Protezione dei dati sensibili e uso di *App* per il benessere delle donne. Una questione di consapevolezza

Arianna Thiene*

SENSITIVE DATA PROTECTION AND APP USE FOR WOMEN'S WELL-BEING. A QUESTION OF AWARENESS

ABSTRACT: The article addresses the issue of APPs dedicated to women's health and well-being from the perspective of the legal rules applicable to the processing of personal data in light of Regulation (EU) 2016/679. Particular attention is paid to the topic of digital education in view of the fact that the main users of these devices are girls.

KEYWORDS: Health Mobile App; Regulation (EU) 2016/679; data protection; teenagers; digital literacy

ABSTRACT: L'articolo affronta il tema delle APP dedicate alla salute e al benessere delle donne dal punto di vista delle regole giuridiche applicabili al trattamento dei dati personali alla luce del Regolamento (UE) 2016/679. Particolare attenzione viene dedicata al tema dell'educazione digitale in considerazione del fatto che le principali fruitrici di questi dispositivi sono le adolescenti.

PAROLE CHIAVE: Health Mobile App; Regolamento (UE) 2016/679; protezione dei dati; adolescenti; educazione digitale

SOMMARIO: 1. *Health Mobile App*, uno strumento prezioso il miglioramento dello stile di vita delle donne: premesse – 2. Dati comuni e dati sensibili: una distinzione necessaria alla luce del Regolamento (UE) 2016/679 – 3. Le regole per il trattamento di categorie particolari di dati personali: il primato del consenso – 4. La tutela dei dati personali delle adolescenti – 5. Strategie per un'efficace educazione digitale alla luce della legge 20 agosto 2019, n. 92 – 6. Nuovi orizzonti per la costruzione di uno *European Health Data Space*: cenni conclusivi.

1. *Health Mobile App*, uno strumento prezioso per la salute e il benessere delle donne: premesse

Come è stato messo in luce il settore *FEMTECH* sta inesorabilmente avanzando perché capace di fondere la tecnologia con i bisogni quotidiani legati alla salute e al benessere delle donne, in particolare il monitoraggio del ciclo mestruale e della fertilità[1].

* *Professoressa associata di Diritto privato, nell'Università degli Studi di Ferrara. Mail: arianna.thiene@unife.it.*
Contributo sottoposto a referaggio anonimo.

[1] È così possibile prevedere i cicli mestruali futuri, determinare le finestre fertili, monitorare gli sbalzi di umore, la temperatura corporea basale: cfr. B. CORBIN, *Digital Micro-Aggressions and Discrimination: FemTech and the*

Al fine di promuovere l'acquisizione di un uso consapevole di questi dispositivi già nel 2015 il Comitato Nazionale per la Bioetica raccomandava «l'istituzione di un osservatorio per il monitoraggio delle App e la costituzione di siti e/o portali accreditati scientificamente, la promozione di un'appropriata informativa e una trasparente comunicazione all'utente al momento dell'utilizzo dell'App, con una specifica attenzione ai minori e la promozione di studi sull'impatto dell'uso delle App, in particolare sull'identità personale e relazionale»[2].

Il moltiplicarsi di *app* specifiche per il benessere delle donne pone delicati interrogativi sul piano medico ed etico. In questo scritto si intende affrontare la questione relativa alle regole giuridiche applicabili al trattamento della grande mole di dati raccolti dalle applicazioni digitali mobili di uso quotidiano[3], informazioni capaci di rivelare gli aspetti più intimi della vita della persona, non solo quelli legati alla salute ma anche alle abitudini e all'orientamento sessuale[4].

Va subito premesso che le *app* dedicate al monitoraggio del ciclo e dell'ovulazione, inventate nel 2013 da Ida Tin, fondatrice danese di Clue, non prevedono di regola una forma di interazione (in tempo reale o differito) tra l'utente paziente e il professionista sanitario con la conseguenza che non sono riconducibili all'ambito della telemedicina[5]. Questi strumenti non sono, in linea generale[6], nep-

---

"Othering" of Women, in *Nova Law Review*, 44, 2020, 345. Il contributo è consultabile *https://ssrn.com/abstract=3630435*.

[2] Comitato Nazionale per la Bioetica, *"Mobile-Health" e applicazioni per la salute: aspetti bioetici*, 28 maggio 2015, p. 96. Il Documento è consultabile al sito *https://bioetica.governo.it/it/pareri/pareri-e-risposte/mobile-health-e-applicazioni-per-la-salute-aspetti-bioetici/*.

