

La tutela dell'identità nell'ambiente digitale alla luce delle norme europee

Identity protection in the digital environment in light of European Union regulations

ANTONELLA DI CERBO 

Dottoranda in Diritto Civile Università degli Studi del Sannio
Funzionaria Autorità Garante per la protezione dei dati personali

Abstract

L'evoluzione tecnologica ed i riflessi che ha avuto sulla società hanno dato luogo al sorgere di nuove istanze di tutela, che con il tempo hanno trovato posto nelle carte sovranazionali e domestiche e che tutt'oggi sono al centro dell'attività parlamentare europea ed internazionale.

Dopo un excursus sull'affermazione di nuovi diritti attraverso il processo d'integrazione europea, il presente contributo analizza l'impatto dei regolamenti in materia di protezione dei dati personali e dei servizi digitali sul diritto all'identità digitale.

Technological evolution and its effects on society have given rise to new demands for protection, which over time have found their place into supranational and domestic charters and are still the focus of european and international parliamentary activity.

After a brief examination of the affirmation of new rights through the process of European integration, this paper analyzes the impact of data protection regulations and digital services on people's right to digital identity.



Keywords: Dati personali; Regolamento 2022/2065/UE; DSA; GDPR; Regolamento 679/2016/UE; identità digitale

Summary: [Introduzione.](#) – [1. Nuove istanze di tutela e nuovi diritti.](#) – [1.1. Il riconoscimento di nuovi diritti nell'ordinamento domestico attraverso il processo d'integrazione europea.](#) – [1.2 La tutela del diritto all'identità digitale ad opera del Regolamento 2016/679/UE.](#) – [1.3 Il consenso come strumento di autodeterminazione informativa.](#) – [2. Il Regolamento 2022/2065/UE.](#) – [2.1. La responsabilità dei prestatori dei servizi.](#) – [2.2. L'affermazione del diritto \(condizionato\) di accedere all'account social.](#) – [Conclusioni.](#)

Introduzione.

Il presente contributo, formulato a titolo personale e senza alcun vincolo per l'Amministrazione di appartenenza (l'Ufficio del Garante), ha per oggetto la tutela dell'identità digitale, alla luce del nuovo quadro normativo: la disciplina del Regolamento 679/2016/UE e quella del Regolamento 2022/2065/UE.

Dallo studio dell'esperienza giuridica nazionale degli inizi del secolo scorso si registra sino agli anni settanta una tutela dell'identità della persona riferita essenzialmente ai segni distintivi, tramite il riconoscimento dei diritti al nome ed all'immagine di cui agli articoli 7 e 10 del codice civile; un'impostazione che rispondeva ad una lettura prettamente patrimoniale delle norme codicistiche ed abbandonata per lasciare spazio ad un'interpretazione costituzionalmente orientata delle stesse e fondata sulla valorizzazione della funzione sociale del diritto civile¹.

Parimenti, l'evoluzione tecnologica ed i riflessi che ha avuto sulla società ed il viver quotidiano delle persone hanno dato luogo al sorgere di nuove istanze di tutela che con il tempo hanno trovato posto nelle carte sovranazionali e domestiche e che tutt'oggi sono al centro dell'attività parlamentare del contesto europeo ed internazionale.

Le risposte legislative messe in campo sono inevitabilmente tardive: l'innovazione tecnologica è molto più rapida dell'intervento regolatore del legislatore, ciononostante è opportuno riconoscere e sottolineare che, ad oggi, la normativa europea rappresenta un modello di riferimento per tutto il mondo.

Gli atti comunitari analizzati nel presente contributo, in particolare i regolamenti in materia di protezione dei dati personali e dei servizi digitali, al

¹ P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, in Edizioni Scientifiche Italiane Spa, Napoli, 2020; P. PERLINGIERI, *La depatrimonializzazione e diritto civile*, in Rassegna di diritto civile Edizioni scientifiche italiane, Napoli, 1983; C. DONISI, *Verso la depatrimonializzazione del diritto privato*, in Rass.dir. civ. Edizioni scientifiche italiane, Napoli, 1980; P. PERLINGIERI, *La dottrina del diritto civile nella legalità costituzionale*, in Rass. dir. civ., Napoli, 2007; P. GROSSI, *La cultura del civilista italiano. Un profilo storico*, Giuffrè Editore, Milano, 2002.

pari di quanto farà il regolamento in materia di intelligenza artificiale², rientrano tra i provvedimenti normativi più innovativi per la regolazione del settore tecnologico. Al contempo, grazie alla solida architettura giuridica europea eretta sul rispetto dei diritti e delle libertà fondamentali e dell'attività dei giudici dell'Unione, unità di interconnessione tra i sistemi giuridici nazionali³, tali norme rappresentano strumenti di innalzamento della tutela in favore della persona.

