amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 2/2023

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudio, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sańchez-Mesa Martĩnez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Salvatore Villani, Stefania Terracciano.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Le pubbliche amministrazioni e il diritto all'oblio

di Luigi Ferrara

(Professore Associato di Diritto Amministrativo presso l'Università degli Studi di Napoli "Federico II")

e

Francesco Rota

(Professore Associato di Diritto Amministrativo presso l'Università degli Studi del Sannio, Benevento)

Sumario

1. Affermazione ed evoluzione del diritto all'oblio; 2. Privacy, gestione dei dati, diritto all'oblio e pubbliche amministrazioni; 3. Poteri e ruolo del garante nel mondo globalizzato; 4. La proporzionalità degli strumenti di tutela tra privacy e libertà di informazione; 5. La "deindicizzazione" e i suoi confini territoriali nella giurisprudenza europea e nazionale; 6. Autorità nazionali, confini nazionali e archivi digitali.

Abstract

The paper analyses the right to be forgotten in Italian legal order and in EU case law. The paper starts analysing the right to be forgotten in Italian legal order, focusing the role of the Italian Data Protection Authority. Then, the article focuses the Italian and EU case law.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review.*

1. Affermazione ed evoluzione del diritto all'oblio.

L'elaborazione dottrinale ha negli ultimi anni, coerentemente con il processo di evoluzione digitale della società, progressivamente affermato, partendo dall'art. 2 Cost., un vero e proprio diritto all'identità digitale che non si esaurisce nella dimensione anagrafica e identificativa riconducibile al Sistema Pubblico Identità Digitale (SPID) e che comprende il complesso di dati, informazioni, attività che consentono di ricostruire una nuova immagine della persona stessa, un suo doppio, che incide nella dimensione sociale in cui la persona opera[1].

In questo senso è possibile affermare che il diritto all'identità digitale è connesso al diritto di ciascun soggetto di essere rappresentato nella vita di relazione con la sua vera identità, insieme di caratteristiche morali, sociali, politiche, ecc., che esprimono la personalità individuale[2], ed è connesso alla pretesa di non vedere distorta la propria immagine e a veder tutelato il diritto ad essere se stessi, nel rispetto del titolare dell'identità ma anche degli altri consociati che hanno il diritto «*di considerare la persona con la sua specifica individualità e non con una diversa*»[3].

Il GDPR sancisce una serie di diritti a favore dell'interessato che, consentendogli di controllare e proteggere i propri dati personali, diventano strumento di tutela dell'identità digitale[4]. Fra questi diritti troviamo il diritto all'oblio[5] che viene

---

* *Il lavoro è frutto della riflessione comune degli autori. Tuttavia, i paragrafi 1, 2 e 3 sono stati redatti da Francesco Rota, i paragrafi 4 5 e 6 da Luigi Ferrara;*

[1] G. ALPA, L'identità digitale e la tutela della persona. Spunti di riflessione, in Contratto e impresa, 2017, p. 723.

[2] La giurisprudenza riconosce ormai da tempo una dimensione dell'identità personale coerente con la prospettiva indicata. Si vedano sul punto, Corte di Cass., sez. I, sent. 22 giugno 1985, n. 3769, ripresa poi dalla giurisprudenza successiva e Corte Cost., n. 7 del 9 febbraio 1994, che annovera tra i "nuovi diritti" anche il diritto all'identità personale. Storicamente il diritto all'identità personale ha subito una notevole evoluzione e si è evoluto sul piano concettuale che su quello degli strumenti di tutela. Il diritto, la cui definizione è opera della giurisprudenza, è stato in un primo momento connesso all'insieme dei connotati che consentivano di identificare la persona rispetto ai pubblici poteri e agli altri consociati ed è poi, alla luce del principio personalista, diventata, in prospettiva costituzionalmente orientata, una situazione soggettiva comprensiva degli elementi che esprimono la personalità, arricchendosi di fattori intellettuali, caratteriali ed ideologici. Per la prima impostazione, si veda G. FALCO, Identità personale, in Nuovo Dig. It., VI, Torino, 1938, p. 649; per la seconda, si veda S. RODOTÀ, Persona, riservatezza, identità. Prime note sistematiche sulla proiezione dei dati personali, in Riv. Crit. Dir. Priv., 1997, p. 583.

[3] Così, T. PASQUINO, Identità digitale, della persona, diritto all'immagine e reputazione, in E. TOSI (a cura di), Privacy digitale , Giuffré, Milano, 2019, p. 93, cui si rinvia anche per il passaggio dall'identità della persona all'identità digitale. Sul punto si vedano anche A. PIRAINO LETO, Il diritto ad essere se stessi, in diritto fam. e pers., 1990, p. 603; S. NIGER, Il diritto all'identità personale, in G. FINOCCHIARO (a cura di), Diritto all'anonimato, Padova, 2008, p. 115.

[4] E. TOSI, Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy, in E. TOSI (a cura di), Privacy digitale , Giuffré, Milano, 2019, p. 34.

[5] F. DI CIOMMO, Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), I dati personali nel diritto europeo, Torino, 2019, p. 373 ss. sostiene che il legislatore del Regolamento europeo non avrebbe inteso disciplinare in modo specifico il diritto all'oblio e si sia preoccupato piuttosto di garantire il diritto alla cancellazione dei dati.

ISSN 2036-7821

ricostruito dalla dottrina come un autonomo diritto della personalità o come uno degli aspetti del diritto alla riservatezza o come un profilo del diritto all'onore[6].

Il rilievo crescente del diritto all'oblio emerge immediatamente se si considera l'evoluzione che l'accessibilità delle informazioni ha subito grazie all'avvento della rete e l'incremento progressivo di efficenza dei motori di ricerca: è stato a tal proposito affermato che si produce «*un fenomeno di trasparenza non solo individuale, ma collettiva, in base al quale, ciascuno può conoscere informazioni relative a ciascun altro (…) e vengono frustrati i principi di pertinenza e di essenzialità che hanno orientato l'interprete nel decidere sulla diffusione delle informazioni personali*»[7] e che internet è un luogo in cui nulla si perde o viene dimenticato, con il rischio che le informazioni, una volta pubblicate on line, siano sempre agevolmente accessibili[8], generando così il rischio che si possa diventare «*prigionieri di un passato destinato a non passare mai*»[9].

L'evoluzione digitale della società ha contribuito a determinare un progressivo cambiamento delle connotazioni e dei contenuti del diritto all'oblio che nella ricostruzione dottrinaria e giurisprudenziale da diritto a dimenticare è diventato prima diritto a contestualizzare e poi, da ultimo diritto alla deindicizzazione[10].

L'art. 17 del Regolamento UE 2016/679 sancisce il diritto all'oblio, ossia il diritto alla cancellazione dei propri dati personali, riprendendo e ampliando nel paragrafo 1 e nel paragrafo 3 le cause che tradizionalmente giustificano il diritto dell'interessato di chiedere e ottenere la cancellazione dei propri dati e le condizioni che consentono al titolare del trattamento di respingere la richiesta mentre, nel paragrafo 2, afferma in modo assolutamente innovativo che l'obbligo di cancellazione deve tener conto delle tecnologie disponibili e dei costi di attuazione per informare della richiesta dell'interessato i titolari che stanno trattando i dati personali oggetto di cancellazione.

In questo modo la norma fa discendere dalla responsabilità di aver reso pubblici i dati, l'obbligo per il titolare di informare anche i terzi, restando ancorata in parte ad

---

[6] La definizione del diritto all'oblio come diritto autonomo sembra essere emersa in relazione al diritto di cronaca. Sul punto vedi ex multis G.B. FERRI, Diritto all'informazine e diritto all'oblio, in Riv. Dir. Civ., 1990, I, 801 ss. Per una lettura diversa si veda D. MESSINA, Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione, in Inf. Dir., 2009, p. 93; F. DI CIOMMO, Quello che il diritto non dice. Internet e oblio, in Danno e resp., 2014, p. 1101. Con riferimento alla disciplina contenuta nel GDPR si veda S. BONAVITA-R. PARDOLESI, GDPR e diritto alla cancellazione (oblio), in Danno e Resp., 2018, p. 269; E. LUCCHINI GUASTALLA, Privacy e data protection: principi generali, in E. TOSI (a cura di), Privacy digitale , Giuffré, Milano, 2019, p. 81. Per una ricostruzione della nascita ed evoluzione del diritto all'oblio L. TULLIO, Tracce evolutive del "Right to be forgotten" tra esigenze di anonimato e richieste di deindicizzazione, in Ianus, 2020, p. 109-111.

[7] P. SAMMARCO, Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato, in E. TOSI (a cura di), Privacy digitale , Milano, 2019, p. 166.

