentali come meta dell'integrazione? I diritti fondamentali e la natura dell'Unione europea,* in *Dir. pubbl*., 2001, 1, 849 ss.; S. MANGIAMELI, *La Carta dei diritti fondamentali dell'Unione europea*, in *DPCE*, 2001, 1, 173 ss.

[11] Cfr. J. KOKOTTE e C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law,* ottobre 2013.

trattamento, ma anche quelle di conferimento dei poteri di controllo e di intervento alla persona interessata e alle preposte autorità di vigilanza[12].

Infine, non può tacersi che la materia è stata oggetto anche di un'ampia regolamentazione secondaria da parte dell'Unione[13]. Difatti, a partire dal 2012, a fronte di una più pressante invadenza degli strumenti tecnologici di comunicazione e del fenomeno della "globalizzazione", il processo di consolidamento della protezione dei dati personali è stato interessato da una intensa attività della Commissione. In particolare, la forte disomogeneità nella tutela di dati personali ha indotto le istituzioni europee a ricercare misure di armonizzazione più intensa delle normative nazionali che garantissero in tutto il territorio dell'Unione un elevato livello di tutela. A questa esigenza rispondono l'adozione del citato GDPR e della direttiva (UE) 2016/680[14] e la più recente proposta del regolamento *e-Privacy*[15]. Su questo punto, si ricorda che il *considerando* 9 del GDPR afferma espressamente che, sebbene i principi e gli obiettivi della direttiva 95/46/CE siano ancora oggi validi, ciò «non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni *online* comportino rischi per la protezione delle persone fisiche». Pertanto, il passaggio dallo strumento della "direttiva" a quello del "regolamento" risponde chiaramente all'esigenza di garantire un'applicazione uniforme della disciplina a tutela dei dati personali in tutto il territorio dell'Unione, evitando effetti distorsivi e dannosi sul mercato unico.

Alla luce del complesso apparato normativo che è derivato nella materia in esame, l'apporto della CGUE continua ad essere fondamentale per fare chiarezza sulla portata della normativa *data protection*, fondata sul crescente coinvolgimento della persona nella gestione della propria sfera individuale. Sulla scia delle pronunce sopra richiamate, gli arresti più recenti in materia di diritto all'oblio e di obblighi gravanti su un *hosting provider* assumono una portata

---

[12] Cfr. S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2012, p. 397; O. POLLICINO e M. BASSINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, p. 185-228.

[13] Cfr. 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, in *GUUE* del 23.11.1995, L281 p. 31-50; Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (Testo rilevante ai fini del SEE), in *GUUE* del 18.12.2009, L337, p. 11-36. Inoltre, il progetto di regolamento *e-Privacy*, su cui v. COM/2017/010 final - 2017/03 (COD), Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche); Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, in *GUUE* del 13.04.2006, L105 p. 54-63.

[14] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 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, in *GUUE* del 4.05.2016, L119, p. 89-131.

[15] Il nuovo regolamento sarà *lex specialis* nell'ambito del regolamento generale sulla protezione dei dati e disciplinerà la materia dei dati afferenti alle comunicazioni elettroniche aventi carattere di dati personali.

assai significativa, in quanto esemplificano in modo emblematico l'intimo legame che esiste tra l'evoluzione delle tecnologie e i concetti di *privacy* e di *data protection*, dalle origini alle più recenti declinazioni, che è al centro della recente consultazione pubblica avviata dalla Commissione europea sul pacchetto relativo alla legge sui servizi digitali[16].

2. La portata territoriale e sostanziale del diritto all'oblio da *Google Spain* ad oggi.

In questa ottica, con lo sviluppo delle più complesse strutture tecnologiche connesse all'uso di Internet è sorta l'esigenza di trovare un necessario punto di equilibrio tra i vantaggi conseguenti all'accesso alla Rete e la tutela dei dati che attraverso i suoi canali digitali vengono veicolati[17].

Vale la pena osservare che nel convincimento che il *Web* costituisca un ambiente intrinsecamente democratico, le persone diffondono informazioni personali, sottovalutando o, addirittura, ignorando le insidie nascoste dietro uno spazio di espressione, solo apparentemente, aperto. In effetti, nel rapporto tra gli utenti delle piattaforme *online* (in specie*, Google, Facebook, Instagram* e la diffusissima *Tik Tok*) prevale una imprudente leggerezza nel condividere molteplici informazioni (anche personali), senza considerare che, una volta *postate*, si trasformano per gli operatori del mondo digitale in uno strumento di ricchezza clamoroso[18].

A tanto si aggiunga, su un fronte parallelo, che la trasformazione dei tradizionali archivi degli organi di informazione in strumenti digitalizzati e indicizzati[19], ha determinato la sovraesposizione pubblica dell'immagine, della reputazione e della stessa identità delle persone.

Questi ultimi aspetti hanno da tempo richiamato l'attenzione della Corte di giustizia che, a partire dalla nota sentenza *Google Spain*[20], ha affermato l'esistenza del diritto all'oblio, de-

---

[16] Cfr. COM(2020) 67 final, 19 febbraio 2020, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al comitato economico e sociale europeo e al Comitato delle Regioni*, "Plasmare il futuro digitale dell'Europa".*

[17] Sulla necessità di trovare un necessario punto di equilibrio tra diritti fondamentali nella conservazione e nell'accesso ai dati di traffico delle comunicazioni da parte delle autorità pubbliche, v. G. CAGGIANO*, Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione,* in *Medialaws,* n. 2, 2018, p. 64.

[18] L'utente/consumatore è assai spesso inconsapevole del reale valore della cessione dei dati personali sul web, né sembra avvedersi di quali dati, volontariamente, ma non scientemente, fornisce durante la navigazione in Rete. Sul punto, v. Corte giust. 20 luglio 2019, causa C-40/17 - *Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW e V,* ECLI:EU:C:2019:629, in cui una società che commercializza articoli di moda online, ha inserito nel proprio sito un *plugin*, il pulsante "LIKE" di Facebook, attraverso il quale le informazioni degli utenti del sito medesimo vengono trasferite, automaticamente e in assenza del previo consenso, al social network per finalità commerciali. Cfr. C. SCHEPISI, *Comunicazione, nuove tecnologie e tutela dei consumatori. L'evoluzione del diritto dell'Unione europea*, in *Mercato e consumatori*, Ed. speciale, 2019, p. 47 ss.