1. Nuove istanze di tutela e nuovi diritti.

1.1. Il riconoscimento di nuovi diritti nell'ordinamento domestico attraverso il processo d'integrazione europea.

Il ruolo assunto dai diritti e dalle libertà affermati nella prima parte della carta costitutiva ha portato al riconoscimento, tramite l'articolo 2 della costituzione di nuovi diritti, tra cui il diritto alla protezione dei dati personali ed il diritto alla riservatezza, con ciò rivelando un'incredibile lungimiranza dei padri costituenti.

Si tratta di situazioni giuridiche sancite dalle carte sovranazionali, in primis dalla Convenzione europea dei diritti dell'uomo, che afferma il diritto di ogni persona "al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza" e, a livello europeo, dalla Carta di Nizza, ove i diritti in argomento, sono disciplinati dagli articoli 7 ed 8 e costituiscono, a seguito del Trattato di Lisbona, il parametro di riferimento costituzionale in materia di diritti fondamentali nel contesto unionale.

Nell'ordinamento interno tali norme vengono astrattamente collocate tra la Costituzione e le leggi ordinarie, assumendo i connotati ed il valore delle norme interposte ed integrando la carta costitutiva, con la conseguenza che la loro osservanza è imposta sia al legislatore sia ai giudici nazionali, che sono tenuti a disapplicare le disposizioni domestiche in contrasto con l'acquis comunitario, favorendo la realizzazione della tutela multilivello dei diritti a cui tende il processo d'integrazione europea. Dai primi anni 90 la Corte di Giustizia è altresì giunta ad affermare che, al pari del giudice, tutte le amministrazioni nazionali hanno l'obbligo di applicare le disposizioni di una direttiva⁴.

Ciò avviene in quanto, diversamente dagli obblighi di diritto internazionali, quelli derivanti dalla normativa comunitaria, non necessitano di un atto di recepimento da parte degli Stati membri, specie se si tratta di atti immediatamente esecutivi come i regolamenti e le direttive self executing⁵.

² Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 06.03.2024 (In attesa di pubblicazione in Gazzetta Ufficiale).

³ O. POLLICINO, *Costruendo le tradizioni dei diritti in Europa: il senso di un gerundio, e di un seminario*, Seminario annuale di diritti comparati, Macerata, 2015

⁴ Corte di Giustizia (C103/88), 22.6.1989 in in *Eur-Lex*;

⁵ Corte di Giustizia (C193/91), 25.05.1993, in *Eur-Lex*; Corte di Giustizia (C6/90 e C 9/90), 19.11.1991, in *Eur-Lex*.

L'efficacia obbligatoria delle norme comuni nell'ordinamento interno è stata resa possibile alla luce dell'articolo 11 della costituzione, seppur in assenza di un espresso riferimento alla realtà comunitaria, ed è divenuta concretamente esecutiva tramite la formulazione delle dottrine del primato del diritto dell'Unione e dell'effetto diretto ad opera della Corte di giustizia dell'Unione europea.

La legittimità del ricorso all'articolo 11 della costituzione, per giustificare le cessioni di sovranità, rappresenta ancora oggi una questione controversa. La dottrina prevalente ritiene che il processo di creazione dell'Unione e la redazione della carta fondamentale dell'ordinamento italiano siano parte del medesimo progetto giuridico: la costituzione del 1948 nasce nello stesso spirito e nella stessa epoca in cui sono piantati i primi semi dell'unione europea (CECA). Mentre la dottrina minoritaria⁶ ritiene che dai lavori preparatori dell'Assemblea costituente e da una lettura fedele del testo dell'articolo 11, che contempla limitazioni di sovranità da parte dell'ONU al sol fine di creare meccanismi di risoluzione delle controversie idonei a disinnescare, ex ante, il rischio di futuri contrasti mondiali, sia chiaro che il ricorso alla norma in argomento sia frutto di una manipolazione interpretativa.

La Corte costituzionale ha da tempo accolto il primo orientamento riconoscendo all'articolo 11 il fine di "porre le fondamenta di una unione sempre più stretta tra i popoli europei", diretta "ad assicurare mediante un'azione comune il progresso economico e sociale dei loro paesi, eliminando le barriere che dividono l'Europa", e ciò nel preciso intento di "rafforzare le difese della pace e della libertà, facendo appello agli altri popoli d'Europa, animati dallo stesso ideale, perché si associno al loro sforzo", nonché di "confermare la solidarietà che lega l'Europa ai paesi d'oltremare, desiderando assicurare lo sviluppo della loro prosperità conformemente ai principi dello Statuto delle Nazioni Unite"⁷.