[8] S. RODOTÀ, La vita e le regole, Milano, 2018, p. 64.

[9] Così, S. RODOTÀ, Il mondo nella rete. Quali i diritti. Quali i vincoli, Roma-Bari, 2014, p. 43.

[10] Per una ricostruzione della menzionata evoluzione si veda G. BEVIVINO, Il diritto all'oblio nell'epoca "digitale": ruolo della giurisprudenza ed esigenze di regolamentazione, in Giust. Civ., 2022, 1, p. 217 ss.

ISSN 2036-7821

una visione "proprietaria" del diritto ma con un'apertura alla prospettiva di controllo sui propri dati, aperta proprio dal contenuto del paragrafo 2[11].
La norma individua analiticamente le circostanze che possono costituire presupposto per l'esercizio del diritto all'oblio, annoverando situazioni di natura obiettiva, quale l'illiceità del trattamento, e di natura soggettiva, quale la revoca del consenso in assenza di altro fondamento giuridico per il trattamento[12].
Il quadro viene completato dall'art. 19 del Regolamento che sancisce l'obbligo di notifica dell'avvenuta cancellazione dei dati.
L'esercizio del diritto all'oblio deve tener conto, ogni qualvolta il titolare del trattamento sia una Pubblica Amministrazione, anche delle linee guida emanate dall'Autorità Garante nel maggio 2014 con il provvedimento n. 243, "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*"[13].
Viene così confermato che la Pubblica Amministrazione, anche nelle ipotesi di pubblicazione di atti o documenti ai sensi del D. Lgs n. 33/2013, deve rispettare i principi in tema di protezione dei dati personali, tra cui il principio di necessità, ma anche il rispetto della privacy by design e by default, che deve comprendere meccanismi di cancellazione senza ritardo dei dati il cui trattamento non è più necessario e il rispetto del diritto all'oblio[14].

2. Privacy, gestione dei dati, diritto all'oblio e pubbliche amministrazioni

Il rilievo giuspubblicistico della disciplina della privacy (rectius della gestione dei dati) nasce da fattori diversi e sfaccettati che arrivano ad avere impatti ed incidenze addirittura sulla sicurezza nella sua attualissima dimensione di cibersecurity, che ha portato addirittura alla istituzione della Agenzia per la Cybersicurezza Nazionale e ha spinto la dottrina ad inquadrare la sicurezza cibernetica fra le funzioni

[11] Per i limiti e le implicazioni del paragrafo 2 dell'art. 17 del Regolamento UE 2016/679 si veda F. PIZZETTI, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, in PIZZETTI (a cura di) Intelligenza artificiale, protezione dei dati personali e regolazione, Torino, 2018, p. 27, secondo il quale la norma «più che sancire un vero e proprio diritto all'oblio, obbliga il titolare che ha ricevuto una richiesta legittima di cancellazione di dati personali da parte dell'interessato, a farsi tramite di tale richiesta anche nei confronti di chiunque lui sappia essere venuto a conoscenza dei dati in questione e li stia trattando».

[12] E. LUCCHINI GUASTALLA, Privacy e data protection: principi generali, cit., p. 82, che evidenzia la difficoltà di ricondurre ad una ratio unitaria i presupposti del diritto all'oblio individuati dal GDPR, riconducendo unitariamente tale diritto.

[13] In tema di applicazione del GDPR alla pubblica amministrazione si veda G. CARULLO, Diritto all'oblio e dovere di provvedere delle pubbliche amministrazioni, in Eurojus, ROSSI DAL POZZO (a cura di), Fascicolo Speciale, Mercato Unico Digitale, Dati personali e Diritti fondamentali, 2020, p. 171 ss..

[14] G. D'ACQUISTO, M. NALDI, Big data e privacy by design, Torino, 2017.

ISSN 2036-7821

pubbliche[15]. A tale rilievo contribuisce poi la maturazione della consapevolezza che la privacy comprende due macro diritti fondamentali, il diritto al rispetto della propria sfera personale e il diritto alla protezione dei dati personali[16] ed è però connesso anche al fatto che, a differenza della Direttiva 95/46, la regolamentazione vigente non ha come unico scopo la tutela dell'interessato ma guarda ad una prospettiva più ampia: la garanzia di diritti e libertà delle persone fisiche, che può subire pregiudizi a causa di trattamenti di dati personali[17]. Come comprensibile, siffatta garanzia non rappresenta una prerogativa assoluta ma, come afferma il considerando 4 del GDPR, «*va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali in ossequio al principio di proporzionalità*». E' stato a tal proposito affermato che la tutela dei dati personali non può né essere irrigidita al punto da «*diventare ostacolo per la libera circolazione dei dati e lo sviluppo di una società democratica*» né «*essere attenuata fino al punto di mettere a rischio la tenuta sociale*»[18]. Essa richiede un uso attento del principio di proporzionalità per il corretto bilanciamento con gli altri diritti[19]. E' del resto incontrovertibile che il diritto all'oblio, in quanto "figlio" della società dell'informazione[20] , abbia subito l'influenza dell'evoluzione digitale e della pervasività della rete, che impattano anche sullo stesso bilanciamento, ridefinendo ad esempio il confine tra diritto all'informazione e diritto all'oblio[21].

L'impiego sempre più ampio di algoritmi e Intelligenza artificiale nell'evoluzione in corso della società digitale aiuta peraltro a comprendere come ci sia un interesse

[15] Per una ricostruzione della sicurezza e dei suoi possibili significati sia consentito il rinvio a F. ROTA, Sicurezza, ordina pubblico e polizie, Napoli, 2012. In tema di Cybersicurezza si veda R. URSI (a cura di), La sicurezza nel cyberspazio, Milano, 2023 e in particolare R. URSI, La sicurezza cibernetica come funzione pubblica, p. 7 ss. e M. MAURINO, Cybersecurity, sicurezza nazionale e trattamento dei dati personali, p. 169 ss., cui si rinvia anche per la disamina e il commento della giurisprudenza europea in tema di bilanciamento tra cybersecurity, sicurezza nazionale e diritto alla protezione dei dati personali. Sul bilancimaento tra sicurezza nazionale e tutela dei diritti fondamentali in relazione alla conservazione dei dati si veda G. NADDEO, Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "Data retention saga" dinanzi alla Corte di Giustizia, in Freedom, Security & Justice, European legal studies, 2, 2022, p. 188 ss. Per una disamina del bilanciamento possibile tra sicurezza e privacy, si veda M. RUBECHI, Sicurezza, tutela dei diritti fondamentali nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi), in federalismi.it, 2016.

[16] E. TOSI, Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy, cit., p. 28.

[17] F. PIZZETTI, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, cit., p. 37.

[18] Così, F. PIZZETTI, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, cit., p. 38.

[19] Per una disamina del bilanciamento nella prospettiva della possibile patrimonializzazione dei dati, si veda N. PICA, Una lettura giuspubblicistica del dibattito civilistico sulla patrimonializzazione dei dati personali in Amministrativamente.com, 2021, 3, p. 503 ss.

[20] G. E. VIGEVANI, Identità, oblio, informazioni e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano, in Federalismi.it, 2014; F. DI CIOMMO, R. PARDOLESI, Dal diritto all'oblio in internet alla tutela della identità dinamica. È la Rete, bellezza!, in Danno e resp., 2012, p. 701.

[21] L. TULLIO, Tracce evolutive del "Right to be forgotten" tra esigenze di anonimato e richieste di deindicizzazione, cit., p. 113-114.

ISSN 2036-7821

pubblicistico alla conformità dei trattamenti rispetto al Regolamento che diventa, insieme alle autorità di controllo, parte del sistema di governance della società digitale[22].

Sotto questo profilo lo spostamento dei dati e delle informazioni sulla rete genera difficoltà connesse ai limiti dei confini nazionali al cospetto di fenomeni globali[23]. La concorrenza di princìpi, valori, diritti (umani), il pluralismo delle fonti e delle giurisdizioni genera difficoltà per l'individuazione e l'applicabilità delle regole e per la risoluzione delle controversie[24].

La pubblica amministrazione è però interessata dal GDPR anche in qualità di possibile titolare del trattamento e quindi di complesso di soggetti che devono rispettare la disciplina della gestione dei dati, seppur soggiacendo ad un regime giuridico che tiene conto delle loro peculiarità. Il GDPR sancisce la liceità dei trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e i soggetti pubblici soggiacciono alle norme speciali dettate appositamente per loro ma restano anche soggetti all'applicazione degli obblighi generali cui sono assoggettati i titolari di trattamento privati[25].

