ISSN 2531-8950

Anno VII - 2022 n. 3

Nuovo Diritto Civile

ESTRATTO

LIVIA AULINO

LA LIBERTÀ DI INFORMAZIONE TRA PROTEZIONE DEI DATI PERSONALI ED ESERCIZIO DELLA PUBBLICA FUNZIONE

DIKE GIURIDICA

ANGOLO DELLE AUTORITÀ INDIPENDENTI

Livia Aulino
(Assegnista di ricerca Università degli studi di Napoli Federico II)

LA LIBERTÀ DI INFORMAZIONE TRA PROTEZIONE DEI DATI PERSONALI ED ESERCIZIO DELLA PUBBLICA FUNZIONE*

Sommario: 1. Il caso: la pubblicazione di foto di minori sulle pagine *social* dei rappresentanti di enti istituzionali. – **2.** *Segue*. Qualificazione della fattispecie e individuazione della disciplina applicabile. – **3.** Il rapporto tra tutela del minore ed esercizio di pubbliche funzioni avendo riguardo al GDPR e al Codice *Privacy*: il diritto all'informazione e il provvedimento del Garante Privacy. – **4.** L'effetto della riforma dell'art. 2 *ter* del Codice Privacy sul provvedimento del Garante – **5.** Il principio di *essenzialità dell'informazione* nel provvedimento del Garante – **6.** I recenti interventi legislativi europei per la tutela dei minori in ambiente digitale. **7.** *Segue*. Punti critici.

1. Il caso: la pubblicazione di foto di minori sulle pagine *social* dei rappresentanti di enti istituzionali

Il Garante italiano della *privacy*, con il provvedimento n. 197/2021[1], ha sancito che non è possibile pubblicare sul sito del Comune o sulle pagine *social*, le immagini e i video che espongono chiaramente minori ovvero persone fragili, sia pure al fine di denunciare una situazione di degrado.

* Il contributo è stato sottoposto, in forma anonima, alla valutazione di due *referee*.

[1] Garante per la protezione dei dati personali, Ordinanza ingiunzione, 13 maggio 2021, consultabile su *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670001*.

In particolare, nella pagina *Facebook* "*De Luca sindaco di Messina*" era stato pubblicato un video che riproduceva persone c.d. "fragili" e in condizioni di difficoltà socio-economica, colte nell'atto di gettare rifiuti ingombranti in un'area non deputata allo smaltimento degli stessi e in modo tale da renderle riconoscibili a quanti riproducessero il video. In un altro *post* della pagina era stata pubblicata la foto di un ragazzo disabile per pubblicizzare il provvedimento di assegnazione ai genitori di un posto auto nei pressi della sua abitazione, rendendo visibile anche l'indirizzo. Inoltre, per documentare la situazione delle "baraccopoli" nella città di Messina, erano state pubblicate altre immagini e video – anche se con persone non riconoscibili – dove si intravedevano alcuni minori in condizioni disagiate.

In tutti questi casi, secondo il Garante, la diffusione è risultata ingiustificata ed in contrasto sia con il principio di essenzialità dell'informazione che con le disposizioni poste a tutela dei minori e delle persone con problemi di salute.

A conclusione del procedimento l'Autorità aveva condannato il Sindaco di Messina al pagamento di una sanzione di cinquantamila euro, vietando l'ulteriore trattamento dei dati, eccetto la loro conservazione ai fini di un eventuale utilizzo in sede giudiziaria.

2. *Segue*. Qualificazione della fattispecie e individuazione della disciplina applicabile

Le nuove tecnologie hanno potenziato gli attuali strumenti di comunicazione, in grado di raggiungere instantemente un numero sempre più ampio di utenti[2], tanto da arrivare a definire la società contemporanea come "società dell'informazione".

Ciò ha comportato l'esigenza di una tutela rafforzata della protezione dei dati dei singoli individui, ed in particolare dei minori[3]. A tal

[2] G. Bazzoni, *La libertà di informazione e di espressione del pensiero nell'era della democrazia*, in *Diritto di Internet*, 2019, p. 635.