La norma in argomento è ancora oggi invocata per consentire le limitazioni introdotte dai trattati comunitari relativamente all'attività legislativa, amministrativa e giurisdizionale, non essendo mai intervenuta una riforma costituzionale in tal senso.

La carta fondamentale italiana è aperta all'Europa e la Corte costituzionale, in quanto garante, è tenuta a garantire il rispetto anche delle norme europee⁸.

Il processo d'integrazione europeo avviato da tali premesse è stato favorito dall'elaborazione delle dottrine di matrice giurisprudenziale del primato del diritto dell'Unione europea e dell'effetto diretto; la Corte di giustizia, sin dall'inizio del processo di interpretazione del diritto dell'Unione, ha ritenuto fondamentale conferire un ruolo di primo piano al diritto europeo escludendo deroghe statali.

Nel corso del lungo cammino comunitario la Corte costituzionale ha però affermato che la prevalenza del dettato comunitario non è senza limiti,

⁶ G. PALMA, *L'incompatibilità tra costituzione italiana e trattati dell'unione europea. I principali aspetti di criticità*, 2015, in *Diritto.it*

⁷ Corte Cost. 18.12.1973, n.183, pag.3, in il *Foro Italiano*.

⁸ Corte costituzionale, *I diritti fondamentali nell'ordinamento giuridico comunitario e negli ordinamenti nazionali*, 2017, in Servizio studi della Corte costituzionale. Consultabile online: https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_306_Diritti_fondamentali_2017.pdf

precisando che, i giudici nel garantire la piena applicazione del diritto europeo devono tener conto dei limiti posti dai principi propri del tessuto della carta costituyente: i principi fondamentali, che costituiscono controlimiti alle limitazioni di sovranità e che sono sottratti alla procedura di revisione costituzionale. Limitazioni di sovranità e controlimiti segnano lo spazio dell'unificazione giuridica europea consentita dalla costituzione italiana⁹.

1.2. La tutela del diritto all'identità digitale ad opera del Regolamento 2016/679/UE.

Il progressivo cambio del paradigma condotto attraverso la valorizzazione dei diritti e delle libertà fondamentali ha consentito un notevole accrescimento della portata del diritto all'identità personale, in linea con le nuove istanze di tutela che la rivoluzione tecnologica ha prodotto nel tempo.

Le nuove tecnologie hanno profondamente modificato il viver quotidiano e le relazioni sociali, creando uno spazio virtuale in cui la persona è frammentata in molteplici identità. La Rete da mezzo è divenuto mondo, orizzonte prevalente dell'agire umano in cui si iscrivono le coordinate della vita pubblica e privata¹⁰.

In tale contesto il diritto alla protezione dei dati personali rappresenta il principale strumento di tutela di cui dispone la persona per avere il controllo delle proprie informazioni, scegliere quali parti di sé rendere note alla generalità dei consociati e ricomporre l'io diviso per avere una rappresentazione della sua persona nella sua integrità¹¹.

La normativa in materia di protezione dei dati personali di derivazione comunitaria è stata introdotta nell'ordinamento nazionale mediante la Direttiva n.95/ 46, oggi sostituita dal Regolamento europeo, sostituzione che ha reso necessaria, ad opera del d.lgs n.101/2018, una revisione del codice della privacy.

Gli articoli da 15 a 22 del Regolamento in argomento attribuiscono all'interessato il diritto di accedere alle proprie informazioni, di chiederne la rettifica, di opporsi al trattamento dei dati personali ovvero, laddove sussistano i presupposti, di ottenere la cancellazione dei suoi dati. L'articolo 22 prevede altresì il divieto, derogabile solo nei casi previsti dal paragrafo 2 della stessa norma, di trattare dati personali per adottare decisioni completamente automatizzate.

⁹ Corte costituzionale, *Le limitazioni della sovranità statale in favore dell'Unione europea nella giurisprudenza costituzionale. Il sistema delle fonti*. in Servizio studi della Corte costituzionale. 2014. Consultabile online: https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_262.pdf; R. BIN, *È scoppiata la "terza guerra tra le Corti"? A proposito del controllo esercitato dalla Corte di cassazione sui limiti della giurisdizione*, in *Federalismi.it*, 2020; M. CARTABIA, *"Unità nella diversità": il rapporto tra la Costituzione europea e le Costituzioni nazionali*, in *Il diritto dell'Unione europea*, n. 3, 2005; A. LO CALZO, *"Dagli approdi giurisprudenziali della Corte costituzionale in tema di controlimiti alle recenti tendenze nel dialogo con le Corti nel contesto europeo"*, in *Federalismi.it*, 2022.