Alla luce di quanto affermato diventa necessario comprendere quali sono i limiti di esercizio del diritto all'oblio quando i dati dell'interessato sono trattati in ragione dell'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri. Fermo restando il possibile ruolo esercitato dal consenso, anche in presenza di trattamenti da parte della pubblica amministrazione[26], già in vigenza del precedente regime giuridico è stato evidenziato in dottrina che la liceità del trattamento da parte di soggetti pubblici è connessa alla predeterminazione delle finalità del trattamento e alle norme attributive di competenze e deve essere connessa all'identificazione dei fini sottesi di volta in volta al trattamento e può quindi in

[22] Si veda sul punto F. PIZZETTI, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, cit., p. 51. Per una considerazione dell'impatto delle nuove tecnologie sul funzionamento dei sistemi democratici, si veda C. COLAPIETRO, Libera manifestazione del pensiero, fake news e privacy, oggi, in dirittifondamentali.it, 2022, 2, p. 422 ss.

[23] Per una disamina delle problematiche sottese alle difficoltà degli Stati nel mondo informatizzato e globalizzato e delle loro prospettive in termini di ruolo e di capacità di intervento, si veda L. CASINI, Lo Stato nell'era di Google, Firenze, 2020. Per una riflessione sul ruolo della cooperazione internazionale al fine di rendere maggiormente effettivo il diritto all'oblio si veda J. CIANI SCIOLLA, Diritto all'oblio e cooperazione internazionale: problemi e prospettive, in Riv. It. Inf. e dir., 1, 2022, p. 157.

[24] L. TULLIO, Tracce evolutive del "Right to be forgotten" tra esigenze di anonimato e richieste di deindicizzazione, cit., p. 115.

[25] S. D'ANCONA, Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo, in Riv. it. dir. pubbl. com., 3, 2018, p. 4.

[26] Per il rilievo del consenso e della funzione nei trattamenti da parte della pubblica amministrazione si veda G. CARULLO, Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa, Torino, 2017, p. 48 e ss.

ISSN 2036-7821

alcuni casi legittimamente prescindere dal consenso[27]. L'art. 24 deI D. Lgs. 196/2003, oggi abrogato, aveva poi specificato che la condizione di liceità prevista dall'art. 6, par. 3 – base giuridica individuata dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del Trattamento - potesse essere costituita, per quanto concerne il diritto nazionale da una norma di legge o, nei casi previsti dalla legge, di regolamento, mentre l'art. 6 GDPR è più generico, facendo riferimento al diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento[28].
I trattamenti che trovano la propria legittimazione nel perseguimento di un interesse pubblico o nell'esercizio di un pubblico potere sono affiancati da un regime particolare che viene organicamente definito e concluso dal regime delle eccezioni all'esercizio del diritto di oblio, che non si applica ai trattamenti necessari al perseguimento dell'interesse pubblico, ogni qualvolta essi siano stati legittimamente posti in essere e rispondano dunque ai principi previsti dal Regolamento e dal codice, primi fra tutti il principio di pertinenza, di limitazione delle finalità e di conservazione per un tempo non superiore a quanto necessario per il raggiungimento delle finalità. E' stato in proposito correttamente affermato che, anche quando la base di liceità di un trattamento sia costituita da un obbligo legale o dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri vale la condizione di necessità del trattamento e il trattamento risulta quindi non lecito se il fine poteva essere raggiunto senza il trattamento di dati personali, tanto che la disciplina del diritto di opposizione consente all'interessato di pretendere che il titolare del trattamento si astenga dal trattare ulteriormente i propri dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per

[27] In questo senso, C. MUCIO, Il diritto alla riservatezza nella pubblica amministrazione: dati sensibili, dati personali e diritto di accesso, Milano, 2003, p. 45. Pur se l'Autore avverte altresì che la sola norma non è di regola sufficiente, dovendo la stessa essere poi specificata per l'identificazione dei fini sottesi di volta in volta al trattamento. Per un'opinione concorde ma successiva al GDPR si veda G. CARULLO, Diritto all'oblio e dovere di provvedere delle pubbliche amministrazioni, cit., p. 172. M. DELL'UTRI, Principi generali e condizioni di liceità del trattamento dei dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), I dati personali nel diritto europeo, Torino, 2019, p. 221 ss. distingue efficacemente la legittimazione "contrattuale" al trattamento da quella "legale".

[28] M. DELL'UTRI, Principi generali e condizioni di liceità del trattamento dei dati personali, cit., p. 223 sottolinea che la genericità dell'espressione contenuta nel GDPR non contraddice però la previsione del codice italiano e che dunque il fondamento delle prerogative di indole pubblicistica potrebbe rinvenirsi comunque in norme primarie o secondarie, con la sola esclusione dei provvedimenti amministrativi a causa del difetto di generalità e astrattezza che ne connota la fattispecie. G. CARULLO, Diritto all'oblio e dovere di provvedere delle pubbliche amministrazioni, cit., p. 173 afferma che «in tal modo viene a configurarsi un potere di tipo autoritativo, in quanto idoneo ad incidere unilateralmente nella sfera giuridica altrui. Il soggetto – pubblico o privato – a ciò autorizzato dalla legge in vista di un interesse pubblico, ovvero nell'esercizio di un pubblico potere, può trattare dati personali indipendentemente dal consenso dell'interessato. In altre parole, sulla base di tale disposizione l'amministrazione, nell'esercizio dei propri poteri autoritativi, può procedere al trattamento di dati personali anche indipendentemente dall'eventuale diverso volere del soggetto interessato e, per converso, in capo a quest'ultimo, non residua alcun margine di apprezzamento circa il rilascio del consenso, in quanto non richiesto».

ISSN 2036-7821

procedere al trattamento, con conseguente dovere di provvedere senza ingiustificato ritardo da parte del titolare del trattamento[29].

3. Poteri e ruolo del garante nel mondo globalizzato

Come noto i compiti affidati all'autorità di controllo italiana, il Garante per la protezione dei dati personali, dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101, sono molteplici e sono poteri, oltre che consultivi e di segnalazione, di indagine, controllo, ammonimento, ingiunzione, prescrizione e imposizione[30]. Il garante può inoltre adottare linee guida e comminare sanzioni pecuniarie[31].

Di particolare interesse per il tema oggetto di analisi sono i poteri sanzionatori del garante e i meccanismi di tutela amministrativa previsti dal GDPR, che si sommano agli strumenti di tutela giurisdizionale.

Il Regolamento, alla ricerca di una tutela effettiva dell'interessato, individua in suo favore una forma di tutela amministrativa dinanzi all'Autorità di controllo per trattamenti dei propri dati effettuati in violazione del Regolamento stesso; una tutela giursdizionale azionata per far valere un diritto riconosciuto dal Regolamento e una tutela giurisdizionale che si potrebbe definire "di garanzia", azionabile contro le decisioni dell'Autorità di controllo, costituzionalmente necessaria[32]. Il diritto di proporre reclamo ad un'Autorità pubblica, indipendente, istituita da uno Stato Membro -nel caso dell'Italia il Garante- è di fatto una forma di tutela aggiuntiva e non sostitutiva di quelle già previste a tutela delle posizioni giuridiche

[29] G. CARULLO, Diritto all'oblio e dovere di provvedere delle pubbliche amministrazioni, cit., p. 174.

[30] Per una disamina dei principali problemi connessi ai poteri delle autorità amministrative indipendenti, ex multis, F. MERLONI, Fortuna e limiti delle c.d. Autorità Amministrative Indipendenti, in Pol. Dir., 1997, p. 639 ss.; F. ZAMMARTINO, Le Autorità Amministrative Indipendenti: aspetti, problematiche e nuove prospettive, in dirittifondamentali.it, 1, 2020. Per l'analisi dei singoli poteri si rinvia a R.TOMEI, I poteri conoscitivi delle Autorità amministrative indipendenti, in Riv. Amm., 2005, p. 310 ss.; G. ALPA, I poteri regolamentari delle Autorità Amministrative Indipendenti, in S. AMBROSINO, G. MORBIDELLI E M. MORISI (a cura di), Istituzioni, mercato, democrazia. Liber amicorum per gli 80 anni di Alberto Predieri, Torino, 2002, p. 13; S. SCREPANTI, La partecipazione ai procedimenti regolatori delle Autorità Indipendenti, in Riv. trim dir. pubbl., 2007, p. 377 ss.;. Per una disamina dei poteri delle autorità di controllo e del loro contenuto cfr. E. GUARDIGLI, Le autorità di controllo: dalla direttiva 95/46/CE al Regolamento n. 679/2016, in G. FINOCCHIARO (a cura di), La protezione dei dati personali in Italia, Bologna, 2019, p. 678.