[3] La Corte di Strasburgo, attraverso un'ampia casistica, ha riconosciuto quale *best interest of the child*, l'interesse allo sviluppo della sua identità personale in quanto tratto imprescindibile del soggetto in formazione (S. c. Francia, 26 luglio 2007). Sul punto: L. Dettole, *Le fonti del diritto minorile*, in L. Dettole, M. Locaputo, V. Valente, *I diritti e le tutele del minore*, Roma, 2022, p. 41.

proposito, è intervenuto il recente Regolamento UE n. 2016/679 (cd. GDPR), il quale, al considerando 38, postula la necessità di una specifica protezione per i minori con riferimento alla diffusione dei loro dati personali, proprio in considerazione della loro limitata consapevolezza dei rischi e dei loro diritti circa il trattamento dei dati personali.

A tal proposito, l'art. 8 del GDPR, in tema di offerta di servizi *web* per i minori, sancisce che il consenso sia lecitamente prestato stesso dal minore ove questi abbia compiuto sedici anni[4]. Al di sotto di tale limite anagrafico il consenso dovrà essere concesso da coloro che esercitano sul minore la responsabilità genitoriale ovvero dal tutore. Inoltre, si rileva che il decreto legislativo n. 101/2018, di adeguamento al GDPR, ha ridotto in Italia il limite di età per i minori a prestare il consenso al trattamento dei loro dati *online* a quattordici anni, mentre per i più piccoli è necessario il consenso di entrambi i genitori. Questo diritto riservato al minore non autorizza, però, terze persone a pubblicare immagini, e in generale i dati del minore di età superiore ai quattordici anni, soprattutto laddove uno dei due genitori ne abbia espressamente negato il consenso[5]. Eppure, va considerato che il GDPR ha previsto alcune ipotesi che costituiscono la base giuridica per il trattamento dei dati, soprattutto da parte delle Istituzioni[6].

---

[4] Sul tema: I.A. Caggiano, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 1, 2018, pp. 3-23. Vedasi anche I. Garaci, *La "capacità digitale" del minore nella società dell'informazione. Riflessioni sul corretto esercizio della responsabilità genitoriale fra esigenze di autonomia e di protezione*, in questa *Rivista*, 2019, pp. 59-86.

[5] L. Aulino, T*utela dei minori e servizi digitali: i rischi dello sharenting,* in *Familia*, 2022, pp. 35-52.

[6] Infatti, l'art. 6 del GDPR dispone quanto segue "*1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti*".

L'art. 6, par. 1, lett. e) e f) del GDPR[7] prevede una deroga non irrilevante a favore dei pubblici poteri, dal momento che esclude *a priori* che nel trattamento di dati svolto dalle pubbliche autorità nell'ambito dei loro compiti possa aversi una interferenza dei diritti del minore.

Tuttavia, affinché tale deroga operi devono ricorrere, *de facto*, due fondamentali condizioni: che il trattamento sia effettuato da soggetti istituzionali (e non da privati); che tale trattamento sia svolto nell'esecuzione dei loro compiti, e quindi va verificato se possa effettivamente essere ricondotto all'ipotesi di cui alla lett. e), ossia che sia necessario per adempiere a un interesse pubblico ovvero che sia connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Il primo requisito, di fatto, si configura quale parametro "soggettivo", attenendo alla qualifica rivestita dal titolare del trattamento. Il secondo, invece, lo si potrebbe definire come parametro "oggettivo", dovendosi accertare non una qualifica quanto piuttosto l'oggettiva possibilità di ricondurre ai "compiti" della pubblica amministrazione l'attività concretamente svolta con tale trattamento.

Sul punto, invero, è necessario riportarsi al Codice della *privacy* (d.lgs. 30 giugno 2003, n. 196 e successive modifiche), che dedica a questa ipotesi una espressa previsione normativa.