[19] Cfr. A. L. VALVO, *Il diritto all'oblio nell'epoca dell'informazione "digitale",* in *Studi sull'integrazione europea*, X, 2015, p. 347-357.

[20] La pronuncia ha assunto una portata dirompente nel panorama europeo ed è stata oggetto di ampio dibattito dottrinale. Per un approfondimento, v. C. KUNER, *The Court of Justice of EU's Judgment on the "Right to be forgotten": An International perspective*, in *Ejil: Talk*!, 20 maggio 2014; F. BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Dir. Un. Eur.*, 2015, p. 21 ss.; O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi*, 24 novembre 2014; i numerosi contributi in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, RomaTrE-Press, 2015; D. MINIUSSI, *Il "diritto all'oblio": i paradossi del caso Google*, in *Rivista italiana di diritto pubblico comunitario*, 2015, n. 1, p. 209-234; H. KRANENBORG, *Google and the Right to be Forgotten*, in *European Data*

clinandolo come diritto dell'interessato ad ottenere la rimozione dal *web* di informazioni personali, quando non siano più rilevanti in ragione del lasso di tempo trascorso dal fatto che ne costituisce l'oggetto.

Come era già stato ben evidenziato prima del *dictum* della Corte, le criticità connesse alla perenne ed immediata disponibilità di informazioni sul *web* non riguardano tanto gli eventuali effetti diffamatori di quelle notizie, disciplinati *aliunde*, né la pubblicazione in sé dei dati, che ben potrebbe essere legittima e veritiera, quanto la loro persistente accessibilità[21]. In tal senso, il tema della protezione del diritto all'oblio assume caratteri peculiari rispetto alla mera divulgazione di notizie di interesse pubblico che, a distanza di tempo, inevitabilmente smarriscono tale carattere, rendendo ingiustificata la loro perdurante reperibilità.

Diversamente dalla direttiva 95/46/CE, che agli artt. 12 e 14 disciplinava l'accesso ai dati e l'opposizione al trattamento dei dati personali dai quali, in *Google Spain,* la Corte ha "dedotto" l'esistenza del diritto all'oblio, l'attuale GDPR all'art. 17 rende esplicita la tutela del diritto alla cancellazione. Tuttavia, occorre rilevare che il legislatore europeo, senz'altro condizionato dall'elaborazione giurisprudenziale sviluppatasi a partire dalla pronuncia da ultimo richiamata, si è semplicemente limitato a recepire[22] i principi di diritto, così come delineati dalla Corte Ue, a livello di diritto positivo.

Difatti, ripercorrendo brevemente i punti chiave della nota sentenza del 2014, è evidente che la Corte di giustizia, nella consapevolezza della portata globale delle problematiche sottese, ha voluto affermare l'esistenza di un vero e proprio modello europeo di protezione della *privacy*, stabilendo che la normativa dell'Unione sui dati personali si applica anche nel caso in cui i titolari del trattamento siano soggetti non europei e i dati medesimi vengano trattati prevalentemente fuori dal territorio UE[23] e che la relativa richiesta deve essere rivolta dall'interessato direttamente al motore di ricerca, in quanto «responsabile del trattamento».

A ben riflettere, il punto d'arrivo di tale decisione è, in astratto, condivisibile: non v'è dubbio che i diritti della personalità sanciti dagli artt. 7 e 8 della Carta, prevalgano sugli interessi economici degli operatori e, in generale, sull'interesse del pubblico ad accedere a specifiche informazioni[24]. Coerentemente con tale assunto, nel bilanciamento tra diritti, quelli alla *privacy*

Protection Law Review, 2015, n. 1, p. 70-79; F. FONTANELLI, *The Mythology of Proportionality in Judgments of the Court of Justice of the European Union on Internet and Fundamental Rights*, in *Oxford Journal of Legal Studies*, 2016, n. 3, p. 630-660; H. KRANENBORG, *Google and the Right to Be Forgotten*, in *EDPL*, n. 1/2015.

[21] Cfr. A. ROVROY, "*Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data,* Council of Europe, Directorate General of Human Rights and Rule of Law, vol. T-PD-BUR (2015)09REV, 2016.

[22] Per un recente contributo sul GDPR, tra gli altri, v. C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *Federalismi*, 3 luglio 2019.

[23] Sotto questo profilo, la Corte ha accolto una concezione flessibile di «stabilimento», sottolineando come l'art. 4 della direttiva 95/46/CE non esige che il trattamento dei dati debba essere effettuato dallo stesso stabilimento, ma è sufficiente che sia svolto nel contesto delle attività di quest'ultimo. In senso conforme, v. sentenza *Weltimmo, cit.* Per un approfondimento, v. G. CAGGIANO, *L'interpretazione del criterio di collegamento del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali*, in *Il diritto all'oblio dopo la sentenza Google Spain,* Roma, 2015, p. 43 ss.

[24] v. Corte giust., 9 novembre 2010, cause riunite C - 92/09 e C - 93/09, *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93 / 09), ECLI: EU: C: 2010: 662, con cui la Corte Ue ha statuito che gli artt. 42, punto 8 ter, e 44 bis del regolamento (CE) del Consiglio 21 giugno 2005, n. 1290, relativo al finanziamento della PAC, come modificato dal regolamento (CE) del Consiglio 26 novembre 2007, n. 1437, ed il regolamento (CE) della Commissione 18 marzo 2008, n. 259, recante modalità di applicazione del regolamento (CE) n. 1290/2005

e alla protezione dei dati personali, da una parte, e quello alla libertà di informazione, dall'altra parte, quest'ultimo è destinato a soccombere[25]. Sebbene i diritti della persona interessata tutelati dagli articoli 7 e 8 della Carta prevalgano, di norma, sulla libertà di informazione degli utenti di Internet, tale equilibrio può nondimeno dipendere, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona interessata[26], nonché dall'interesse del pubblico a disporre di tale informazione, che può variare a seconda del ruolo che tale persona riveste nella vita pubblica[27]. Difatti, in ragione del ruolo ricoperto, la *privacy* di un personaggio pubblico deve ritenersi cedevole rispetto all'interesse della comunità ad accedere al dato personale diffuso sul *web*[28]. Ancora, costituisce una eccezione il caso in cui il trattamento riguardi dati contenuti in pubblici registri, a fronte del quale, nella sentenza *Manni*, la Corte di giustizia ha riconosciuto carattere di prevalenza alle finalità di pubblicità legale rispetto alle esigenze di tutela del singolo[29].