[31] E.A. MATARAZZO, L'aspetto sanzionatorio della nuova legge sulla privacy, in Stato civ. it., 2018, 12, p. 57 ss.; D. TROMBINO, Il GDPR verso il suo primo anno di vita. Informativa, trasferimento transnazionale e sanzioni, in Disc. comm. serv., 2019, 2, p. 43 ss.; B. BORRILLO, La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR, in dirittifondamentali.it, 2020, 2, 328 ss.

[32] R. GIORDANO, La tutela amministrativa e giurisdizionale dei dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), I dati personali nel diritto europeo, Torino, 2019, p. 1002.

ISSN 2036-7821

nell'ordinamento e, anche per ovviare ai rischi che connessi all'esercizio di alcuni poteri delle autorità amministrative indipendenti, è possibile che sulle decisioni del Garante o quando il Garante, benché sollecitato, non tratti il reclamo o non informi l'interessato nei tempi previsti dello stato e dell'esito del reclamo, intervenga dell'autorità giurisdizionale nazionale competente.

Mentre le sanzioni penali restano di competenza dello Stato, per quanto concerne invece le sanzioni amministrative[33], il Regolamento UE 2016/679, con un cambio di passo e un rafforzamento della protezione nei confronti dei trattamenti illeciti, introduce un sistema sanzionatorio che individua le possibili violazioni, stabilendo condizioni, ammontare e modalità di irrogazione delle sanzioni in modo estremamente specifico e se, da un lato, guarda alla tutela dell'interessato attraverso sanzioni adeguate, dall'altro, mira a «*sanzionare in modo rigoroso i trattamenti illegittimi nell'interesse della collettività*»[34]. In questo modo al Garante viene riconosciuto un ampio margine di discrezionalità nella valutazione della fattispecie concreta e nell'applicazione della sanzione che, pur dovendo avere una capacità dissuasiva, deve ovviamente rispettare sempre il principio di proporzionalità e deve essere esercitato con una particolare attenzione al procedimento di irrogazione delle sanzioni, che deve essere caratterizzato da una forte garanzia del contraddittorio[35].

Il potere sanzionatorio deve però essere esercitato applicando svariati parametri di applicazione: alcuni come natura, gravità, durata della violazione, categorie di dati personali coinvolte dalla violazione, sono connessi alle caratteristiche della violazione; altri, come oggetto, natura e finalità del trattamento, sono connessi alle caratteristiche del trattamento; altri, come numero degli interessati lesi dal danno, livello di danno subito, riguardano l'impatto della violazione; altri ancora come il carattere doloso o colposo della violazione, concernono l'elemento psicologico della condotta sanzionata; infine deve essere considerata la presenza di precedenti violazioni commesse dal titolare o dal responsabile del trattamento e il rispetto o meno dell'obbligo di notifica della violazione da parte del titolare o del responsabile del trattamento[36].

---

[33] Sui caratteri della sanzione amministrativa si vedano A. TRAVI, Sanzioni amministrative e pubblica amministrazione, Padova, 1983; M. A. SANDULLI, Le sanzioni amministrative pecuniarie, Napoli, 1983; F. PELLIZZER- E. BURANELLO, Disciplina delle sanzioni amministrative ed ambito di applicazione, in A. CAGNAZZO-S. TOSCHEI (a cura di), Le sanzioni amministrative. Principi generali, Milano, 2012, 3 ss. e più di recente G. MARTINI, Potere sanzionatorio della P.A. e diritti dell'uomo, Napoli, 2018.

[34] Così, S. ANTONIAZZI, Le sanzioni amministrative, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), I dati personali nel diritto europeo, Torino, 2019, p. 1098-1099.

[35] Per una disamina sistematica della disciplina delle sanzioni, dei procedimenti e della relativa tutela giurisdizionale, R. TITOMANLIO, Funzione di regolazione e potestà sanzionatoria in M. FRATINI (a cura di), Le sanzioni delle Autorità Amministrative Indipendenti, Milano, 2011, p. 23 ss.; R. CHIEPPA, Poteri esercitati, procedimento e contraddittorio davanti alle Autorità, Padova, 2010, p. 12.

[36] Così, S. ANTONIAZZI, Le sanzioni amministrative, cit., p. 1100, che specifica come, in caso di pluralità di violazioni per uno stesso trattamento, si applica la sanzione prevista per la violazione più grave.

ISSN 2036-7821

L'art. 83, comma 7, prevede poi che gli ordinamenti nazionali possano prevedere norme che incidono sulla possibilità di infliggere sanzioni amministrative pecuniarie alle autorità e agli orgnaismi pubblici nazionali.
In realtà il sistema sanzionatorio appena tratteggiato a grandi linee, nonostante la sensibilità delle Autorità garanti, continua a essere pensato in funzione di soggetti e mercati tradizionali e mostra vistosi limiti che non gli consentono di tutelare adeguatamente diritti e interessi individuali, collettivi e pubblici da soggetti privati operanti sulla rete in condizione di autonomia e indipendenza dai poteri pubblici e connotati da una grande concentrazione di potere[37]. Benché i nuovi diritti come il diritto all'oblio abbiano contribuito a erodere l'irresponsabilità di alcuni soggetti come le piattaforme, attenta dottrina ha osservato che il GDPR dovrebbe «*regolare le grandi aziende del web e i loro comportamenti per prevenire possibili violazioni della privacy delle persone, attraverso un uso disinvolto nel trattamento dei dati posseduti e archiviati*» ma, di fatto, «*poiché i cd. giganti globali dell'informazione online padroneggiano il complesso ambiente normativo, che invece penalizza le piccole aziende indigene schiacciate dal peso della burocrazia imposta dal GDPR*» finisce con l'avvantaggiare i colossi della rete[38].
Per questo oggi il legislatore europeo sta intervenendo con nuovi strumenti, relativi ai mercati digitali, ai servizi digitali e all'intelligenza artificiale, che dovrebbero integrare in modo più efficace il quadro di tutela al servizio delle persone[39].

4. La proporzionalità degli strumenti di tutela tra privacy e libertà di informazione
Allorché ci si sposti sull'analisi degli strumenti di tutela, la ricostruzione degli orientamenti giursprudenziali, a partire da quelli della Corte Costituzionale, palesa chiaramente che sia il principio generale di *proporzionalità* che orienta la configurazione di questi. Come si cercherà di evidenziare nella prosecuzione dell'indagine, questo principio opera in due prospettive. Da un lato, deve guidare la

[37] In questo senso L. TORCHIA, I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale, in Riv. Trim. Dir. Pubbl., 4, 2022, p. 1101 ss., cui si rinvia anche per una suggestiva lettura del significato dell'esercizio dell'autoregolazione da parte delle piattaforme.
[38] T. E. FROSINI, L'orizzonte giuridico dell'intelligenza artificiale, in Dir. Informazione e Informatica, 1, 2022, p. 5.
[39] Per una disamina delle implicazioni della patrimonializzazione dei dati, si veda N. PICA, Una lettura giuspubblicistica del dibattito civilistico sulla patrimonializzazione dei dati personali in Amministrativamente.com, 2021, 3, p. 500 ss. Per un approfondimento sul Digital Markets Act, si vedano G. BRUZZONE, Verso il Digital Markets Act: obiettivi, strumenti e architettura istituzionale, in Riv. reg. mercati, 2022, p. 323 ss.; A. MANGANELLI, La proposta di regolamento EU per i mercati digitali: ratio, criticità e prospettive di evoluzione, in Mercato conc. reg., 2021. Per un approfondimento sulla regolamentazione in materia di intelligenza artificiale, si vedano E. CHITI E B. MARCHETTI, Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale, in Riv. reg. mercati, 2020, p. 29 ss.; C. CASONATO E B. MARCHETTI, Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale, in BioDiritto, 2021; F. RODI, Gli interventi dell'Unione europea in materia di intelligenza artificiale e robotica: problemi e prospettive, in G. ALPA (a cura di), Diritto e intelligenza artificiale, Pisa, 2020, p. 187 ss. Più in generale si veda M. MIDIRI, Le piattaforme e il potere dei dati (Facebook non passa il Reno), in Dir. Informazione e Informatica, 2021, 2, p. 111 ss.

ISSN 2036-7821

scelta applicativa degli strumenti di tutela, affinché il diritto all'oblio sia contemperato con le libertà costituzionali di manifestazione del pensiero e di stampa, nelle diverse declinazioni che possano assumere, soprattutto nei media digitali, ovvero, con riferimento alle pubbliche amministrazioni, con i principi di trasparenza e publicità. Dall'altro, secondo l'interpetazione della giurisprudenza europea (e, di riflesso, presso le corti nazionali), opera per l'individuazione dei confini territoriali di efficacia degli strumenti di tutela, siano essi amministrativi o giurisdizionali.