Tale disposizione è prevista in ossequio al disposto dell'art. 6, par. 3 del GDPR il quale richiede che la base su cui si fonda il trattamento dei dati previsto in quelle due specifiche ipotesi deve essere tipizzata dalla normativa europea ovvero nazionale.

Ebbene, ai sensi dell'art. 2-*ter*, co. 1 del codice *privacy*, si impone che detta base giuridica nazionale sia costituita da norma di legge o da regolamento o da atti amministrativi generali. Il successivo co. 1-*bis* prevede, poi, che nel caso in cui il trattamento risulti non previsto dalla normativa, questo sia quantomeno considerabile come "necessario" ai fini dell'adempimento ai doveri pubblici. Però, in tale ultimo caso, come precisa l'ultimo inciso del co. 3, si deve comunicare al Garante la

[7] Art. 6 GDPR, lett. e) *"il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento"*. Art. 6 GDPR, lett. f) "*Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*".

necessità di effettuare tale trattamento con un preavviso di dieci giorni rispetto alla data di inizio.

Pertanto, dal combinato disposto delle norme presenti nel GDPR e nel Codice della *privacy*, emerge come il diritto dei minori (e, quindi, quello dei soggetti più fragili) a non veder trattati i loro dati senza consenso possa esser retrocesso di fronte alle necessità che si manifestano nell'ambito dell'operato della P.A., sia pur in presenza di determinate condizioni e, comunque nel rispetto del principio di stretta necessità e di minimizzazione del trattamento di cui all'art. 3 del Codice.

Si noti che l'art. 2-*ter* del Codice è stato oggetto di profondi cambiamenti mediante il D.L. n 139/2021, in quanto è stato inserito al co. 1 il riferimento agli "atti amministrativi generali", poi è stato introdotto il co. 1-*bis* nonché l'inciso, nel co. 3, che prevede il preavviso di dieci giorni prima di iniziare il trattamento dei dati. Ne consegue che l'analisi del provvedimento del Garante, essendo questo antecedente a tale modifica normativa, richiede di essere svolta sia con riferimento alla formulazione previgente sia con riguardo all'efficacia interpretativa e persuasiva che potrebbe avere in seguito alla suddetta novella legislativa.

3. Il rapporto tra tutela del minore ed esercizio di pubbliche funzioni avendo riguardo al GDPR e al Codice *Privacy*: il diritto all'informazione e il provvedimento del Garante Privacy

Al fine di qualificare la condotta dell'allora Sindaco di Messina, è necessario operare la distinzione innanzi anticipata. In primo luogo, si considerino le testuali parole utilizzate dal Garante nel suo provvedimento: "[...] *la base giuridica per il trattamento di dati necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e), del Regolamento) è costituita, secondo quanto previsto dall'art. 2-ter, commi 1 e 3 del Codice, esclusivamente da una norma di legge o di regolamento che lo preveda e ciò con riferimento a qualsiasi operazione di trattamento, ivi inclusa la diffusione*". Non solo, il trattamento "*non è apparso sorretto dalla base giuridica richiesta dalle norme, né comunque disciplinato da atti interni dell'ente diretti a contemplare l'utilizzo dei social network nell'ambito del perseguimento di finalità connesse all'esercizio di compiti di interesse pubblico*" e, si dovrebbe aggiungere, tracimerebbe fuori da qualsiasi

limite attualmente posto in tema di comunicazione istituzionale[8]. È, infatti, pacifico come, in assenza dei requisiti della necessarietà e della "tipizzazione" del trattamento dei dati con riferimento ad attività della P.A., tale trattamento vada inteso come illegittimo, indifferentemente dalla situazione del soggetto interessato (che potrebbe essere anche minore o fragile).

Inoltre, il Garante si è espresso sulla non riconducibilità del profilo *Facebook* all'Ente locale quanto, piuttosto, alla persona fisica chiamata a ricoprire la carica di Sindaco.