Del pari, sembra condivisibile l'affermazione per la quale le attività compiute dai motori di ricerca, quali reperire contenuti tra i vari siti internet, indicizzarli e memorizzarli temporaneamente (c.d. *caching*), integrino un «trattamento di dati personali».

Nondimeno, discutibile è l'asserzione per cui il gestore di un motore di ricerca possa essere considerato, attraverso una interpretazione in senso lato[30], «responsabile del trattamento» dei dati personali, pur in presenza di un processo automatizzato di ricerca e di una selezione volontaria dei contenuti.

---

per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR), sono invalidi nella parte in cui, con riguardo a persone fisiche beneficiarie di aiuti del FEAGA e del FEASR, tali disposizioni impongono la pubblicazione di dati personali relativi ad ogni beneficiario, senza operare distinzioni sulla base di criteri pertinenti come i periodi durante i quali esse hanno percepito simili aiuti, la frequenza o ancora il tipo e l'entità di questi ultimi.

[25] In senso conforme due ordinanze recentissime, BVerfG, Beschluss des Ersten S nats vom 06. November 2019 - 1 BvR 16/13 -, Rn. (1-157), ECLI:DE:BVerfG:2019:rs20191106.1bvr001613; BVerfG, Beschluss des Ersten Senats vom 06. November 2019- 1 BvR 276/17 -, Rn. (1-142), ECLI:DE:BVerfG:2019:rs20191106.1bvr027617. Sul ruolo della Corte di giustizia nel riconoscere l'effettiva tutela del diritto alla *privacy* oltre i confini letterali e formali previsti dalla Carta, cfr. F. FERRARO, *Vecchi e nuovi problemi in tema di efficacia diretta orizzontale della Carta*, in *Federalismi,* 22 maggio 2019; O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*,in *Rivista diritto dei media*, 3/2018, p. 1.

[26] In senso conforme a quanto già statuito in *Google Spain*, tra i più recenti arresti v. Corte giust. 24 settembre 2019, causa C-136/17, *GC e a. (Déréférencement de données sensibles),* ECLI:EU:C:2019:773, su cui, per un primo commento, si rinvia a E. ROSSI, *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 *SIDIBlog* 2019.

[27] v., in tal senso, *Google Spain, cit.*, punto 81.

[28] Cfr. *Google Spain*, *cit.* punto 99.

[29] Cfr. Corte giust., 9 marzo 2017, causa C-398/15, *Camera di commercio c. Manni*, ECLI:EU:C:2017:197. Per un commento, si rinvia a M. FORTI, *Diritto all'oblio e conservazione dei dati iscritti nei pubblici registri: qualche considerazione a margine della Sentenza della Corte di giustizia della Corte di giustizia nel caso Manni*, in *Contratto e impresa*. *Europa*, 2018, p. 565.

[30] Una conferma della nozione ampia di responsabile del trattamento è contenuta nella recente sentenza che ha stabilito che l'amministratore di una *fanpage* di Facebook è congiuntamente responsabile, insieme a Facebook, per l'elaborazione dei dati personali degli utenti del *social network* e di quelli che visitano la *fanpage* attraverso *cookie*. Cfr. Corte giust. 20 luglio 2019, causa C-40/17 - *Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW e V,* ECLI:EU:C:2019:629.

Eppure, in *Google Spain* la Corte di giustizia ha compiuto una chiara scelta di carattere politico dal momento che, assimilando la posizione del motore di ricerca a quella di un "responsabile del trattamento", ha ribaltato, non solo l'opinione dell'Avvocato Generale[31], ma anche quella del Gruppo di lavoro Articolo 29[32], che auspicavano la necessità di una lettura «fattuale, piuttosto che formale» della direttiva con «attribuzione di responsabilità solo in presenza di un'influenza effettiva».

Invero, a parte le perplessità suscitate, soprattutto in punto di possibili scenari di censura preventiva, su cui si tornerà in seguito, la sentenza lascia irrisolte questioni di primaria importanza.

Innanzitutto, essa si connota per la vaghezza dei toni adoperati in ordine alla trasparenza della procedura per la cancellazione dei contenuti oggetto di richiesta da parte dell'interessato, con la conseguenza che un ampio margine di manovra – e in definitiva l'effettiva garanzia del diritto all'oblio – è praticamente lasciata a *Google* o comunque al motore di ricerca. In particolare, rimane aperto l'interrogativo se l'ordine di rimozione dei *links* lesivi del diritto all'oblio abbia una portata limitata al territorio dell'Unione o se, invece, spieghi effetti su scala mondiale, in tal modo alimentando un intenso dibattito[33] sulla questione dell'applicazione extraterritoriale delle norme dell'Unione europea, in specie degli artt. 7 e 8 della Carta. Peraltro, la politica messa in atto da *Google*, negli anni successivi alla pronuncia *Google Spain*, è stata quella di deindicizzare solo nei domini relativi agli Stati membri, e non anche nei domini *.com*.

Solo di recente, nella sentenza con cui ha deciso il rinvio pregiudiziale sollevato dal Conseil d'Etat nella controversia tra insorta tra *Google* e la Commissione nazionale francese per

---

[31] Conclusioni dell'AG Jääskinen, 25 giugno 2013, causa C-131/12, *Google Spain SL Google Inc. contro Agencia Española de Protección de Datos (AEPD) Mario Costeja González*, ECLI:EU:C:2013:424, punti 78 e 84, in cui l'Avvocato Generale aveva sostenuto l'inapplicabilità del ruolo di titolare del trattamento ai motori di ricerca. La Corte di Giustizia, peraltro, già nel caso *Lindqvist*, 6 novembre 203, C-101/01, Racc., 2003 I-12971, aveva adottato un'interpretazione della direttiva adeguandola al mutato scenario tecnologico, ritenendo che, in caso di trasferimento dei dati personali via internet, non fossero applicabili all'uso di Internet i criteri elencati nella direttiva.