In ordine alla perimetrazione dell'incisività degli strumenti di tutela, si può muovere dalla decisione n. 20/2019 della Corte Costituzionale, che approfondisce il rapporto tra diritto all'oblio e gli obblighi di trasparenza amministrativa[40]. Nel dichiarare incostituzionale l'obbligo di pubblicare on-line i dati personali sul reddito e sul patrimonio dei dirigenti pubblici diversi da quelli che ricoprono incarichi apicali, la decisione ha ribadito il fondamento costituzionale del diritto alla riservatezza dei dati personali, declinato come risvolto della manifestazione del diritto fondamentale all'intangibilita` della sfera privata, protetto negli artt. 2, 14 e 15 Cost. Inoltre, la decisione ricostruisce minuziosamente la specifica protezione che si ritrova in alcune norme sovranazionali, quali gli artt. 8 della CEDU e gli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione europea, quali disposizioni che «stabiliscano principi di proporzionalità, pertinenza e non eccedenza nel trattamento dei dati personali»[41].

[40] Sul portato della sentenza n. 20/2019, cfr., ex multis, B. PONTI, Il luogo adatto dove bilanciare. Il "posizionamento" del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019, in Le istituzioni del federalismo, 2/2019, p. 525; R. PINARDI E S. SCAGLIARINI, Riflessioni a partire dalla vicenda del "bonus Covid" in favore dei titolari di cariche pubbliche: quale bilanciamento tra privacy e trasparenza?, in federalismi.it, 14/2021, p.139ss.; S. SCAGLIARINI, La tutela della privacy e dell'identità digitale nel qudro dell'evoluzione tecnologica, in Consultaonline, II/2021, p.489. Come è noto, la Corte, sin dalla sentenza n. 139 del 1990, con riferimento ai dati raccolti a fini statistici, ha ricondotto la funzione della tutela della riservatezza e della protezione dei dati personali al «prevenire qualsiasi rischio che i dati raccolti siano conosciuti all'esterno nel lororiferimento nominativo o individuale ovvero in modo tale che siffatto riferimento possa esser ricostruito pur in presenza di dati anonimi e/o aggregati. Lo scopo di tale principio è duplice, in quanto, senza siffatte garanzie, da un lato, le statistiche potrebbero risultare non veridiche e, dall'altro lato, potrebbero essere messi in pericolo beni individuali strettamente connessi al godimento di libertà costituzionali e, addirittura, di diritti inviolabili». Con la sentenza n. 271 del 2005, che si riferisce alla disciplina organica dettata dal d.lgs. n. 196 del 2003, la Corte argomenta che questa disciplina, «tende a tutelare per la prima volta in modo organico il trattamento dei dati personali…qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione».

[41] La decisione, come è noto, ha dato alla Corte l'occasione anche per ribadire il suo orintamento già espresso nella decsione n. 269 del 2017, in ordine ai rapporti dell'ordinamento interno con la Carta di Nizza, affermando che «i principi e i diritti enunciati nella CDFUE intersecano in larga misura i principi e i diritti garantiti dalla Costituzione italiana (e dalle altre Costituzioni nazionali degli Stati membri), e che la prima costituisce pertanto «parte del diritto dell'Unione dotata di caratteri peculiari in ragione del suo contenuto di impronta tipicamente costituzionale…in tali fattispecie, la Corte costituzionale giudicherà alla luce dei parametri costituzionali interni, ed eventualmente anche di quelli europei (ex artt. 11 e 117, primo comma, Cost.), comunque secondo l'ordine che di volta in volta risulti maggiormente appropriato. Questo orientamento va confermato anche nel caso di specie,

ISSN 2036-7821

La Corte ha trovato l'occasione di chiarire che nell'era digitale il diritto alla riservatezza si evolve da «manifestazione del diritto fondamentale all'intangibilità della sfera privata» e si configura «quale diritto a controllare la circolazione delle informazioni riferite alla propria persona, e si giova, a sua protezione, dei canoni elaborati in sede europea per valutare la legittimità della raccolta, del trattamento e della diffusione dei dati personali». Questi criteri sono ritrovati nei «già ricordati principi di proporzionalità, pertinenza e non eccedenza, in virtù dei quali deroghe e limitazioni alla tutela della riservatezza di quei dati devono operare nei limiti dello stretto necessario, essendo indispensabile identificare le misure che incidano nella minor misura possibile sul diritto fondamentale, pur contribuendo al raggiungimento dei legittimi obiettivi sottesi alla raccolta e al trattamento dei dati». Cosi, «I diritti alla riservatezza e alla trasparenza si fronteggiano soprattutto nel nuovo scenario digitale: un ambito nel quale, da un lato, i diritti personali possono essere posti in pericolo dalla indiscriminata circolazione delle informazioni, e, dall'altro, proprio la più ampia circolazione dei dati può meglio consentire a ciascuno di informarsi e comunicare». Nella prospettiva del bilanciamento tra più ampia circolazione delle informazione, da un lato, e diritto a controllare la circolazione delle proprie informazioni, dall'altro, secondo la Corte la valutazione delle norme interne deve essere svolta con un giudizio ragionevolezza che «si avvale del cosiddetto test di proporzionalità, che richiede di valutare se la norma oggetto di scrutinio, con la misura e le modalità di applicazione stabilite, sia necessaria e idonea al conseguimento di obiettivi legittimamente perseguiti, in quanto, tra più misure appropriate, prescriva quella meno restrittiva dei diritti a confronto e stabilisca *oneri non sproporzionati* [corsivo di chi scrive] rispetto al perseguimento di detti obiettivi». In definitiva, secondo la Corte, la disciplina europea, pur riconoscendo un ampio margine di regolazione autonoma e di dettaglio agli Stati membri con riguardo a certe tipologie di trattamento, impone loro il principio di proporzionalità del trattamento». Le consegnuenze delineate dalla Corte sono particolarmente rilevanti in ordine all'attività dei motori di ricerca su internet, oggetto più specifico delle riflessioni che seguiranno: le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»; gli obblighi di pubblicazione (ai sensi della disciplina sulla trasparenza amministrativa) dei dati personali "comuni", diversi dai dati sensibili e dai dati giudiziari, comportano la loro diffusione attraverso siti istituzionali, «nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i

nel quale principi e diritti fondamentali enunciati dalla CDFUE intersecano, come meglio si chiarirà, principi e diritti fondamentali garantiti dalla Costituzione».

ISSN 2036-7821

motori di ricerca web, e anche il loro riutilizzo, nel rispetto dei principi sul trattamento dei dati personali».

La precisazione dei contenuti, dell'estensione, dei soggetti destinatari delle diverse misure di tutela del diritto all'oblio, si è definita nel tempo grazie all'evoluzione della giurisprudenza ordinaria, facendo evolvere le tecniche di tutela tradizionali nell'era digitale[42].

Con la decisione n. 5525 del 2012, la Corte di Cassazione affronta il tema della pubblicazione online delle notizie e della loro *permanenza* nella rete internet (ed in particolare negli "archivi digitali", disponibili ancora online, delle testate giornalistiche in formato digitale), con riferimento a specifiche notizie di stampa realative a passate vicende giudiziarie, che ne rappresentavano solo frammenti o fasi, senza dare contezza degli sviluppi successivi e conclusivi. Nonostante la piattaforma digitale della testata giornalistica tenesse distinta l'edizione quotidiana del fascicolo digitale dall'archivio delle notizie, veniva in rilievo l'*indicizzazione* dell'archivio operata dai motori di ricerca più diffusi, e quindi la facilità di diffusione di vecchie e frammentate notizie e la loro persistenza[43]. La vicenda muoveva da una Decisione del Garante del 22 Maggio 2009, che aveva respinto la richiesta di spostamento di un articolo in una sezione di un sito non indicizzata dai motori di ricerca. Da un lato, la Corte rilevava comunque la persistenza dell'interesse pubblico alla divulgazione della notizia; dall'altro, chiariva l'importanza del diritto alla riservatezza, intenso nella nuova accezione dinamica come disegnata dal Codice della privacy, che imponeva il trattamento dei dati personali in modo lecito e secondo correttezza, non eccedendo le finalità di trattamento, oltre che non conservati per un periodo di tempo non superiore a quello previsto dalle medesime finalità. Secondo la Corte,