In tal modo, sulla base del dettato legislativo ante novella, si è potuta dichiarare l'illegittimità del trattamento dei dati a tutela dei soggetti a vario titolo coinvolti, senza che valga asserire – come fatto dal Sindaco – che alcuni di loro erano stati colti in flagrante mentre commettevano il reato di abbandono di rifiuti introdotto con il Codice dell'ambiente (D.lgs. n. 152/2006) e che siano stati filmati da un privato cittadino unicamente al fine di denunciarli presso la Casa Pubblica. Al contrario, la norma dell'art. 192 del T.U. Ambiente non prevede che il Sindaco sottoponga i rei a una pubblica ordalia – neppure a fini di sensibilizzazione dell'opinione pubblica – bensì è chiamato a disporre con ordinanza la rimozione dei suddetti rifiuti a carico del soggetto che li ha dolosamente abbandonati. Ordinanza che, nel caso di specie, pare sia stata considerata meno rilevante rispetto a quelli che erano i fini politici che hanno animato l'azione dell'esponente politico locale.

4. L'effetto della riforma dell'art. 2 *ter* del Codice Privacy sul provvedimento del Garante

Come si è anticipato, le principali innovazioni normative si sono avute non molto tempo dopo rispetto a tale pronuncia del Garante, ma probabilmente se fossero state anteriori avrebbero potuto influire sulla decisione emessa, il cui contenuto avrebbe potuto essere diverso. Per meglio comprendere questo aspetto, si consideri l'ordinanza n. 54/2021, emessa nei confronti del Ministero dello Sviluppo Economico, in cui è stato censurato un trattamento dei dati disposto sulla

[8] D. Rinaldi, N. Brutti, *Comunicazione istituzionale e sociale*, in S. Sica, V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione*, Trento, 2015, pp. 187 ss.

base di un decreto direttoriale, provvedimento non qualificabile come "*regolamento*" bensì come "*atto amministrativo generale*"[9].

Eppure, nonostante ciò, se anche dovesse essere emanato – in futuro – un atto amministrativo generale che permetta, testualmente, ad un Comune di operare un trattamento dei dati come quello censurato nel provvedimento fin qui commentato, ugualmente non si avrebbe un trattamento legittimo.

Ciò per due ragioni: in primo luogo, dovrebbe aversi un trattamento effettuato attraverso profili e *device* intestati non alla persona fisica chiamata a svolgere la funzione di sindaco, bensì all'Ente Locale, in tal modo impedendo indirettamente che possa essere svolto senza remore alcuna, dovendosi trasmettere la facoltà di rappresentare l'Ente sui canali *social* ad ogni elezione. In tal modo, i toni sarebbero ricondotti ad un livello più istituzionale. Laddove si utilizzasse un profilo privato, invece, si ricadrebbe negli eccessi da "sceriffo" denunciati dal Garante.

Inoltre, va considerato l'art. 2-*sexies*, il quale così dispone al secondo comma: "*2. fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: [...] h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo*".

Ne deriva che lo svolgimento delle funzioni di controllo e di indirizzo politico è connesso unicamente a finalità di espletamento di un mandato elettivo. Per cui, dette funzioni sono connesse alla necessità di far funzionare la "macchina amministrativa" e non certo a quella di renderne più difficoltoso, esasperando gli animi e concentrandosi sulla legittimazione politica, l'operato.

Infatti, come evidenziato prima, in presenza di un abbandono dei rifiuti il Sindaco è chiamato ad emettere una ordinanza ai fini della loro rimozione e, quindi, anche a verificarne il rispetto. Laddove, invece, questi dovesse sottoporre alla gogna per fini politici i rei conclamati,

---

[9] Consiglio di Giustizia amministrativa per la regione Sicilia, 14 marzo 2011, n. 200 in *https://www.osservatoriosullefonti.it/archivi/archivio-rubriche/archivio-rubriche-2011/287-fonti-degli-enti-locali/418-caratteri-distintivi-dei-regolamenti-dagli-atti-amministrativi-generali-e-conseguente-differenza-di-disciplina-quanto-alla-loro-impugnazione.*

dimostrerebbe di utilizzare tali dati non ai fini dell'espletamento di un mandato elettivo bensì per fini personali.