¹⁰ A. SORO, *Intervento del Presidente Antonello Soro, Presidente dell'Autorità Garante per la privacy I confini del digitale*, Atti del convegno *I confini del digitale. Nuovi scenari per la protezione dei dati*, Roma, 2019. Consultabile online: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9078531>

¹¹ S. RODOTÀ, *Una costituzione per Internet?*, *Politica del diritto*, Fascicolo 3, in *Il Mulino – Rivistaweb.*, 2010

Si tratta di diritti che offrono una tutela in forma specifica in un'ottica di valorizzazione del principio di autodeterminazione informativa e la cui violazione consente l'esercizio dei poteri correttivi da parte dell'autorità di controllo di cui all'articolo 58, par. 2, del Regolamento, che consistono nella possibilità di rivolgere al titolare o al responsabile avvertimenti, ammonimenti, ovvero di ingiungere loro di soddisfare le richieste dell'interessato di esercitare i diritti, di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine e di comunicare all'interessato una violazione dei dati personali. L'autorità ha altresì i poteri di imporre una limitazione provvisoria o definitiva al trattamento, ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento, revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a infliggere una sanzione amministrativa pecuniaria, nonché di ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Al netto della tutela rimediabile, l'intero impianto normativo del Regolamento generale in materia di protezione dei dati personali garantisce la tutela della persona attraverso obblighi che incombono sul titolare in via preventiva e che sono modellati sulle specifiche attività di trattamento che svolge, quindi sui rischi specifici derivanti dalle stesse, in virtù del principio di accountability di cui all'articolo 5, par. 2, del Regolamento. Ne consegue che il titolare è tenuto a strutturare le attività che coinvolgono i dati personali in modo da assicurare, sin dalla progettazione e per impostazione predefinita, il rispetto dei principi generali e delle norme fissate dalle discipline europea e nazionale.

Tramite un approccio sostanzialistico di tipo preventivo il regolamento favorisce l'adozione di una strategia aziendale su misura ed al contempo traccia il limite oltre il quale l'iniziativa economica deve cedere il passo alla tutela della persona.

Con l'ingresso nella normativa unionale del Regolamento ogni formalismo che consentiva di ricondurre (e ridurre) gli obblighi del titolare a meri adempimenti burocratici è stato definitivamente abbandonato.

Dalle relazioni annuali dell'Autorità di controllo emerge un ampio ricorso ai diritti di cui al Capo III del Regolamento, in particolare al diritto alla cancellazione dei dati personali, che rappresenta il principale strumento per impedire la diffusione di informazioni nel contesto online, in cui le istanze di tutela della identità digitale e quella personale si sovrappongono.

L'esperienza giuridica rivela che le autorità preposte alla tutela della persona considerino tale diritto una prerogativa relativa da contemperare con diritti di pari rango; ciò onde evitare che una situazione giuridica si atteggi in modo tiranno e goda di un'ingiustificata iperprotezione.

La contesa tra il diritto alla identità personale ed il diritto alla libertà di manifestazione del pensiero è particolarmente evidente nel contesto giornalistico, ambito in cui sono infatti previste espressa deroghe (assistite da altrettanti limiti) alla disciplina generale. Come chiarito anche dalla Corte costituzionale, la composizione di tale contrasto deve avvenire attraverso l'abbandono di soluzioni precostituite che prediligano la costante prevalenza di un diritto su un altro, lasciando spazio ad un delicato bilanciamento che tenga

conto delle circostanze del caso concreto e che sia condotto alla stregua dei principi generali, in primo luogo quelli di minimizzazione e di finalità del trattamento sanciti dagli articoli 5, par.1, lett. b) e c).

La giurisprudenza europea e nazionale ha in più occasioni individuato una soluzione di compromesso tra i diritti alla riservatezza ed alla protezione dei dati personali ed il diritto alla libertà di informazione nella deindicizzazione dei dati personali dell'interessato, in modo tale che, da un lato, le notizie di cui venga richiesta la cancellazione non siano immediatamente a lui riconducibili attraverso una ricerca (mediante query) che parta dal suo nome, e, dall'altro, l'interesse conoscitivo della generalità dei consociati sia comunque soddisfatto.

Da un'altra prospettiva si osserva che, nel contesto online, il diritto alla libertà di manifestazione del pensiero di cui all'articolo 21 della carta costituzionale, inteso nella sua accezione più ampia, sia frequentemente minato dagli algoritmi che governano la rete e che rinchiudono l'interessato in camere dell'eco caratterizzate dalla presenza di contenuti in linea con le preferenze da lui espresse attraverso un susseguirsi di click.