[32] Cfr. Gruppo di lavoro Articolo 29, parere n. 1/2008, pag. 14, disponibile online at*: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148en.pdf.*

[33] v. *ex multis*, V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA E V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "Privacy Shield"*, Roma, 2016, p. 7 ss.; B. VAN ALSENOY – M. KOEKKOEK, *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted', 5 Int'l Data Privacy L.* 105, 2015, p. 110-111; M.L. RUSTAD – S. KULEVSKA*, Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow, 28 Harvard J. L. & Tech*, 2015, p. 349; J. DASKAL, *The Un-Territoriality of Data*, in *Yale L.J*, 2016; A.CHANDER, *U.P.LE,* 64 Emory L.J, 2015, p. 677; D.J.B. SVANTESSON, *Sovereignty in International Law - How the Internet (Maybe) Changed Everything, But Not for Long*, in *8 Masaryk U. J.L. & Tech*, 2014, p. 137; W. HEINTSCHEL VON HEINEGG, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKY (a cura di), *4th International Conference on Cyber Conflict*, 2012 NATO CCD COE Publications, p. 9; DAN J.B. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 Stan. J. Int'l L. 53*, 2014, p. 71; Id*., Extraterritoriality in the Context of Data Privacy Regulation, 7 Masaryk Univ. J. L. & Tech. 87,* 2013; L. MOEREL, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites Worldwide?*, in *Int'l Data Privacy L.*, 2010, n. 1; Y. POULLET, *Transborder Data Flows and Extraterritoriality: The European Position, 2 J. Int'l Commerc. L. & Tech. 146,* 2007; T.S. WU, *Cyberspace Sovereignty? The Internet and the International System,* 10 Harv. J. L.&Tech. 647, 1997.

l'informatica (CNIL)[34], la Corte ha provato a colmare quest'ultima lacuna. In particolare, sgombrando il campo da ogni equivoco sulla portata sostanziale del *right to be forgotten* e sui limiti territoriali di deindicizzazione dei *links* potenzialmente lesivi, essa ha escluso che in capo a *Google* sia ravvisabile un obbligo di cancellazione dei dati su tutte le versioni del suo motore. Pertanto, posto che in capo ai gestori di un motore di ricerca non sussiste alcun obbligo di cancellazione derivante dal diritto UE i cui effetti si estendano su scala globale, la Corte ha concluso che l'obbligo di rimozione dei *links,* oggetto di richiesta, ha implicazioni soltanto negli Stati membri dell'Unione.

Come accaduto già all'indomani della sentenza *Google Spain,* il tema della portata locale o globale dell'obbligo di rimozione citato ha visto contrapporsi due diverse visioni[35]. Da una parte, non può tacersi la tesi prospettata dalla CNIL, secondo la quale, se si confinasse il diritto all'oblio entro rigidi limiti nazionali o continentali, gli esperti internauti ben potrebbero aggirare il dominio nazionale di *Google* in cui avviene il *delisting* e accedere alle notizie cancellate. Dall'altra parte, prospettando la necessità di operare un giusto contemperamento tra il diritto all'oblio e la libertà di espressione, *Google* ha opportunamente rappresentato che l'eliminazione totale di quei contenuti costituirebbe un pericoloso precedente in ordine alla portata applicativa della disciplina UE, potendo indurre i regimi autoritari a richiedere parimenti l'attuazione a livello mondiale dei loro provvedimenti di censura[36].

Nella composizione delle prospettate posizioni contrastanti, la Corte ha rilevato che circoscrivere la portata della deindicizzazione al solo territorio dello Stato membro di residenza del richiedente sarebbe certamente illegittimo[37]. Pertanto, in linea con la volontà del legislatore europeo di garantire un elevato livello di tutela dei dati personali in tutti gli Stati membri, manifestata attraverso la sostituzione della direttiva 95/46/CE con il GDPR, direttamente applicabile in modo uniforme negli ordinamenti nazionali, a fronte di una eventuale richiesta di deindicizzazione, il gestore del motore di ricerca è tenuto a rimuovere i contenuti richiesti a partire da tutti i domini attivi negli Stati membri dell'Unione[38].

Diversamente, con riferimento alla portata extra-UE dell'obbligo di rimozione dei contenuti richiesti, pur mostrandosi consapevoli degli effetti che, grazie alla globalizzazione, produce l'accesso degli utenti al mondo senza confini di *Internet*, i giudici hanno affermato che, al di fuori dell'ambito territoriale delineato dall'art. 355 TFUE, il diritto UE non è destinato a trovare applicazione.

Vero è che, come evidenziato dall'Avvocato generale nelle sue conclusioni[39], il diritto UE conosce ipotesi eccezionali in cui spiega effetti extraterritoriali. A titolo esemplificativo, si

---

[34] Cfr. Corte giust., causa C-507/17, *cit.*

[35] Il Gruppo di lavoro articolo 29, in particolare, ha adottato linee guida per l'attuazione della sentenza Google Spain della Corte di giustizia. *Cfr.* Gruppo di lavoro articolo 29 (2014*), Guidelines on the implementation of the CJEU judgment on «Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González»*, C-131/12, WP 225, Bruxelles, 26 novembre 2014.

[36] In tal senso, v. Conclusioni AG, C-507/17*, cit*., punto 35.

[37] Cfr. Corte giust., C-507/17, *cit.,* punti 55-58.

[38] Cfr. Corte giust., C-507/17, *cit.,* punti 64 e 65.

[39] Cfr. Conclusioni AG, C-507/17, *cit.,* punti 47-53.

ricorda la giurisprudenza in materia di diritto della concorrenza[40], in virtù della quale la disciplina contenuta negli artt. 101 e 102 TFUE si applica anche quando una delle imprese coinvolte in un accordo o in una pratica anticoncorrenziale si trova al di fuori del territorio dell'Unione, purché tali comportamenti producano effetti nel mercato interno UE.

Ma è altrettanto vero che, in casi siffatti, ciò che rileva è l'impatto che le fattispecie vietate hanno su un ambito territoriale specificatamente delimitato dai Trattati, quale è il mercato interno. *Internet*, al contrario, per le sue caratteristiche intrinseche, coinvolgendo la globalità dei territori, sfugge ad una delimitazione precisa, sicché la ricerca di eventuali analogie tra le une e le altre fattispecie si risolverebbe necessariamente in un accostamento improprio.