Da ciò conseguirebbe, nuovamente, l'illegittimità del trattamento di dati svolto nelle modalità contestate al Sindaco di Messina e il ristabilimento delle tutele per gli interessati[10].

5. Il principio di *essenzialità dell'informazione* nel provvedimento del Garante

Oltre ai profili di tutela del minore ai sensi del GDPR, il Garante ha evidenziato anche quelli inerenti alla violazione dell'art. 10 c.c., laddove la pubblicazione delle immagini delle persone – tra cui minori – non è da ritenersi lecita nel caso in cui non vi sia prevalenza dell'interesse pubblico all'informazione rispetto al diritto alla riservatezza (art. 2 Cost.)[11].

A ciò va poi aggiunto il mancato rispetto degli artt. 6, 7, 8 delle regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica (cd. codice deontologico).

Al fine di comprendere meglio, è necessario ricordare che il GDPR, all'art. 85, ha lasciato liberi gli Stati membri di prevedere esenzioni o deroghe rispetto al Regolamento, nel caso siano necessarie per conciliare il bilanciamento tra il diritto alla protezione dei dati personali e la libertà di espressione e d'informazione.

A tal proposito, il Codice della *privacy* disciplina agli art. 136 e ss. il trattamento dei dati effettuato nell'esercizio della professione di gior-

[10] Si noti, poi, come un simile trattamento dei dati sarebbe tale da necessitare quantomeno di una valutazione preventiva dell'impatto. Sul punto si veda: G. Magri, S. Martinelli, S. Thobani, *Manuale di diritto privato delle nuove tecnologie*, Torino, 2022, 186-187.

[11] Il diritto all'immagine è oggetto di una disciplina restrittiva che consente di escludere la liceità della sua utilizzazione, da parte di terzi, anche in alcuni casi in cui sia ravvisabile l'esercizio del diritto di cronaca. La giurisprudenza di Legittimità ha chiarito che il diritto all'identità personale, garantito all'art. 2 Cost., non è necessariamente recessivo nel bilanciamento con il diritto di cronaca, dovendosi considerare i rischi della diffusione dell'immagine per la dignità della persona e la rilevanza del diritto all'identità personale. Sul punto si veda, A.G. Cianci, *Il diritto all'immagine. Cass., 22 luglio 2015*, n. 15360, in M. Bianca, A. Gambino. R. Messinetti, *Libertà di manifestazione del pensiero e diritti fondamentali*, Milano, 2016, pp. 111-119.

nalista; all'art. 137 si sancisce che possono essere trattati i dati di cui agli artt. 9 e 10 del GDPR anche senza il consenso dell'interessato, purché nel rispetto delle regole deontologiche. Ne consegue l'efficacia del codice deontologico dei giornalisti[12], la cui rilevanza sul piano normativo[13] è confermata anche dal codice *privacy*.

In particolare, nel caso di specie, era stata posta in essere una violazione degli artt. 6, 7, 8 del codice deontologico dei giornalisti. L'art. 7, si sofferma sulla tutela del minore, sancendo che al fine di tutelarne la personalità, il giornalista non fornisce particolari in grado di condurre alla loro identificazione. Inoltre, il terzo comma chiarisce che il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca, salvo nel caso di rilevante interesse pubblico, il giornalista dovrà farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi e limiti stabiliti dalla Carta di Treviso.

L'art. 8 nel tutelare la dignità della persona limita la liceità della pubblicazione dell'immagine all'essenzialità dell'informazione, principio disciplinato all'art. 6 del medesimo codice.

È proprio tale principio che viene, più volte, richiamato dall'Autorità garante *privacy* nel provvedimento in commento.

Il principio di essenzialità dell'informazione prevede un nesso di necessarietà tra i dati pubblicati e la notizia; ciò comporta un bilanciamento tra l'interesse pubblico all'informazione ed il diritto alla riservatezza del singolo individuo.

Il principio è frutto di un combinato disposto di alcune norme, nonché dell'evoluzione giurisprudenziale e dei precedenti di Autorità indipendenti, quale il Garante *Privacy*.