[3] «Si genera un'enorme quantità di dati complessi, eterogenei, velocemente e continuamente accumulati mediante il monitoraggio di parametri fisiologici che vengono raccolti, studiati, interpretati e correlati con modelli algoritmici»: Comitato Nazionale per la Bioetica, *"*Mobile-Health*" e applicazioni per la salute: aspetti bioetici*, cit., 106.

[4] «Il problema non investe solo i dati sanitari e medici, ma anche i dati desunti da app per il benessere e stili di vita. Si tratta di dati detti "grezzi" (*raw data*) che anche se non direttamente medici, combinati con altri dati, possono avere una rilevanza medica e consentire la definizione di un profilo sanitario dell'utente, con riferimento alla salute e ai rischi per la salute»: Comitato Nazionale per la Bioetica, *"*Mobile-Health*" e applicazioni per la salute: aspetti bioetici*, cit., 106-107. Cfr. L. CADUFF *et al.*, *Privacy issues in healthcare and their mitigation through privacy preserving technologies*, in D. CIRILLO, S. CATUARA-SOLARZ e E. GUNEY (edited by), *Sex and Gender Bias in Technology and Artificial Intelligence. Biomedicine and Healthcare Applications*, Amsterdam, 2022, 205 ss.; B. SAINZ-DE-ABAJO, I. DE LA TORRE-DIEZ, S. GONGORA-ALONSO, M. LOPEZ-CORONADO, *Privacy issues in eHealth and mHealth apps*, in M. TZANOU (edited by), *Health Data Privacy under GDPR. Big Data Challenges and Regulatory Responses*, London, 2021, 71 ss.

[5] Come osserva C. IRTI, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e Mercato*, 2023, 1, 34. In arg. si veda il Documento "Telemedicina – Linee di indirizzo nazionale", frutto di un'intesa, intervenuta nel 2014, tra Governo, Regioni e Province autonome di Trento e Bolzano. Per approfondire cfr. C. BOTRUGNO, *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Pol. dir.*, 4, 2014, 639 ss.; G. BINCOLETTO, mHealth app *per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in questa *Rivista*, 2021, 4, 381 ss.; M. FACCIOLI, *Telemedicina e responsabilità civile degli operatori e delle strutture sanitarie*, in S. TROIANO (a cura di), *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, Napoli, 2022, 293 ss.; N. POSTERARO, *La telemedicina*, in V. BONTEMPI (a cura di), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Roma, 2022, 201 ss.; M. FOGLIA, *La relazione di cura nell'era della comunicazione digitale*, in *MediaLaws*, 2020, 77 ss.

[6] La questione è affrontata diffusamente in questo *Focus* da E. MAESTRI, Femtech *e l'avvento della medicina pervasiva: incubo o nobile sogno?*.

pure inquadrabili come dispositivi medici (e cioè come *Medical Mobile App*)[7] secondo quanto previsto dal Regolamento UE 2017/745, che richiede per questi ultimi un'espressa destinazione ad uso medico (ad es. diagnosi, prevenzione, monitoraggio, prognosi, trattamento della malattia)[8]. Si tratta in definitiva di generiche *Health Mobile App*, che beneficiano di una libera circolazione e commercializzazione in quanto strumenti di controllo del benessere e dello stile di vita dell'utente[9].

Il fatto che la conclusione di questi contratti di licenza d'uso del *software* non preveda il pagamento di un corrispettivo in denaro da parte delle utenti non deve trarre in inganno. Sappiamo bene che i dati personali, definiti il nuovo petrolio della società digitale[10], oggi assumono una valenza economica definita: l'autorizzazione a trattare i dati personali può essere configurata come corrispettivo per la fruizione di servizi[11]. I contenuti forniti dall'utente si rivelano preziosi per gli interessi patrimoniali e commerciali dei titolari del trattamento produttori di *software*[12].

Queste applicazioni devono quindi rispettare la disciplina legale in materia di protezione dei dati personali. Ed è proprio dalla normativa europea che si deve partire per cercare di ricostruire le regole applicabili al trattamento dei dati personali anche al fine di capire quali sono le modalità capaci di accrescere la consapevolezza delle utenti, spesso giovanissime, di questo mercato in espansione. Non è possibile, ovviamente, rassegnarsi all'idea che la ragione tecnologica possa prendere il sopravvento sulle esigenze di protezione della sfera intima della persona.