[42] Si sottolinea, come è noto, l'importanza della sentenza n. 3679 del 1998, con cui la Cassazione, richiamando principi espressi nella sentenza n. 5259 del 1984 sulla libertà di stampa, ha ribadito innanzitutto i confini del diritto di cronaca legittimamente esercitato (la libertà di trattamento de fatti, nell'osservanza del codice deontologico), ovvero la persistenza di un interesse pubblico, inteso come l'utilità sociale dell'informazione, mutevole nel tempo, che tende a scemare con trascorrere degli anni; la pertinenza delle notizie, ovvero l'espressione della verità oggettiva o putativa dei fatti; la correttezza dell'esposizione dei fatti e della loro valutazione. La Suprema Corte si sofferma in particolare sul limite al diritto di cronaca consistente nell'attualità della notizia. Questo limite si configura come il carattere dinamico dell'interesse pubblico del fatto, che può aumentare (se ad esempio il soggetto condannato per reati politici si ricandida) o diminuire (per il trascorrere del tempo). In questa decisione il diirtto indivduale viene ricondotto propriamente alla protezione del diritto alla riservatezza. Su questi orientamenti storici, cfr., ex multis, P. LAGHEZZA, Il diritto all'oblio esiste (e si vede), in Il Foro italiano, 6/1998, 1, p. 1835; A.L. VALVO, Il diritto all'oblio nell'epoca dell'informazione "digitale", in Studi sull'integrazione europea, 2/2015, p. 347; F. AGNINO, Il diritto all'oblio e diritto all'informazione: quali condizioni per il dialogo?, in Danno e responsabilità, 1/2018, p. 104; M. MEZZANOTTE e A. R. RIZZA, La trasfigurazione del diritto all'oblio, in Consulta online, 3/2020, 1, p. 645.

[43] La decisione è stata oggetto di molte analisi. Cfr., ex multis, G. FINOCCHIARO, Identità personale su Internet: il diritto alla contestualizzazione dell'informazione, in Il Diritto dell'informazione e dell'informatica, 3/2012, p. 383; T. E. FROSINI, Il diritto all'oblio e la libertà informatica, in Il Diritto dell'informazione e dell'informatica, 4-5/2012, p. 911; M. BELLANTE, Diritto all'identità personale e obbligo di aggiornamento degli archivi storici di testate giornalistiche, in Giurisprudenza italiana, 5/2013, p. 1073.

ISSN 2036-7821

proprio il principio di correttezza era alla base di un bilanciamento degli interessi, tra il diritto di cronaca e di informazione in generale, e il diritto al rispetto della riservatezza altrui, «cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati».

Così come aveva fatto l'autorità garante, occorreva la verifica della permanenza o del rinnovamento dell'interesse pubblico alla divulgazione della notizia, per esigenze storiche, didattiche, culturali o sociali, in modo tale da modificare le finalità del trattamento originario. Tale ipotesi, sulla base dall'articolo 11, lettera b, del Codice della privacy, veniva a giustificare la conservazione del dato in un archivio avente finalità diverse (storiche) rispetto a quelle dell'originaria raccolta. La Corte precisava poi le specifiche peculiarità degli archivi digitali: «se vera, esatta ed aggiornata essa era al momento del relativo trattamento quale notizia di cronaca, e come tale ha costituito oggetto di trattamento, il suo successivo spostamento in altro archivio di diverso scopo (nel caso, archivio storico) con memorizzazione anche nella rete internet, deve essere allora realizzato con modalità tali da consentire alla medesima di continuare a mantenere i suindicati carattere di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante il relativo aggiornamento e contestualizzazione». Anche il dato personale raccolto e diffuso lecitamente per finalità di cronaca, e lecitamente mantenuto per finalità storiche, poteva connotarsi di illecietà, allorché si connotasse come incompleto, non contestualizzato, e quindi inesatto o non vero. La tecnica di tutela era così individuata nel «collegamento della notizia ad altre informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi dalla notizia originaria», al fine di garantire che la notizia fosse storicamente completa, corretta, e quindi non violi i diritti fondamentali dell'interessato. La tutela si articolava così nel diritto a conoscere chi possiede i dati, quali dati possedesse, nonché di opporsi al trattamento dei dati, «ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione».

La tecnica di tutela dell'aggiornamento e dell'integrazione iniziava a porre il problema delle sedi frammentate di permanenza della notizia nella rete internet, nell'archivio della testata editoriale, titolare del sito sorgente, e nelle altre sedi, anche estranee alla titolarità della testata, in cui i dati fossero trasmigrati in sede di archiviazione e indicizzazione.

Infatti, la Corte sobbarcava tutta la responsabilità sull'azienda editoriale, stabilendo che non spettasse al motore di ricerca procedere agli obblighi di integrazione, poiché

ISSN 2036-7821

questi dovesse configurarsi solo come un intermediario della comunicazione, disciplinato dal decreto legislativo n. 70/2003[44].

Il tema era, per la verità, già stato oggetto di attenzione da parte dell'autorità garante, a partire da un provvedimento del 18 gennnaio 2006, nel quale era stato messo in rilievo che la rettifica o cancellazione effettuata dal gestore del sito non fosse sufficiente a tutelare l'interessato, menzionando le copie cache dei siti e le relative sintesi nei campi del motore di ricerca, non aggiornate o rettificate.

Le Sezioni Unite della Corte di Cassazione, nell'evoluzione della giurispruduenza successiva, hanno avuto occasione di precisare almeno le casistiche del diritto all'oblio, sia che assumesse le forme della "deindicizzazione" dai motori di ricerca, sia che si cofigurasse come diritto alla cancellazione: «quando si parla di diritto all'oblio ci si riferisce, in realtà, ad almeno tre differenti situazioni: quella di chi desidera non vedere nuovamente pubblicate notizie relative a vicende, in passato legittimamente diffuse, quando è trascorso un certo tempo tra la prima e la seconda pubblicazione; quella, connessa all'uso di internet ed alla reperibilità delle notizie nella rete, consistente nell'esigenza di collocare la pubblicazione, avvenuta legittimamente molti anni prima, nel contesto attuale [...]; e quella, infine, trattata nella citata sentenza Google Spain della Corte di giustizia dell'Unione Europea [di cui ci si occuperà più avanti], nella quale l'interessato fa valere il diritto alla cancellazione dei dati»[45]. Sul tema, occorre osservare come gli interpreti abbiano discusso sulla omogeneità o eterogeneità del diritto alla deindicizzazione con il diritto all'oblio, pervenendo a interpetazioni diverse da quelle sostenute dalla Corte. In particolare, si osserva che con la deindicizzazione non verrebbe in rilievo nessun giudizio di liceità della pubblicazione originaria del dato[46].

---

[44] L'azienda editoriale titolare del sito, in cui era collocato l'archivio storico della testata disponibile grazie all'indicizzazione dei motori di ricerca, doveva cosi «garantire la contestualizzazione e l'aggiornamento della notizia già di cronaca oggetto di informazione e di trattamento, a tutela del diritto del soggetto cui i dati pertengono alla propria identità personale o morale nella sua proiezione sociale, nonché a salvaguardia del diritto del cittadino utente di ricevere una completa e corretta informazione».

[45] Cfr., tra le altre, Cass., sez. un. civ., sent. 22.7.2019 n. 19681. Sulla questa decisione, cfr., ex multis, S. SCAGLIARINI, op.cit., p. 499; G. CALABRESE, Il diritto alla deindicizzazione non si estende alla cancellazione delle copie ''cache'', in NGCC, 6/2022, p. 2015; G. PARDOLESI E B. SASSANI, Bilanciamento tra diritto all'oblio e diritto di cronaca: il mestiere del giudice, in Foro it., 2019, I, p. 235; G. DI CIOMMO, Oblio e cronaca: rimessa alle Sezioni Unite la definizione dei criteri di bilanciamento, in Corr. giur., 2019, p. 5.