---

[12] C. Di Martino, *La disciplina della stampa e la professione giornalistica*, in S. Sica, V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione*, cit., pp. 74-85.

[13] Sul valore di fonte normativa del codice dei giornalisti, si era già espressa anche la giurisprudenza di Legittimità, secondo cui "*Le regole deontologiche in esso contenute non sono soltanto regole di comportamento per i giornalisti professionisti dettate dall'Ordine di appartenenza, la cui violazione li esponga esclusivamente a possibili sanzioni disciplinari da parte del Consiglio dell'Ordine, ma sono regole di condotta aventi efficacia generale la cui violazione può essere fonte di responsabilità civile in capo al giornalista o alla sua testata*". Sul punto si veda, M. Bianca, *Il codice deontologico del giornalista. Cass., 6 giugno 2014*, n. 12834, in M. Bianca, A. Gambino. R. Messinetti, *Libertà di manifestazione del pensiero e diritti fondamentali*, cit., pp. 51-55.

In particolare, si tiene conto dell'art. 21 della Costituzione[14] sulla libertà di manifestazione del pensiero e dell'art. 10, sulla libertà di espressione della Convenzione Europea dei diritti dell'uomo. Per cui, non è possibile cristallizzare il concetto dell'essenzialità dell'informazione in una nozione specifica e astratta, dovendosi lasciare tale bilanciamento tra la tutela dei dati ed il diritto di cronaca alla valutazione di volta in volta operata dal giornalista[15]. Però, un dato è ineludibile: il principio di essenzialità impone la non necessarietà della divulgazione di fatti privati – anche di terzi estranei alla vicenda e addirittura di persone vulnerabili – che risultino privi di un obiettivo pubblico, come è successo nel caso *de quo*.

A tal proposito l'Autorità Garante *Privacy* sia è, già in passato, espressa sul tema cercando di chiarire, sia pur con difficoltà, i limiti del principio di essenzialità[16], arrivando in alcuni casi a riscontrare la violazione delle norme suddette e, in altre ipotesi, è giunta a considerare legittimo il bilanciamento operato dal giornalista.

Per esempio, è stata censurata la diffusione dell'indirizzo dell'interessato, in occasione di fatti di cronaca[17]; nonché la prassi di un quotidiano solito a pubblicare i numeri delle targhe ed altre informazioni delle auto parcheggiate irregolarmente[18]; inoltre, il Garante ha ritenuto primario rispetto al diritto di cronaca il diritto dei minori alla riservatezza, condannando la pubblicazione delle foto dei minori, anche se figli di personaggi noti[19]. Inoltre, il Garante *privacy* aveva riscontrato l'illicei-

---

[14] Sul punto: S. SICA, *Le libertà di informazione e principi costituzionali*, in S. SICA, V. ZENO-ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, cit., pp. 9-17.

[15] Il giornalista, nonostante la sua attività rivesta anche una funzione sociale, non ha una libertà di informazione più ampia rispetto a quella riconosciuta agli altri soggetti. G. TINELLO, *Diritto delle tecnologie informatiche e principi costituzionali*, in G. CASSANO (a cura di), *Diritto delle tecnologie informatiche e dell'Internet*, Milano, 2002, p. 124.

[16] Si veda: M. PAISSAN, *Privacy e giornalismo. Diritto di cronaca e diritto dei cittadini*, (a cura di) Garante per la protezione dei dati personali, in *https://www.airf.it/privacy_e_giornalismo.93541.pdf*, 2008, p. 17.

[17] Garante per la protezione dei dati personali, Provvedimento del 12 ottobre 1998, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/39524*.

[18] Sul punto si veda, Garante per la protezione dei dati personali, *Nota dell'11 marzo 2002*, in *Risposta del 11 marzo 2002 (privacy.it)*.