Il pedinamento digitale, ad opera di strumenti di tracciamento online come i cookie, si colloca tra le pratiche più pericolose per l'integrità del diritto alla identità personale digitale, in quanto capace di condizionare l'autodeterminazione dei singoli e le loro opinioni, che, infatti, risultano sempre più polarizzate.

La pratica di queste attività è oggi ammessa e subordinata alla (sola) raccolta preventiva del consenso libero, informato, specifico ed inequivocabile dell'interessato.

1.3 Il consenso come strumento di autodeterminazione informativa.

Il quadro giuridico che regola l'utilizzo ed il funzionamento dei cookie e degli altri strumenti di tracciamento online è costituito dal Regolamento generale, nonché dalle disposizioni della Direttiva 2002/58/CE (c.d. direttiva e-Privacy) relativa alla vita privata e alle comunicazioni elettroniche, recepite nell'ordinamento nazionale con l'art. 122 del Codice privacy.

Per quanto concerne l'interazione tra le due normative il comitato europeo dei garanti ha chiarito che¹² le disposizioni della direttiva e-Privacy precisano quelle del regolamento per quanto riguarda il trattamento dei dati personali nel settore delle comunicazioni elettroniche e che, in conformità con il principio *lex specialis derogate legi generali*, le prime prevalgono sulle seconde nelle situazioni che intendono disciplinare in modo specifico. Di contro, qualsiasi trattamento di dati personali non specificamente disciplinato dalla direttiva e-Privacy rimane soggetto alle disposizioni del regolamento.

L'articolo 4, numero 11, del regolamento in materia di dati personali definisce il consenso come "qualsiasi manifestazione di volontà libera,

¹² European Data Protection Board (EDPB), *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, 2019; E. NUNZIANTE, *Rapporto tra direttiva e privacy e GDPR: l'opinione dei Garanti Ue*, in *Agenda Digitale*, 2019

specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

I requisiti del consenso sono specificati nell'articolo 7 del Regolamento e, più dettagliatamente, nelle linee guida n.5/2020¹³ adottate dal Comitato europeo, secondo cui il consenso, per essere valido, deve essere specifico, al fine di evitare che venga utilizzato per le attività di trattamento di volta in volta individuate dal titolare e non corrispondenti a quelle illustrate nell'informativa, nonché libero. Non è rispondente a tale ultimo requisito la volontà positiva espressa dall'interessato che si trovi a scegliere tra la cessione dei suoi dati personali e la rinuncia del servizio (take it or leave it). La volontà della persona appare tanto più frustrata se si considerano, ai fini dello scambio, quei servizi che consentono l'esercizio di diritti fondamentali, come la posta elettronica rispetto al diritto alla corrispondenza garantito all'articolo 15 della costituzione.

In attesa che l'Autorità garante si pronunci¹⁴, le uniche risposte in merito provengono dalla Corte europea che ha chiarito che, dinanzi all'opzione take it or leave it, il consenso sia da ritenersi coartato, salvo che lo stesso titolare offra servizi equivalenti di cui l'interessato possa fruire anche senza cedere i propri dati personali¹⁵.

2. Il Regolamento 2022/2065/UE.

2.1. La responsabilità dei prestatori dei servizi.

Gli obiettivi di autodeterminazione informativa e di tutela dell'identità digitale della persona sono perseguiti altresì dal Regolamento (UE) 2022/2065 (d'ora in poi DSA)¹⁶ relativo al mercato unico dei servizi digitali, che modifica la direttiva 2000/31/CE, inserendosi nel complesso quadro della strategia digitale europea.

L'articolo 26 del DSA rubricato "Pubblicità sulle piattaforme online regola le attività pubblicitarie sulle piattaforme online, ampliando la sfera giuridica dei destinatari dei servizi digitali attribuendo loro il diritto di essere messi in grado di identificare in modo chiaro, conciso, inequivocabile ed in tempo reale "che l'informazione costituisce una pubblicità; la persona fisica o giuridica per conto della quale viene presentata la pubblicità; la persona fisica o giuridica che paga

¹³ European Data Protection Board (EDPB), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 2020.

¹⁴ Garante per la protezione dei dati personali, *Cookie wall: prosegue l'istruttoria del Garante privacy su alcune testate giornalistiche online*, 2022, Consultabile online: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9822601>

¹⁵ Corte di giustizia (673/17-Planet49), 1 ottobre 2019, in *Eur-Lex*; R. COBAZZI, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso Planet49*, in *Medialwas*, 2020; M. C. MENEGHETTI, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *Medialwas*, 2021

¹⁶ Regolamento 2022/2065/UE

per la pubblicità, se detta persona è diversa dalla persona fisica o giuridica di cui alla lettera; le informazioni rilevanti direttamente e facilmente accessibili dalla pubblicità relative ai parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e, laddove applicabile, alle modalità di modifica di detti parametri”.