Inoltre, come chiarito dalla Corte Ue, il gestore di un motore di ricerca non potrebbe essere tenuto ad eseguire l'ordine di cancellazione su scala globale, anche perché «molti Paesi terzi non riconoscono il diritto alla deindicizzazione o comunque adottano un approccio diverso rispetto ad esso»[41]. Né può dimenticarsi 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 gli altri diritti fondamentali, in ossequio al principio di proporzionalità»[42]. Per il vero, anche all'interno dell'Unione, il bilanciamento fra l'interesse del pubblico ad accedere alle informazioni può variare da uno Stato membro all'altro, con la conseguenza che il risultato del bilanciamento da realizzare tra tale interesse, da un lato, e i diritti alla tutela della vita privata e alla protezione dei dati personali dell'interessato, dall'altro lato, non è necessariamente identico per tutti gli Stati membri.

3. Il problema dell'estensione degli obblighi di rimozione dei contenuti illeciti dal *web*.

Le problematiche connesse alla controllabilità dei dati che circolano sul *web* e delle legittime pretese di quanti, in ragione del decorso del tempo, abbiano interesse a porre un limite alla memoria storica della rete, si sono acuite, in forza della crescente diffusione delle piattaforme online e, tra di esse, soprattutto, dei *social networks*.

La nuova realtà digitale ha assunto contorni sempre più complessi, poiché al già delicato coinvolgimento dei gestori dei motori di ricerca nell'indicizzazione delle pagine create dai proprietari dei siti web, si è aggiunto quello degli amministratori dei *social* che, consentendo di condividere contenuti sulle proprie piattaforme, sono sempre più coinvolti nel trattamento dei dati personali. Del resto, che l'esigenza di assicurare una adeguata protezione dei dati personali si intrecci fittamente con la previsione di più stringenti profili di responsabilità degli *hosting providers* appare confermata dalla Corte Ue, che ha qualificato anche quest'ultimi come «responsabili del trattamento», con tutte le implicazioni che ne derivano[43], sia in punto di sicurezza

---

[40] Cfr. Corte giust. 6 settembre 2017, causa C-413/14*, Intel c. Commissione*, EU:C:2017:632, punto 43 e giur. ivi citata. Cfr. P. DE PASQUALE, *La tutela della concorrenza oltre i confini comunitari tra applicazione extraterritoriale e cooperazione,* Editoriale Scientifica, Napoli, 2005, *Voce extraterritorialità,* in *Dizionario sistematico del diritto della concorrenza*, Napoli, 2013, p. 144 ss.

[41] Cfr. causa C-507/17*, cit.* punti 55-59.

[42] Cfr. causa C-507/17, *cit.* punto 60.

[43] Cfr. Corte giust. 5 giugno 2018, causa C-210/16 - *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig-Holstein GmbH,* ECLI:EU:C:2018:388, su cui sia consentito rinviare a A. CORRERA*, Dati personali: la nozione di "responsabile del trattamento" include il gestore di una fanpage presente su un social network*, in *DPCE Online*, [S.l.], v. 36, n. 3, oct. 2018; nonché, Corte giust. 20 luglio 2019,

dei dati, per cui su di essi grava l'obbligo di adottare tutte le misure di sicurezza adeguate al rischio[44]; sia in punto di riservatezza dei dati, per cui devono informare il titolare del trattamento di eventuali violazioni avvenute ed occuparsi della cancellazione dei dati alla fine del trattamento.

Eppure, a distanza di pochi giorni dal *Google 2 judgement*, la stessa Corte, chiamata, nel rinvio pregiudiziale proposto dal *Oberster Gerichtshof* nella causa *Glawischnig-Piesczek*, ad intervenire nell'esame della fattispecie che ha coinvolto il *social network* più famoso dei nostri tempi, *Facebook*[45], sembrerebbe essere entrata in contraddizione con quanto statuito nel pronunciamento anzi esaminato, affermando che gli effetti dell'ordine di rimozione di specifici contenuti diffamatori, emesso da una autorità giudiziaria statale nei confronti di un *hosting provider,* possono estendersi a livello mondiale.

Invero, la dimensione territoriale viene solo in apparenza diversamente declinata dalla Corte, ma, a ben vedere, secondo un disegno coerente e razionale.

Per comprendere l'importanza che la pronuncia *Glawischnig-Piesczek* riveste nel contesto che ci occupa, vale la pena ricostruire brevemente il quadro normativo europeo delineato dalla direttiva 2000/31/CE sul commercio elettronico che, com'è noto, regola la responsabilità degli *Internet service providers*.

Sul versante applicativo, essa non investe il settore della tutela dei dati personali[46]; sicché, dal regime speciale di responsabilità ivi previsto per gli *Internet service providers* è esclusa l'attività di trattamento delle informazioni personali che, viceversa, all'epoca dei fatti in giudizio, era disciplinata dalla direttiva 95/46, e oggi è regolata dal GDPR. Così come deve ritenersi esclusa dal relativo campo di regolamentazione l'attività dei motori di ricerca e il *linking*.

L'impianto normativo così delimitato si fonda sul principio della neutralità degli operatori, per cui gli *Internet service providers* non sono responsabili se la loro attività si limita ad operazioni tecniche che non contemplano la selezione dei contenuti e dei destinatari delle informazioni; oltre che sull'assenza di un obbligo generale di sorveglianza in capo agli *Internet service providers* sui contenuti diffusi dai destinatari dei propri servizi. Pertanto, coerentemente con la disciplina in esame, il *provider* è civilmente responsabile solo se, venuto a conoscenza dell'illiceità dei contenuti diffusi per mezzo dei servizi digitali offerti, non si attivi per rimuoverli.

Il legislatore europeo, a ben vedere, ha scelto un modello di responsabilità imperniato sulla colpa del *provider*, considerato come mero depositario dei contenuti informativi, rinunciando al diverso schema della responsabilità oggettiva, come quella da rischio di impresa o

---

causa C-40/17, *Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW e V,* ECLI:EU:C:2019:629, su cui sia consentito rinviare a A.CORRERA, *Digitalizzazione e profilazione degli utenti: la Corte Ue sul consenso informato e sulla responsabilità degli operatori online*, in *Diritto dell'Unione europea*, 24 maggio 2020.

[44] v. art. 32 GDPR.

[45] Cfr. Corte giust., causa C-18/18, *cit.*

[46] In particolare, restano escluse dalla disciplina in esame, secondo la previsione di cui all'art. 1, par. 4, lett. b), della direttiva sul commercio elettronico le «*questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE*».

editoriale[47]. Questa scelta, che ha agevolato lo sviluppo economico dei nuovi operatori, risponde, sin dal progetto normativo originario, all'esigenza di scongiurare il rischio di assegnazione di poteri "censori" in capo agli ISP.