[19] Garante per la protezione dei dati personali, Provvedimento del 5 giugno 2001, consultabile in *Diritto di cronaca: sbagliato pubblicare foto di minori, anche se figli di... – Garante Privacy*.

tà del trattamento di dati personali del Ministero dell'Interno, in quanto erano stati divulgati video ed immagini di un episodio di violenza autolesionistica da parte di un uomo in uno stato di alterazione psico-fisica, avvenuta all'interno di un commissariato[20]. Diversamente, il Garante ha ritenuto lecita la pubblicazione di dati reddituali, in quanto comunque assoggettati per legge ad un regime di pubblicità[21].

6. I recenti interventi legislativi europei per la tutela dei minori in ambiente digitale

In questo contesto è intervenuto il regolamento sui servizi digitali, *Digital Service Act*[22] (DSA), che insieme al regolamento sui mercati digitali, *Digital Markets Act*[23] (DMA), rappresentano i pilastri della futura regolamentazione digitale.

In particolare, il DSA persegue lo scopo di tutelare la libertà di espressione degli utenti attuando una responsabilizzazione dei servizi intermediari quali quelli offerti da prestatori di servizi di hosting, motori di ricerca e piattaforme comunemente noti come ISP (*Internet Service Provider*), esentando però da tali obblighi le piccole imprese con meno di 45 milioni di utenti attivi al mese nell'UE[24].

Si comprende, quindi, come si tratti di una normativa volta a responsabilizzare soprattutto le grandi piattaforme quali i *social network* più utilizzati i quali, proprio in ragione della loro diffusione, rappresentano i maggiori veicoli di iniziative volte a danneggiare le libertà degli utenti.

---

[20] Garante per la protezione dei dati personali, Provvedimento del 20 novembre 2020, consultabile in *Provvedimento del 26 novembre 2020 [9522206] – Garante Privacy.*

[21] Garante per la protezione dei dati personali, Provvedimento del 17 gennaio 2001, in *Dati reddituali dei contribuenti – Garante Privacy*.

[22] Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo ad un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regoamento sui servizi digitali), in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065&from=IT.*

[23] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo ai mercati equi e contendibli nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=IT.*

[24] *Legge sui servizi digitali: il Consiglio e il Parlamento europeo raggiungono un accordo per un ambiente online più sicuro*, in *https://www.consilium.europa.eu/it/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/*, 2022.

Pertanto, secondo gli ultimi sviluppi è emerso che le piattaforme dovranno valutare i rischi che i loro sistemi comportano non solo per contenuti e prodotti illegali ma anche per rischi sulla tutela degli interessi pubblici, dei diritti fondamentali, della salute e sicurezza pubblica[25]. In particolare, i motori di ricerca sono sottoposti ad obblighi rigorosi, e le piattaforme devono, quindi, tracciare i propri fornitori e gli utenti in generale in modo da individuare i prodotti e i contenuti illegali e bloccarli sin da subito, affinché non possano attuare condotte lesive nei confronti degli altri utenti; nonché saranno vietati *dark patterns* e pratiche ingannevoli[26].

Se da un lato l'art. 8 del DSA prevede che non sia imposto agli *Internet Service Provider* (ISP) un dovere di sorveglianza generalizzata nei confronti dei propri utenti, dall'altro, gli *host* sono onerati – per valersi della clausola di esclusione della responsabilità di cui all'art. 6 – del dovere di rimuovere qualsiasi contenuto chiaramente illecito di cui dovessero acquisire conoscenza nel corso delle loro normali attività.

Ne consegue che, in presenza di contenuti palesemente illegali e dannosi per gli altri utenti (a mero titolo esemplificativo si pensi alle *fake news* o alle sfide tra adolescenti), sono chiamati ad agire immediatamente e, quindi, anche a costo di subirne un danno economico dalla scelta.

Lo scopo è quello di assicurare la trasparenza e l'informazione corretta per ogni livello e servizio, in particolare nel caso di piattaforme accessibili ai minori, ove le misure di protezione saranno amplificate e sarà vietata la pubblicità mirata. A tal proposito si è pensato all'introduzione di clausole contrattuali contenenti obblighi a tutela dei diritti fondamentali degli utenti, con particolare riferimento alle modalità di informazione e al trattamento dei dati personali[27].