Parimenti, l'articolo 27 rubricato “Trasparenza dei sistemi di raccomandazione” mira a garantire la massima trasparenza in favore dei consumatori e riequilibrare, seppur parzialmente, l'asimmetria informativa che caratterizza i rapporti business to consumer (B2C) prevedendo in favore dei destinatari dei servizi online un diritto innovativo, che si presume avrà un significativo impatto nel contesto digitale: il diritto di chiedere la modifica dei criteri sulla base dei quali avviene la personalizzazione dei contenuti che vengono mostrati all'utente. I gestori delle piattaforme che si avvalgono di sistemi di raccomandazione saranno tenuti a specificare nelle condizioni generali di utilizzo del servizio, in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché le ragioni per cui talune informazioni sono loro suggerite. Unitamente a tale diritto, il DSA prevede che siano offerte ai fruitori dei servizi digitali delle opzioni di scelta che consentano loro di modificare i parametri impostati di default ai fini della determinazione dei sistemi di raccomandazioni, anche attraverso una sezione specifica dell'interfaccia della piattaforma. Tale funzionalità dovrà essere sempre disponibile all'utente, consentendogli di selezionare e modificare l'opzione preferita in qualsiasi momento, così determinando liberamente ed autonomamente le informazioni a cui dare priorità.

La trasparenza ed il controllo sottesi a tale previsione rimarcano quanto già previsto dall'articolo 22 del Regolamento in materia di protezione dei dati personali in punto di processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione, e dal considerando 71 della stessa normativa che recita “Tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore”.

In continuità con il suddetto considerando, il legislatore del DSA, consapevole dei rischi della profilazione e dell'impatto che può avere sul grado di sviluppo ed autoconsapevolezza dei minori, vieta ex articolo 28, par.2,¹⁷ ogni tipo di attività di profilazione basata sui dati personali dei minori ed individua tale trattamento tra i rischi sistemici significativi di cui le piattaforme di dimensioni molto grandi devono tener conto ai fini dell'individuazione di misure tecniche ed organizzative adeguate, nonché nell'ambito degli audit indipendenti a cui devono periodicamente sottoporre la loro attività.

In particolare, con riferimento alle c.d. Large Online Platforms - LoPs - di cui all'articolo 34, par.1, lett. d) del DSA, la normativa richiede che nel valutare i rischi sistemici si tenga conto di “qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute

pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona”.

La lettura del DSA suggerisce ulteriori considerazioni in ordine alla tutela dell'identità della persona nell'ambiente digitale.

In particolare, per quanto concerne la responsabilità dell'Hosting provider si rammenta che la Direttiva 2000/31 prevedeva *ex* articoli 12-15 (oggi espressamente soppressi dall'articolo 89 del DSA) un discusso regime di (ir)responsabilità dei prestatori dei servizi, secondo cui tali soggetti venivano esonerati da responsabilità in presenza di determinate condizioni, essendo escluso nei loro riguardi un obbligo generale sia di sorveglianza sulle informazioni che trasmettono o memorizzano che di accertamento attivo dei fatti o delle circostanze che indichino la presenza di attività illegali.¹⁸

La disciplina era completata dal decreto d.lgs. n. 70 del 2003, attuativo della Direttiva 2000/31, ove l'articolo 16 prevedeva la responsabilità in capo al prestatore dei servizi che non avesse provveduto alla immediata rimozione dei contenuti illeciti ovvero che avesse continuato a pubblicarli, pur in presenza delle seguenti condizioni: conoscenza legale dell'illecito perpetrato dal destinatario del servizio, a seguito di una comunicazione da parte del titolare del diritto leso ovvero in quanto appreso *aliunde*; evidente l'illiceità dell'altrui condotta, laddove fosse imputabile all'hosting provider una colpa grave per non averla positivamente riscontrata; ciò alla stregua del grado di diligenza ragionevolmente atteso da un operatore professionale della rete in un determinato momento storico; possibilità concreta di attivarsi utilmente, in quanto edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere”.¹⁹

Parte della dottrina e della giurisprudenza²⁰ hanno a lungo adottato un'interpretazione *sui generis* delle suddette norme, operando una distinzione tra due figure di hosting provider in realtà non rinvenibile nel dettato normativo, secondo cui il regime di favore stabilito dal d.lgs. 70/2003 non trova applicazione in presenza di un provider che completi e arricchisca in modo non passivo la fruizione dei contenuti da parte degli utenti, attraverso operazioni di: filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione, promozione dei contenuti; ovvero l'impiego di strumenti di valutazione del comportamento degli utenti.