[46] Come osserva CALABRESE, op.cit., p. 1217, le interpetazioni dottrinali prevalenti concordano nell'affermare che il diritto alla deindicizzazione non coincida con il diritto all'oblio, per quanto affini: «Infatti, tramite l'esercizio del diritto all'oblio l'interessato chiede che la notizia a sé riferibile venga cancellata dal sito web che la ospita, mentre con il diritto alla deindicizzazione chiede che venga preclusa una particolare modalità di ricerca di quella notizia, ossia quella effettuata inserendo specifiche chiavi di ricerca. Invece, la deindicizzazione è il rimedio atto ad evitare che il nome della persona sia associato dal motore di ricerca ai fatti di cui internet continua a conservare memoria; la deindicizzazione asseconda, dunque, il diritto della persona a non essere trovata facilmente sulla rete…proprio perché la notizia continuerà ad essere accessibile da chi, intenzionato realmente ad essa, porrà in essere un'attività di ricerca più articolata ed attraverso chiavi di ricerca che non contemplino il nome dell'interessato. La deindicizzazione opera, infatti, escludendo solamente le azioni di ricerca eseguite partendo

ISSN 2036-7821

In altre decisioni[47] La Cassazione ricorda che il diritto all'oblio consiste nel non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza, a causa della ripubblicazione, a distanza di un importante intervallo temporale, di una notizia relativa a fatti del passato, ma la tutela del menzionato diritto va posta in bilanciamento con l'interesse pubblico alla conoscenza del fatto, espressione del diritto di manifestazione del pensiero e quindi di cronaca e di conservazione della notizia per finalità storico-sociale e documentaristica, cosicché nel caso di notizia pubblicata sul ''web'', il medesimo puo` trovare soddisfazione anche nella sola ''deindicizzazione'' dell'articolo dai motori di ricerca.
Il tema è poi connesso, come si è visto, all'individuazione dei soggetti che possono essere destinatari di misure di tutela. Stavolta è la giurisprudenza amministrativa[48] a chiarire che non si configura la responsabilità di un gestore di una piattaforma online, o meglio di un motore di ricerca, qualificato come *hosting provider*, qualora venga su di essa pubblicato da un inserzionista un annuncio pubblicitario. La sola diffusione dei contenuti ha natura automatizzata e non comporta la manipolazione dei messaggi, venendo così a mancare il "ruolo attivo" del gestore del servizio, necessario per la configurazione di una sua responsabilità. Secondo la tipologia di servizio offerto, gli ISP sono classificati in *access provider* o *gatekeeper*, i quali forniscono, secondo varie modalità, l'accesso alle reti di comunicazioni elettroniche; *service provider*, che mettono a disposizione servizi di posta elettronica; *content provider*, fornitori di propri contenuti digitali; *mere conduit*, *caching* e *hosting provider*, che diffondono contenuti altrui.

5. La "deindicizzazione" e i suoi confini territoriali nella giurisprudenza europea e nazionale
La deindicizzazione chiama in causa non solo i diversi soggetti a cui in rete sono riconducibili gli archivi digitali e le loro "copie cache", ma anche la sede dei server di conservazione di essi. Come già accennato, nella nota sentenza Google Spain[49], la Corte di giustizia europea ha affrontato la declinazione che il diritto all'oblio possa assumere nei confronti dei motori di ricerca, configurando le specifiche

dal nome della persona, che rendano noti ambiti della vita passata di questa; si evita che gli utenti online, che ignorino il coinvolgimento della persona nelle vicende in questione (che non vengono oscurate del tutto perché potrebbero rivestire ancora un interesse attuale), si imbattano nelle relative notizie casualmente, solo perché hanno digitato il nome della persona sulla ''barra di ricerca''. Quest'ultima modalità di ricerca, in quanto notevolmente potenziata dagli algoritmi di indicizzazione e predittivi del motore di ricerca, é idonea a determinare un'ingerenza eccessiva e pregiudizievole per il diritto fondamentale al rispetto della vita privata delle persone».

[47] Cassazione civile, Sez. I, 19 maggio 2020, n. 9147.

[48] Cons. Stato, Sez. VI, sent. 18 maggio 2021, n. 3851, e prima ancora T.A.R. Lazio, Roma, Sez. III-ter, 28 ottobre 2021, n. 11036, Google Ireland Limited c. Autorità per le Garanzie nelle comunicazioni.

[49] Corte giust., sent. 13 maggio 2014, causa C-131/12. Su questa decisione, ex multis, cfr. F. BALDUCCI ROMANO, La Corte di Giustizia 'resetta' il diritto all'oblio, in federalismi.it, 3/2020, p. 31; SCAGLIARINI, op.cit.; CALAB RESE, op.cit.

ISSN 2036-7821

caratteristiche di un "diritto alla deindicizzazione". L'argomentazione della Corte muove dalla considerazione che il motore di ricerca realizzi una "rappresentazione digitale" del soggetto ricercato allorché restituisca un elenco di risultati selezionati e aggregati con le notizie relative al soggetto. Questa rappresentazione, prodotta dalla sintesi di tutte le notizie frutto di un'unica ricerca, secondo uno specifico ordine determinato dall'algoritmo del motore di ricerca, costituisce un trattamento dei dati che involge sì il diritto alla riservatezza, ma più incisivamente, secondo la Corte europea, chiama in causa il diritto all'autodeterminazione nella realtà digitale: «l'organizzazione e l'aggregazione delle informazioni pubblicate su internet, realizzate dai motori di ricerca allo scopo di faci- litare ai loro utenti l'accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa per- sona reperibili su internet, che consente loro di stabilire un profilo più o meno dettagliato di quest'ultima»[50].

La controversia ha fatto emergere l'opposizione dei gestori dei motori di ricerca, che hanno sollevato la questione dell'estensione territoriale della deindicizzazione, assumendo che i dati personali dovessero essere rimossi solo dalle ricerche effettuate nei domini internet corrispondenti allo Stato membro dell'interessato (.it, .es, e così via) e non dall'intera rete globale del motore di ricerca. Con una successiva decisione[51] la Grande Sezione della Corte ha affermato che il gestore del motore di ricerca è obbligato tendenzialemente ad eseguire la deindicizzazione solo dalle estensioni del motore di ricerca corrispondenti a tutti gli Stati membri dell'Unione. La questione si originava dall'impugnazione della sanzione pecuniaria irrogata dall'Autorità francese di protezione dei dati personali CNIL nei confronti del motore di ricerca Google per l'inottemperanza di un provvedimento con cui l'autorità, a seguito di molte istanze proposte nel 2014, disponeva che la società californiana provvedesse al *dereferencing* a livello globale, ossia su tutti i nomi di dominio del motore di ricerca.

Secondo la Corte, il trattamento dei dati da parte del motore di ricerca va ritenuto sostanzialmente unitario, poiché i vari nomi di dominio vanno intesi puramente quali percorsi tecnici di accesso a tale trattamento. Tuttavia, la deindicizzazione non potrebbe avere portata mondiale, perché l'articolo 17 del RGDP avrebbe mancato di esercitare la competenza legislativa dell'Unione, non avendo effettuato alcun bilanciamento tra diritto alla privacy e libertà di informazione degli utenti della rete «per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione».

[50] Cfr. ancora CALABRESE, op.cit., p. 1216.

[51] Sentenza del 24 settembre 2019, Google c. CNIL (Corte giust., sent. 24 settembre 2019, causa C-507/17, CNIL, autorità francese di garanzia della privacy). Sulla decdsione, cfr. BALDUCCI ROMANO, op.cit.

ISSN 2036-7821

Nella pronuncia, sulla scorta della decisione Google Spain, sembrano configurarsi differenti declinazioni di diritti all'oblio, tra loro differenti: quello europeo, avrebbe un'estensione coincidente – di default – con il territorio dell'Unione; gli altri, di stampo nazionale, sarebbero "a geometria variabile", estendendo o restringendo il proprio perimetro in misura inversamente proporzionale alle plurime libertà di informazione nazionali, anch'esse puntiformi e plasmabili dagli Stati. Secondo un orientamento recente, affermato nella decisione della Grande Sezione dell'8 dicembre 2022, in causa C-460/20, spetta al diretto interessato che richiede la cancellazione fornire la prova dell'inesattezza del contenuto del testo indicizzato.

Gli orientamenti del giudice europeo condizionano il nostro giudice nazionale, che, in prima battuta[52], accoglieva le limitazioni sostenute dalla Corte. Il giudice di uno Stato membro può, in teoria, statuire sulla rimozione delle informazioni, manifestamente illecite, diffuse a mezzo Internet a livello mondiale. Tuttavia, a causa delle differenze esistenti fra le leggi nazionali, da un lato, e la tutela della vita privata e dei diritti della personalità da esse prevista, dall'altro, e al fine di rispettare i diritti fondamentali ampiamente diffusi, un siffatto giudice deve adottare piuttosto un atteggiamento di autolimitazione. Tale autolimitazione si realizza attraverso l'applicazione del principio di proporzionalità.

Nella giursprudenza successiva, la Cassazione civile (Sez. I, 21 luglio 2021, n. 20861) afferma che in tema di diritto all'oblio, la domanda giudiziale di deindicizzazione di alcune pagine web deve contenere la precisa individuazione dei risultati della ricerca da rimuovere, sia per ragioni processuali, poiché l'atto introduttivo del giudizio esige, a pena di nullità, l'indicazione del ''petitum'' mediato, sia per ragioni sostanziali, poiché l'obbligo di intervento del ''provider'' presuppone la conoscenza da parte di quest'ultimo dell'esistenza di contenuti suscettibili di rimozione. Inoltre, è l'individuazione di detti risultati che consente al giudice di effettuare, nella singola fattispecie, il fondamentale bilanciamento tra diritto alla protezione dei dati personali e interesse pubblico all'informazione, in base ad elementi di fatto acquisiti al processo e sottoposti al contraddittorio delle parti.