Tuttavia, il maggior limite di questa normativa consiste nella mancata previsione delle condizioni in presenza delle quali i titolari dei diritti possono indirizzare una richiesta di rimozione di eventuali contenuti illeciti agli ISP; nonché nell'assenza di indicazioni per individuare il momento in cui questi ultimi, venuti a conoscenza della commissione di un illecito, possono essere tenuti a rimuovere i contenuti oggetto di richiesta.

Inoltre, preme osservare che, a distanza di quasi un quindicennio, lo scenario entro cui è stata concepita la direttiva 2000/31 è radicalmente mutato. Difatti, le imprese della *digital economy* presentano molteplici peculiarità rispetto a quelle tradizionali, *in primis* la capacità di realizzare, in un lasso di tempo relativamente breve, posizioni monopolistiche o dominanti sul mercato di riferimento.

In questo quadro si inserisce la recente sentenza *Glawischnig-Piesczek c. Facebook* che origina da un caso di diffamazione sul noto *social network,* che ha spinto la Corte suprema austriaca a rivolgersi alla Corte di giustizia.

In particolare, i giudici hanno chiarito due aspetti di primaria importanza connessi all'applicazione della direttiva sull'*e-commerce*, segnatamente la portata personale e sostanziale degli obblighi gravanti su un *host provider* (che mette a disposizione uno spazio web attraverso la memorizzazione "duratura" delle informazioni)*,* alla luce della previsione di cui all'art. 15, par. 1 della direttiva richiamata, che vieta l'imposizione di un obbligo generale di sorveglianza; e la portata territoriale dell'ordine di rimozione emesso da un giudice interno che intima all'*host provider* di cancellare i contenuti dallo stesso memorizzati (non solo per gli utenti di Internet dello Stato membro interessato, ma a livello mondiale).

Con riferimento alla prima questione, preme osservare che essa concerne la rimozione di informazioni diffuse attraverso una piattaforma di rete sociale *online*, il cui contenuto è soggetto a mutamenti continui, in ragione degli scambi costanti tra gli utenti, e che, come ricordato, sull'*hosting provider* non grava alcun obbligo di controllo preventivo sulle informazioni dagli stessi condivise.

Ciò consente di affermare che il *provider* non è responsabile dell'illiceità delle informazioni memorizzate o dell'attività svolta per mezzo delle stesse, perché gode rispetto ad esse di

[47] Sul tema della responsabilità civile degli ISP si vedano: V. ZENO-ZENCOVICH, *I rapporti tra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari)*, in *Riv. Dir. Inf.* 1999, p. 1050 ss.; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; S. SICA, *Le responsabilità civili*, in E. TOSI (a cura di), *Commercio elettronico e servizi della società dell'informazione*, Milano, 2003, p. 267 ss.; M. GAMBINI, *Le responsabilità civili dell'Internet service provider*, Napoli, 2006; E. TOSI, *Diritto privato dell'informatica e di Internet. I beni - I contratti - Le responsabilità*, Milano, 2006; M. DE CATA, *La responsabilità civile dell'internet service provider*, Milano, 2010; A. MANTELERO, *La responsabilità online: il contratto nella prospettiva dell'impresa*, in *Riv. Dir. Inf.*, 2010, p. 405 ss.; E. TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine di recenti casi «Google Suggest» per errata programmazione dei Software di ricerca e «Yahoo Italia!» per link illecito in violazione dei diritti di proprietà intellettuale*, in *Riv. Dir. Inf.*, 2012, p. 44 ss.

una immunità relativa. Viceversa, l'*hosting provider* è tenuto ad attivarsi per rimuovere le informazioni in questione o a disabilitarne l'accesso[48] se, per una qualsiasi ragione, venga a conoscenza della loro illiceità. Inoltre, gli Stati membri possono adottare ingiunzioni a tutela della vittima di un illecito di cui l'*hosting provider* può essere destinatario, anche nell'ipotesi in cui non sia ritenuto responsabile[49].

In considerazione dell'assenza di un obbligo generale di sorveglianza, la Corte ha ritenuto compatibile con le esigenze di tutela che la normativa UE vuole assicurare una ingiunzione promanante dall'autorità pubblica nazionale che imponga al *social network* di rimuovere tutte le informazioni da esso memorizzate il cui contenuto sia "identico" o "equivalente" rispetto a quello di un'informazione precedentemente dichiarata illecita, purché l'attività di ricerca e di sorveglianza delle stesse sia limitata ad informazioni contenenti messaggi dall'oggetto sostanzialmente invariato rispetto a quello sottoposto ad accertamento di illiceità[50] da parte dell'organo giurisdizionale competente. E, sempre che le differenze nella formulazione di tale contenuto, non siano tali da costringere l'*hosting provider* a compiere autonome valutazioni, rivelandosi sufficiente a tal fine il ricorso a strumenti automatizzati.

Per questa via, non risulterebbe contravvenuto il menzionato divieto degli obblighi di sorveglianza e di ricerca attiva, perché l'individuazione dei termini integranti una "equivalenza" è di fatto rimessa all'autorità pubblica e non è lasciata al libero apprezzamento dell'*hosting provider*.

Per quanto riguarda l'estensione territoriale degli effetti di tale ingiunzione, invece, la Corte, condividendo la tesi prospettata dall'Avvocato Generale, ha rilevato come dal diritto dell'Unione non derivino limitazioni quanto alla rimozione su scala mondiale di un contenuto illecito *online* e che, dunque, la questione vada analizzata in base al diritto internazionale[51]. In tal guisa, spetta agli Stati membri assicurarsi che i provvedimenti di ingiunzione da essi emanati - che producono effetti a livello mondiale – siano in armonia con le norme dell'ordinamento internazionale.

4. Alcune considerazioni a margine dei recenti arresti della Corte di giustizia.

All'indomani della recente sentenza *Google 2 judgement,* v'è chi ha sostenuto che essa rappresenti una vittoria per la libertà di espressione. Difatti, secondo i rappresentanti del motore di ricerca e le associazioni intervenute[52] in giudizio, la pronuncia scongiurerebbe il rischio di un potenziale danno al diritto degli utenti di *Internet* di accedere alle informazioni, che si verificherebbe in caso di estensione dell'obbligo di deindicizzazione previsto dal diritto UE in difesa del diritto all'oblio su scala mondiale.