Viceversa, secondo tale impostazione, l'hosting provider passivo, autore di una un'attività di prestazione di servizi neutra, di ordine meramente tecnico, automatico e, pertanto, non in grado di esercitare alcun controllo sulle informazioni trasmesse o memorizzate dai destinatari dei suoi servizi, è esente da responsabilità²¹.

¹⁸ Cass.civ.,19.03.2019, n. 7708, par. 5.1, in *Italggiure Web*; D. IASELLI, *Responsabilità del provider: la Cassazione detta rilevanti principi di diritto*, *Cassazione civile*, sez. I, sentenza 19/03/2019 n° 7708, in *Altalex*, 2019; C. D'ONOFRIO, *La Cassazione si pronuncia sulla responsabilità di un hosting provider attivo e sul risarcimento del danno*, in *Diritto al digitale*, 2022; T.A.R. Lazio Roma Sez. IV, 24 gennaio 2024, n. 1393

¹⁹ Cass. pen., 17.12.2013 n.3672 in *Italggiure Web*.; Cass. civ., 16.09.2021, n. 25070, in *Italggiure Web*.

²⁰ Cass., 19.03.2019, n.7708, in *Italggiure Web*

²¹ Corte di giustizia (C-291/13), 11.09.2014 in *Eur-Lex*; Corte di giustizia (C-324/09), 12.07.2011 in *Eur-Lex*.; C. D'URSO, *I profili informatici nella valutazione della responsabilità dell'Hosting Provider*, 2021, in *Rivista Italiana di Informatica del Diritto*.

Con il DSA, operativo dal 17 febbraio 2024, il legislatore europeo chiarisce i dubbi del passato prevedendo un chiaro quadro per l'esenzione condizionata dalla responsabilità dei prestatori di servizi intermediari, in particolare affermando all'articolo 8, collocato nel Capo II titolato "Responsabilità dei prestatori di servizi intermediari", che "ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali" e precisa ai considerando 21 e 22 che "un prestatore dovrebbe poter beneficiare delle esenzioni dalla responsabilità per i servizi di semplice trasporto e memorizzazione temporanea se non è in alcun modo coinvolto nelle informazioni trasmesse o alle quali è stato fatto accesso. A tal fine è necessario, tra l'altro, che il prestatore non modifichi le informazioni che trasmette o alle quali fornisce accesso. Tale prescrizione non dovrebbe tuttavia intendersi riferita alle manipolazioni di carattere tecnico effettuate nel corso della trasmissione o dell'accesso, purché tali manipolazioni non alterino l'integrità delle informazioni trasmesse o alle quali è fornito accesso." "Al fine di beneficiare dell'esenzione dalla responsabilità per i servizi di memorizzazione di informazioni, il prestatore dovrebbe agire immediatamente per rimuovere le attività illegali o i contenuti illegali o per disabilitare l'accesso agli stessi non appena ne venga effettivamente a conoscenza o ne divenga consapevole."

L'atto europeo afferma dichiaratamente che le esenzioni dalla responsabilità dovrebbero applicarsi in relazione a qualsiasi tipo di responsabilità per ogni tipo di contenuto illegale, indipendentemente dall'oggetto preciso o dalla natura esatta di tali leggi²²; ciò in quanto il problema dei contenuti e delle attività illegali online non dovrebbe essere affrontato concentrandosi esclusivamente sulla loro responsabilità e sulle loro competenze ma coinvolgendo anche attori, tra cui i moderatori dei gruppi negli ambienti online chiusi, limitando il coinvolgimento degli intermediari solo laddove dispongano, effettivamente, della capacità tecnica e operativa per contrastare contenuti illegali.²³

Ad ogni modo, trattandosi di una esenzione condizionata, la stessa non trova applicazione laddove il destinatario del servizio agisca sotto l'autorità o il controllo del prestatore di servizi di memorizzazione di informazioni. Ad esempio, nel caso in cui il fornitore di una piattaforma online consenta ai consumatori di concludere contratti a distanza con operatori commerciali, definendo il prezzo dei beni o dei servizi, ovvero qualora lo stesso collabori deliberatamente con il destinatario dei servizi al fine di commettere attività illegali.