E ancora[53], viene sottolineato che il diritto alla cancellazione delle copie cache, relative a una informazione accessibile tramite il motore di ricerca, diversamente dal rimedio della deindicizzazione del dato a partire dal nome della persona, esige un bilanciamento più stringente del diritto dell'interessato all'oblio con il diritto della collettività all'informazione, connessa al fatto nel suo complesso, attraverso parole chiave diverse dal nome dell'interessato.

[52] Tribunale di Milano, Sez. I, 17 giugno 2020. Su questa decisione, cfr. S. GRISANTI, Internet service providers e diffamazione in rete: una recente ordinanza del Tribunale di Milano, in Il diritto industriale, 3/2021, p. 285.

[53] Cass. Civ., I sez., 8.2.2022, n. 3952.

ISSN 2036-7821

L'ordine di cancellazione delle copie cache appare come misura esorbitante e certamente più radicale della sola deindicizzazione, in quanto non consente, o rende comunque più complesso, raggiungere la medesima notizia attraverso il motore di ricerca anche utilizzando chiavi di ricerca che non contemplino il nome dell'interessato. La disassociazione del nome della persona rispetto ai link delle pagine web è rimedio atto a tutelare l'identità personale: più precisamente, tutela l'identità digitale del soggetto e la sua libertà di autodeterminarsi sul web. L'elenco dei risultati della ricerca è idoneo, infatti, a fornire una rappresentazione online della persona a cui le notizie si riferiscono, rappresentazione che, in quanto ''trattamento di dati'', deve essere pertinente, veritiera, corretta e non deve determinare un'illecita intromissione nella sfera privata del soggetto.

La condotta dell'*Hosting provider* viene poi differenziata in "attiva" e "passiva"[54]: ai sensi dell'art. 16 del D.Lgs. n. 70/2003, il gestore di un motore di ricerca è responsabile per il contenuto delle informazioni memorizzate e diffuse in rete qualora, sebbene a conoscenza del carattere manifestamente falso e diffamatorio delle stesse, non ottemperi alla richiesta di deindicizzare le pagine web contenenti tali informazioni rispetto alla chiave di ricerca costituita dal nominativo dell'interessato. L'hosting provider può essere soggetto a differenti regimi di responsabilità a seconda dell'attività, passiva o attiva, svolta: si configura così un esonero di responsabilità ex art. 16, D.Lgs. n. 70/2003 per il caso di trattamento passivo di dati personali, da un lato; dall'altro, una responsabilità pressoché oggettiva ai sensi dell'art. 82, Reg. UE 2016/679 (incorporato dal D.Lgs. n. 196/2003) per il caso di trattamento attivo di dati personali.

Infine, nella giursprudenza più recente[55], la Cassazione, accogliendo un ricorso del Garante della privacy contro Google LLC, ha esteso globalmente l'ordine di rimozione degli URL (*Uniform Resource Locator* che identifica l'indirizzo webmail su rete), al di là dei confini nazionali ed europei, imponendo la rimozione anche nelle versioni extraeuropee del motore di ricerca. Secondo la Corte, «il diritto all'oblio si correla al diritto alla riservatezza e in questa prospettiva protegge l'interessato nella pretesa di non veder ulteriormente divulgate notizie, già legittimamente pubblicate, ma superate nel tempo che ha dissolto l'interesse pubblico alla circolazione dell'informazione». Si ribadisce ancora una volta che «occorre un bilanciamento del diritto all'oblio con il diritto alla libertà di informazione», considerando che per l'ordinamento giuridico italiano «a fronte delle modalità liquide e pervasive della circolazione dei dati sulla rete di internet, non è consentita una limitazione della tutela assicurata alla tutela della vita privata della persona». Si precisa poi che il parametro di valutazione al quale bisogna ispirarsi per il bilanciamento degli opposti

[54] Cassazione Civile, Sez. I, 8 giugno 2022, n. 18430, P.A. c. Google LLC.
[55] Cass. Civ., Sez. I, 24 novembre 2022, n. 34658.

ISSN 2036-7821

interessi è quello conforme agli standard costituzionali italiani che «legittimano di richiedere al gestore di effettuare una deindicizzazione su tutte le versioni del proprio motore, incluse quelle extraeuropee».
La condotta esigibile dal caching provider consisterà nel mutare i propri algoritmi per dissociare il nominativo del danneggiato dalle pagine internet che riportano la notizia lesiva, affinché gli utenti, nell'immettere il nominativo del danneggiato come chiave di ricerca, non possano visualizzare e venire cosı` a conoscenza o rinnovare il loro ricordo dei fatti ascritti all'interessato, non più di pubblico interesse. La tutela inibitoria contro il provider potrà anche assumere una tonalità più intensa, e la domanda giudiziale sarà cosı` caratterizzata da un diverso petitum mediato, allorquando il danneggiato chieda la eliminazione delle stesse copie chace delle pagine internet memorizzate dal provider sui propri server (al fine di rendere più veloce la visualizzazione dei risultati), di modo che nessuna interrogazione del motore di ricerca, a prescindere dalla chiave di ricerca utilizzata, possa più restituire, tra i risultati, le pagine internet riportanti la notizia lesiva. Tali pagine rimarranno bensı` accessibili al pubblico, ma solo previa digitazione dello specifico indirizzo nel browser, mentre non saranno visualizzabili tra i risultati di una interrogazione del motore di ricerca.

6. Autorità nazionali, confini nazionali e archivi digitali

La decisione n. 9782890 del 9 giugno 2022 del Autorità garante per la protezione dei dati personali consente di accennare, in conclusione, anche ad un altro indirizzo della Corte di Giustizia, in tema di limitazione della circolazione degli archivi degitali, anche quando protetta da trattati internazionali. Recentemente l'Autorità garante per la protezione dei dati personali italiana, l'Autorità austriaca e l'autorità francese hanno adottato misure per inibire l'utilizzo di "Google Analytics" in ragione dei rischi connessi al trasferimento di dati personali oltreoceano dal suolo europeo.
Tali provvedimenti seguono l'orientamento assunto dalla Corte di Giustizia nelle decisioni c.d. Schrems[56] che hanno sancito l'invalidità dell'accordo (c.d. Privacy Shield) tra Commissione europea e Stati Uniti, in base al quale i dati personali potevano liberamente transitare tra le due sponde dell'Oceano Atlantico, sulla base del capitolo V del GDPR sul trasferimento di dati verso Paesi terzi. Il Capo V del Regolamento – rubricato per l'appunto "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali" – è interamente dedicato alle tutele e alle

[56] CGUE, C 362/14, Schrems I, 2015, relativa al c.d. Safe Harbour nonché la sentenza c.d. CGUE, C-311/18, 2020, Schrems II. Sul portato delle decsioni Schrems, cfr. G. GENTILE E O. LYNSKEY, Deficient by design? The transnational enforcement of the GDPR, in ICLQ, 71/2022, p. 79; O. GSTREIN E A.J. ZWITTER, Extraterritorial application of the GDPR: promoting European values or power?, in Internet Policy Review, 10(3), 2021; C. SCARPELLINO, Un oblio tutto europeo, in Danno e responsabilità, 2/2020, p. 210.

ISSN 2036-7821

garanzie richieste per i trasferimenti in questione. Il Principio generale – ex art. 44 GDPR – dispone che tali trasferimenti sono possibili nella misura in cui «il livello di protezione delle persone fisiche garantito […] dal regolamento non sia pregiudicato». Questa disciplina, come interpretata dalla Corte, attribuisce i poteri *ad hoc* alle Autorità per poter sondare la legittimità di ciascun trasferimento nonché la congruità delle misure adottate. Come ricordato dalla sentenza Schrems II, all'Autorità del singolo Stato membro spetta «sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 del GDPR e dalla Carta, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo». Come si è visto, gli argini alla circolazione indefinita dei dati degli archivi digitali (e alla loro proteiforme riproduzione e trasformazione) possono essere molteplici e diffierenziati. Probabilmente, molti strumenti giuridici di tutela sono sempre più inefficaci. Tuttavia, solo una rete di cooperazione efficace tra autorità amministrative garanti nazionali, giudici nazionali e autorità politiche, da un lato, e i loro corrispondenti nell'ordinamento europeo, dall'altro, potrà sperimentarne di nuovi efficaci.

ISSN 2036-7821