---

[7] Per una ricognizione delle *app* sanitarie rinvio a R.M. Colangelo, App *mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice* privacy *novellato e chiarimenti del Garante*, in *Aut. loc. e serv. soc.*, 2019, 280 ss.

[8] G. Bincoletto, mHealth app *per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, cit., 388. *Amplius* C. Perlingieri, *eHealth and Data*, in R. Senigaglia, C. Irti, e A. Bernes (a cura di), *Privacy and Data Protection in Software Services*, Berlino, 2022, 127 ss.

[9] I. Rapisarda, *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app *mediche*, in *Nuove leggi civ. comm.*, 2023, 186. Ficcanti le critiche di C. Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, cit., 35, secondo cui in questo modo i produttori di *software* per il benessere e stile di vita (*Health MobileApp*) riescono ad aggirare tutte le regole e i controlli previsti per i *software* qualificati come dispositivi medici (*Medical MobileApp*).

[10] F. Pizzetti, *Il prisma del diritto all'oblio*, in Id. (a cura di), *Il caso del diritto all'oblio*, Milano, 2013, 41.

[11] Al nesso sinallagmatico tra servizi digitali e dati personali sono stati dedicati studi anche monografici: A. De Franceschi, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017; G. Versaci, *La contrattualizzazione dei dati personali*, Napoli, 2020. *Adde* le riflessioni di E. Battelli, *I modelli negoziali di* business *degli operatori digitali "a prezzo zero" non sono "gratuiti"*, in *Contratti*, 2022, 355 ss.

[12] A. Thiene, *L'inconsistente tutela dei minori nel mondo digitale*, in *Studium iuris*, 2012, 532. I nodi problematici relativi alla profilazione e all'utilizzo dell'intelligenza artificiale sono approfonditi in questo *Focus* dalle pagine di Stefano Corso, a cui rinvio. Ci si limita qui a ricordare che l'opacità del sistema di profilazione è da tempo segnalata in letteratura: E. Maestri, *Il minore come persona digitale. Regole, tutele e* privacy *dei minori sul* Web, in A. Thiene, E. Marescotti (a cura di), *La scuola al tempo dei* social network, in *Annali online della Didattica e della Formazione Docente*, 9, 13, 2017, 14; I. Garaci, *Minori e pubblicità mirata*, in *Diritto mercato tecnologia*, www.dimt.it, 24 gennaio 2022; Ead., *Profili di tutela delle persone vulnerabili nell'ecosistema digitale. Il divieto di profilazione dei minori di età ai fini di* marketing, in S. Orlando e G. Capaldo (a cura di), *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2022, 89 ss.; C. Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, cit., 47.

2. Dati comuni e dati sensibili: una distinzione necessaria alla luce del Regolamento (UE) 2016/679.

Il Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati, ha accolto la sfida di coniugare i diritti della persona con le esigenze di mercato. Da un lato l'art. 1, par. 2, del GDPR pone tra i suoi obiettivi la necessità di «proteggere i diritti e le libertà fondamentali delle persone e in particolare il loro diritto alla protezione dei dati personali». Dall'altro emerge, soprattutto dalla lettura dei considerando, l'attenzione per la dimensione economica dei dati, oggetto di sempre crescente mercificazione, al punto che si afferma che lo scopo precipuo del Regolamento è quello di favorire un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno (7° considerando)[13].

Non è sempre facile distinguere la dimensione ideale dei dati personali, che sono frammenti dell'identità personale[14], da quella patrimoniale perché spesso la sfera dell'*essere* si interseca e si confonde con quella dell'*avere*[15].

Questa natura anfibologica e complessa dei dati ha evidentemente condizionato la scelta del legislatore europeo di adottare due diversi modelli di trattamento a seconda del loro contenuto informativo.