In questa ottica, un obbligo di tal portata apparirebbe sproporzionato con le esigenze di tutela che la normativa europea vuole assicurare. Del resto, già in *Google Spain* la Corte ha

---

[48] In senso conforme, v. Corte giust., 12 luglio 2011, causa C-324/09, *L'Oréal e a.,* EU:C:2011:474, punti 139 e 144; nonché, 24 novembre 2011, causa C-70/10, *Scarlet Extended*, EU:C:2011:771, punti 36 e 40; 16 febbraio 2012, causa C-360/10, *Sabam*, EU:C:2012:85, punti 37 e 38.
[49] Cfr. causa C-18/18, *cit.* punto 25.
[50] Cfr. causa C-18/18, *cit.* punto 41.
[51] Conclusioni AG, causa C-18/18 *cit.,* punto 92
[52] Cfr. *Written Observations of Article 19 and others*, intervenuti nel corso del giudizio, disponibile online at: *www.articolo19.org*

fatto espresso riferimento «all'interesse legittimo degli utenti di Internet potenzialmente interessati ad avere accesso a tali informazioni", osservando che "in situazioni come quella di cui trattasi occorre ricercare un giusto equilibrio tra tale interesse e i diritti fondamentali dell'interessato ai sensi degli artt. 7 e 8 della Carta».

Pertanto, alla luce dell'importanza che *Internet* riveste per la libertà di espressione e di informazione, tutelata dall'articolo 11 della Carta, e che i collegamenti ipertestuali contribuiscono al suo buon funzionamento, nonché allo scambio di opinioni e di informazioni in quella rete, un obbligo generale di cancellazione delle informazioni su base globale per motivi di protezione dei dati, che ometta di tenere in debito conto la libertà di espressione o di accesso alle informazioni, costituirebbe un pericoloso precedente che potrebbe essere strumentalmente adottato in Stati membri in cui tali diritti fondamentali sono già minacciati. Senza dimenticare l'influenza che una decisione di tal genere potrebbe avere sulle pratiche delle autorità di regolamentazione e dei tribunali di numerosi altri Paesi extra-UE, che non godono di un elevato livello di protezione dei diritti fondamentali.

A ben riflettere, la portata quasi dirompente della pronuncia sembra sfumare ad una attenta analisi del *dictum* della Corte. Difatti, sebbene i giudici europei escludano che dal diritto UE deriva un obbligo di cancellazione su scala mondiale, fanno salvo il potere delle autorità di controllo o giurisdizionali nazionali di chiedere al fornitore di servizi di motore di ricerca di effettuare una deindicizzazione su tutte le versioni del motore medesimo.

Il rilievo a cui si espone quest'ultima affermazione di principio semmai è che essa non sembra pienamente conciliante con lo spirito del GDPR, nella misura in cui, restituendo agli Stati membri il potere di "regolamentazione", rischia di generare una frammentazione della relativa disciplina con l'attribuzione ai cittadini UE di un *right to delisting information* universalmente in un Paese e solo a livello nazionale in un altro. Né si comprende se ci sarà, a questo punto, la possibilità per gli interessati europei di scegliere e selezionare il tipo di cancellazione che preferiscono.

Oltretutto la Corte ha probabilmente perso l'occasione di affrontare il tema del diritto all'oblio in una prospettiva più universale, optando per un approccio anacronistico e conservatore al quale eravamo evidentemente disabituati nel contesto che ci occupa. Difatti, se in *Google Spain* si era coraggiosamente fatta promotrice del modello europeo di protezione dei dati personali, all'occorrenza ricorrendo ad una interpretazione "manipolativa" della disciplina UE, nel suo più recente pronunciamento, pur non essendo revocabile in dubbio la validità degli argomenti giuridici utilizzati sotto il profilo formale, la Corte rallenta e rende più difficile l'effettività del diritto all'oblio[53].

---

[53] In tal senso, le prime dichiarazioni rilasciate dal Garante per la protezione dei dati personali italiano, cfr. Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali, *Diritto all'oblio - "Barriere territoriali anacronistiche, questa sentenza penalizza gli utenti",* di Claudia Guasco, "Il Messaggero" e "Il Mattino", 25 settembre 2019. Tra i contributi dottrinali, v. O. POLLICINO, *L'"autunno caldo" della Corte di giustizia in tema di diritti forndamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri dei privati in ambito digitale,* in *Federalismi*, 16 ottobre 2019; O. J. GSTREIN, *The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), VerfBlog,* 2019/9/25; E. ROSSI, *Forget me... or not?, cit.*; A. MIGLIO, *Enforcing the Right to Be Forgotten Beyond EU Borders*, in *Use and Misuse of New Technologies Contemporary Challenges in International and European Law*, Springer, 2019.

La soluzione adottata sembra proprio andare incontro a quei rischi che, in parte, erano già stati paventati al tempo di *Google Spain*[54], per cui le informazioni non più accessibili nell'ambito dell'area dell'Unione, per effetto di una deindicizzazione necessariamente parziale, continuano ad essere, invece, assolutamente fruibili *aliunde*. Conseguentemente, lo scenario verso il quale ci si potrebbe orientare determinerà, verosimilmente, da un lato, una quantità di informazioni accessibili differente, a seconda del luogo nel quale avviene la ricerca (i contenuti non indicizzati in Europa continueranno ad esserlo fuori dal territorio dell'Unione), e, dall'altro lato, consentirà agli operatori, a seconda del luogo nel quale sono stabiliti - luogo che non incide sulle possibilità di accesso e di utilizzo degli utenti - di offrire contenuti diversi[55].

Inoltre, la Corte di giustizia ha perso nuovamente l'occasione per chiarire la dimensione sostanziale del diritto alla cancellazione e definire la portata del potere di autodeterminazione informativa dell'individuo nel dominio digitale. Pertanto, continua a non essere chiaro in che modo il *delisting* sia implementato nel GDPR in dettaglio, lasciando privi di risposta i nodi problematici che minacciano lo Stato di diritto e il controllo democratico dello spazio digitale.

Ad ogni modo, in disparte i profili di criticità evidenziati, la circostanza che la Corte abbia salvato il potere dei garanti nazionali di emettere ordini di rimozione dei *links* contestati con effetti extra-UE, consente di affermare che le statuizioni previste nel caso *Facebook* sulla natura globale dell'ordine di rimozione non costituiscono una contraddizione con quanto rilevato in riferimento al caso *Google 2 judgement*.