2.2 L'affermazione del diritto (condizionato) di accedere all'account social.

Il DSA regola altresì il regime applicabile ai provvedimenti adottati dai fornitori a seguito della violazione da parte del destinatario del servizio degli

²² Considerando 17 Reg. 2022/2065/UE

²³ Considerando 27 Reg. 2022/2065/UE

standard della community o della diffusione di contenuti illegali, introducendo una maggiore trasparenza in favore degli utenti. Si tratta di provvedimenti che dispongono: restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; la sospensione o la cessazione totale o parziale della prestazione del servizio ovvero la sospensione o la chiusura dell'account del destinatario del servizio.

Le novità normative confermano l'importanza delle piattaforme social: vere e proprie comunità parallele, ove trova espressione l'identità personale dell'individuo ed in cui vengono instaurate relazioni sociali e professionali²⁴.

Il DSA introduce nella sezione 2 obblighi aggiuntivi applicabili ai prestatori di servizi di memorizzazione di informazioni, comprese le piattaforme online, che mirano, da un alto, a preservare la sicurezza dell'ambiente digitale e, dall'altro, a rendere edotto il destinatario di un provvedimento di restrizione, sospensione o blocco dell'account.

In particolare l'articolo 16 della normativa in argomento richiede ai prestatori di servizi di memorizzazione di informazioni l'introduzione di meccanismi che permettano agli utenti di segnalare la presenza di contenuti che ritengano in contrasto con i termini e le condizioni di utilizzo del servizio. Le segnalazioni devono essere precise ed adeguatamente motivate.

A tutela del titolare dell'account del destinatario del servizio, l'articolo 17 del DSA prevede che i fornitori instaurino un dialogo con l'utente segnalato affinché questo sappia, attraverso una motivazione chiara, che specifichi in che modo i contenuti caricati sulla piattaforma siano incompatibili con le condizioni generali del servizio ovvero illegali.

Tali questioni meritano di essere esaminate anche in considerazione delle pretese risarcitorie che potrebbero legittimamente vantare i titolari di un account destinatari di provvedimenti che ne impediscano, ingiustificatamente, la piena fruibilità, con evidenti lesioni della loro sfera giuridica. Tra i primi interventi giurisprudenziali sul punto si segnala la pronuncia con cui il Tribunale Ancona²⁵ ha recentemente statuito che "prima di procedere alla disabilitazione definitiva dell'iscrizione di un utente ad un social network s'impone, al fornitore del servizio, una puntuale verifica delle violazioni contrattuali, stante che ciò comporta la cancellazione definitiva dei dati associati all'account, con la conseguenza che, altrimenti, si avrebbe una lesione dell'identità digitale e una responsabilità contrattuale (...) alla quale consegue un risarcimento del danno alla persona, in questo caso digitale, risarcimento ancor più consistente allorquando l'account non è più ripristinabile e sono stati distrutti i dati personali ad esso collegati."

²⁴ A. AMIDEI, *Tutela del consumatore – Il vaglio di validità delle clausole contrattuali di content moderation online*, in *Giur.It.*, 2023; S. FLAMINIO, *Lotta alle fake news: dallo stato dell'arte a una prospettiva di regolamentazione per il "vivere digitale" a margine del Digital Service Act*, in *Rivista italiana di informatica e diritto*, Fascicolo 2, 2002

²⁵ Tribunale Ancona Sez.I, 15.06.2023, pag.1, in *Leggi d'Italia*

Conclusioni.

Le garanzie introdotte dal nuovo regolamento in materia di servizi digitali si inseriscono, unitamente a quelle previste dal regolamento in materia di protezione dei dati personali, nella sfida europea di coniugare dignità e innovazione nella consapevolezza di non poter demandare a protocolli informatici o contrattuali, unilateralmente stabiliti dai big tech, la disciplina del contesto, quello digitale, in cui più di ogni altro si dispiega la nostra esistenza²⁶.

Le piattaforme hanno acquisito un potere tale da sopravanzare perfino quello statale, ridisegnando con le condizioni del contratto il perimetro dell'esercizio dei diritti e delle libertà fondamentali²⁷.

È in tale contesto che lo Stato, anche attraverso l'attività delle Autorità di controllo, è chiamato a riappropriarsi del ruolo di garante del rispetto dei diritti fondamentali.

²⁶ A. SORO, *Proteggere i dati per governare la complessità*, Relazione Autorità garante per la protezione dei dati personali, Roma, 2017; A. VERCELLOTTI, *Reputazione online, come difenderla? Guida pratica per aziende e professionisti*, in *Agenda Digitale*, 2022

²⁷ P. STANZIONE, *Relazione introduttiva. Il Metaverso tra utopie e distopie*, in atti del Convegno *Il Metaverso tra utopie e distopie. Orizzonti e sfide della protezione dei dati*, Roma, 2023, 13. Consultabile online: <https://www.garanteprivacy.it/web/quest/home/docweb/-/docweb-display/docweb/9939113>