7. *Segue.* Punti critici

Si ritiene che la decisione esaminata non solo valorizzi il principio dell'interesse superiore del minore, che deve essere considerato preminente, così come tutelato dalle norme di diritto nazionale ed interna-

[27] *Digital services act, la Ue a una svolta: cosa cambia per utenti, aziende e big tech*, in *https://www.agendadigitale.eu/mercati-digitali/digital-services-act-la-ue-a-una-svolta-cosa-cambia-per-utenti-aziende-e-big-tech/*, 2022.

zionale – con la conseguenza che nessun minore può subire intromissioni arbitrarie o illegali che ledono la sua vita privata, la sua famiglia, la sua casa, il suo onore o la sua reputazione – ma che possa anche essere vista come un possibile punto intermedio verso un traguardo ermeneutico ulteriore.

Infatti, per quanto tale principio sia stato introdotto con riferimento al contesto soprattutto familiare, esso ben potrebbe trovare una vasta applicazione in quella società con cui questi è chiamato a relazionarsi e ad integrarsi. In tal modo, dovendosi garantire un sereno inserimento del minore nel contesto sociale, non sarebbe errato asserire che possa parlarsi – nel caso di specie – di un interesse superiore dell'interessato minore d'età da applicare in modo da prevenire contrasti insanabili nei confronti della società stessa. In più, in ragione della funzione sociale che il quarto considerando del GDPR[28] assegna al trattamento dei dati personali e della funzione di indirizzo ermeneutico pacificamente riconosciuta ai considerando degli atti normativi europei, sarebbe possibile ipotizzarsi una futura evoluzione del principio di modo che possa parlarsi dell'interesse superiore dell'interessato, anche laddove non sia un minore.

Ma, ancor di più, il DSA introduce una nuova effettiva tutela, di tipo preventivo, che si va ad affiancare ai normali sistemi di tutela giurisdizionale ed amministrativa attualmente esistenti. Infatti, laddove l'Autorità indipendente ovvero giudiziaria intervengano, si tratterà pur sempre di un intervento *post factum* e per ciò inidoneo (in ragione delle immense velocità raggiungibili in rete) a fornire una reale protezione alle vittime di trattamenti di dati totalmente illegittimi (si pensi anche al *cyberbullismo* ovvero al *revenge porn*). Per contro, la previsione di un intervento dello stesso ISP consente di bloccare qualsiasi fenomeno

[28] Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

allo stato iniziale, limitando i danni in attesa dell'ingresso in scena delle Autorità nazionali ed europee.

Pertanto, qualsiasi ipotesi di trattamento dei dati che ricalchi la condotta dell'ex Sindaco di Messina potrebbe essere arginata in modo preventivo, evitandosi così un trattamento sanzionatorio quale è stato quello fornito attraverso il provvedimento in esame, dal momento che è stata comminata una sanzione di 50.000,00 euro nell'anno 2021 per fatti effettivamente commessi nel 2019.

This article focuses on the protection of the minor's personal data and the exercise of the public function among European laws, application practices and reforms.

In particular, starting from some cases dealt by the Italian Privacy Authority, an excursus is made on what is the privileged treatment reserved for data protection for minors in the GDPR and in the Italian Privacy Code, putting it in relation with the special rules provided for the exercise of public functions. In the final analysis, these are the reforms currently being studied by the European legislator, such as the Digital Service Act and the Digital Market Act.

Il presente articolo si concentra sul rapporto tra la protezione dei dati personali del minore e l'esercizio della funzione pubblica con riguardo sia alla normativa europea ed italiana, che alle recenti riforme del settore.

In particolare, a partire da alcuni casi trattati dall'Autorità Garante della Privacy italiana, viene svolto un excursus con riferimento al trattamento dei dati disciplinato dal GDPR e dal Codice Privacy italiano. In ultima analisi, si analizzano le riforme del legislatore europeo, quale il regolamento sui servizi digitali e il regolamento sul mercato digitale.