Nel caso *Glawischnig-Piesczek c. Facebook*, i giudici ricordano che la direttiva sul commercio elettronico non prevede alcuna limitazione in ordine alla portata territoriale dei provvedimenti di rimozione che le autorità giudiziarie o amministrative hanno il potere di adottare. Peraltro, com'è stato giustamente rilevato, la posizione da ultimo assunta è chiaramente tesa a scongiurare il rischio di una privatizzazione della "giustizia digitale", che si verificherebbe laddove il *social network*, secondo quanto annunciato, procedesse alla costituzione di un organismo "indipendente" al servizio degli utenti che vogliano ottenere la rimozione di specifici contenuti dalla piattaforma *online*[56].

Difatti, la privatizzazione della censura derivante dalla delega alle piattaforme della rimozione di contenuti specificatamente individuati dalle autorità giudiziarie assume un rilievo centrale nel caso *Facebook*, diversamente dal caso *Google 2*, in cui la Corte Ue, come già osservato, si è concentrata solo sulla portata territoriale degli obblighi di rimozione dei *links* lesivi del diritto all'oblio[57].

---

[54] Il riferimento è, in particolare, ai rilievi del Gruppo di lavoro articolo 29, cit., secondo cui nell'ottica di garantire una tutela effettiva ai diritti fondamentali, la cancellazione dei soli domini europei non può essere considerata una valida soluzione, giacchè essa non impedisce che le informazioni possano essere raggiunte *aliunde*.

[55] A conferma del fatto che la materia in esame sia ormai in continuo fermento, è utile osservare che il 2 dicembre scorso è stato diffuso il progetto di Linee guida sul diritto all'oblio. Peraltro, tale progetto è stato messo a disposizione della pubblica consultazione sino al 05 febbraio scorso, termine entro il quale cittadini o autorità hanno potuto inviare le proprie osservazioni al Comitato prima della successiva adozione. European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, 2 dicembre 2019.

[56] Si veda in tal senso, O. POLLICINO, *cit.* secondo cui la Corte ha voluto ribadire che l'operazione di bilanciamento dei diritti fondamentali online deve essere affidata ad autorità giurisdizionali o comunque a rilevanza pubblicistica e non ad un operatore privato o ad un organismo dallo stesso nominato.

[57] Cfr. M. MONTI, *La Corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18-18 sul discorso pubblico online e sul ruolo di Facebook*, in *Medialaws*, 15 ottobre 2019.

In particolare, la Corte affida al *social network* l'onere di rimuovere contenuti identici o equivalenti a quelli dichiarati illeciti, ma individuati *a priori* dall'autorità giudiziaria o amministrativa. Da qui l'adeguatezza nel perseguimento di detta finalità di un'attività automatizzata, che non lascia spazio ad alcuna valutazione discrezionale da parte dello stesso *social network*.

Occorre, però sottolineare che, sebbene detto meccanismo abbia indubbi risvolti positivi in termini di tempestività della tutela, non va esente da rilievi critici con riferimento al legittimo esercizio della libertà di espressione *online*. Ciò in quanto l'impiego di strumenti di controllo automatizzato, pur secondo le prescrizioni contenute nell'ingiunzione dell'autorità competente, se, da una parte, riduce il rischio di una violazione della previsione di cui all'art. 15 della direttiva sul commercio elettronico, dall'altra parte, ben potrebbe comportare la rimozione e, dunque, la censura di contenuti che ripropongono in maniera identica o equivalente quel tipo di esternazioni per fini estranei alla diffamazione, come avviene, ad esempio, nel caso della critica o della satira[58]. La mancanza di attenzione a questo profilo, unitamente al mancato riferimento alla predisposizione di specifici mezzi di ricorso, è acuita dall'assenza, nell'*iter* motivazionale della sentenza *Glawischnig-Piesczek c. Facebook* di qualsivoglia riferimento all'art. 11 della Carta e alla necessità di tutelare, oltre alla reputazione e alla libertà di impresa, anche la libertà di espressione *online.* Aspetti quest'ultimi sui quali, invece, l'Avvocato Generale si è ampiamente soffermato nelle proprie conclusioni, laddove, evidenziando i rischi di censure sistematiche insiti nella delega al *social network* della rimozione di contenuti senza istruzioni precise da parte di un'autorità pubblica, ha sottolineato l'importanza di un'operazione di bilanciamento tra diritti fondamentali, non limitata alla tutela della dignità e agli interessi delle *Internet platforms*, ma inclusiva anche della libertà di espressione *online*[59].

In definitiva, non v'è dubbio che la soluzione adottata dalla Corte sia condivisibile nelle sue conclusioni. Ciononostante, non può tacersi che essa non risolve il problema delle censure sistemiche determinate da rimozioni automatizzate, già evidenziato con riferimento al diritto all'oblio[60] sin da *Google Spain.*

Il rischio è quello di riesumare proprio le criticità che la direttiva sul commercio elettronico si proponeva di superare. E, dunque, la circostanza che gli intermediari della rete si trasformino in «censori istituzionali», divenendo àrbitri delle informazioni accessibili, incentivati e legittimati ad operare una selezione non solo della loro quantità, ma anche della loro qualità, all'occorrenza eliminando i contenuti scomodi e sgraditi[61].

---

[58] Cfr. Conclusioni AG, causa C-18/18, *cit.,* punto 74, ove si legge che «l'attuazione di siffatte soluzioni darebbe luogo ad una censura, con la conseguenza che la libertà di espressione e di informazione potrebbe essere sistematicamente limitata».

[59] Cfr. B. NASCIMBENE, F. ROSSI DAL POZZO, *L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea e orientamenti giurisprudenziali*, in *Eurojus*, 23 dicembre 2019.

[60] Sul punto, v. O. POLLICINO, *Google rischia di «vestire» un ruolo para-costituzionale,* in *Il Sole 24 Ore*, 14 maggio 2014. E, inoltre, v. A. PALMIERI - R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro italiano*, 1/2014.

[61] Cfr. S. RODOTÀ, *Libertà, opportunità, democrazia e informazione, in Internet e privacy: quali regole?,* Atti del Convegno di Roma, 8-9 maggio 1998, *Cittadini e Società dell'informazione*, Supplemento n. 1 al Bollettino n. 5 del Garante, 1998, 15, che, a proposito degli ISP, paventò il rischio che potessero divenire dei "censori istituzionali".