Per i dati comuni o neutri, perché incapaci di rivelare la condizione intima ed esistenziale della persona, la dimensione circolatoria sembra decisamente prevalere. Effettuando un ponderato bilanciamento tra diritto alla protezione dei dati personali ed esigenze rilevanti sotto il profilo economico e sociale[16], l'art. 6, par. 1, GDPR prevede diverse condizioni di liceità del trattamento dei dati, che si trovano tutte sullo stesso piano. In questo elenco il consenso dell'interessato non svolge un ruolo da protagonista (lett. *a*), ma è semplicemente una tra le diverse basi giuridiche che giustificano il trattamento dei dati[17]. Non è nemmeno quella che ricorre più frequentemente, trovando spesso applicazione anche la previsione contenuta alla lettera *b*, e cioè il caso di trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Evidente è l'esigenza di favorire un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno[18].

---

[13] G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 5 ss. Cfr. N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla* privacy, in Ead. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 35 ss.

[14] G. Finocchiaro, *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro e F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, 151 ss. (s. 153).

[15] A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, 415. Cfr. A. De Franceschi, in R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta (a cura di), *Codice della* privacy *e* data protection*,* Milano, 2021, *sub* art. 4, reg. Ue n. 679/2016, 156 ss. (s. 158 ss.)

[16] V. il considerando 4. Cfr. F. Bravo, *Il "diritto" a trattare dati personali*, Milano, 2018, 149 ss. e 188 ss.; A. Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2017, 586 ss.; A. Iuliani, *Note minime in tema di trattamento dei dati personali*, in *Eur. e dir. priv.,* 2018, 293 ss.

[17] A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione,* in *Diritto mercato tecnologia*, 2017, 4.

[18] R. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, 760 ss.

Dalla lettura dell'art. 9 del GDPR, dedicato al trattamento di categorie *particolari* di dati personali, emerge, invece, la scelta del legislatore europeo di escludere tendenzialmente dai circuiti conoscitivi le informazioni che attengono alla sfera intima e privata della persona. Per quelle categorie di dati personali che «sono particolarmente sensibili per loro natura e che meritano una protezione più intensa dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali»[19], il primo paragrafo della previsione in esame stabilisce un divieto di trattamento. Si fa esplicito riferimento ai dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, ai dati genetici, ai dati biometrici (intesi a identificare in modo univoco una persona fisica), ai dati relativi alla salute o alla vita sessuale della persona.

Questo divieto, come vedremo, ha un valore sistematico, perché epifania della già rammentata essenza personalista. Questa rigidità non coglie certo di sorpresa l'interprete, anzi è perfettamente in linea con i principi generali del sistema costituzionale-privatistico europeo, tratteggiato dalla Carta dei diritti fondamentali dell'Unione europea, in particolare dall'art. 7, *Rispetto della vita privata e della vita familiare*, e dall'art. 8, *Protezione dei dati di carattere personale*, che ben evidenziano come il diritto alla protezione dei dati personali sia uno sviluppo e un arricchimento del diritto alla riservatezza[20] nel segno di una visione monista dei diritti della personalità[21]. Il divieto di raccogliere dati legati alla sfera intima è, infatti, una forma di tutela della dignità della persona perché impedisce, tra l'altro, l'utilizzo delle informazioni per scopi discriminatori[22].

Come tosto si indagherà, nel secondo paragrafo dell'art. 9 sono elencate le eccezioni legali al divieto di trattamento, giustificate da finalità pubbliche che legittimano la circolazione di dati sensibili. Dal punto di vista civilistico, si presentano come cause di esclusione dell'antigiuridicità, da interpretare in maniera rigorosamente restrittiva e in modo favorevole all'interessato[23].

Anche se il Regolamento europeo n. 679 del 2016 riserva molta attenzione agli aspetti definitori con una disposizione, l'articolo 4, che in modo analitico e preciso chiarisce cosa debba intendersi per dati genetici[24], per dati biometrici[25] e per dati relativi alla salute[26], i confini tra le singole categorie di dati

[19] Considerando 51.

[20] I confini tra questi due diritti sono ricostruiti da M. Bianca, *Il minore e i nuovi media*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età*, Pisa, 2019, 152 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, 417.

[21] Per i riferimenti cfr. A. Thiene, *La tutela della personalità dal* neminem laedere *al* suum cuique tribuere, in *Riv. dir. civ.*, 2014, 373 ss.

[22] Cfr. S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, spec. 84; G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, 732. V. anche M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 179 ss., spec. 239 s.; L. Bozzi, *I dati del minore tra protezione e discriminazione: per una lettura non retorica del fenomeno*, in *Eur. e dir. priv.*, 2020, 271.

[23] Sia consentito il rinvio ad A. Thiene, *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR*, in A. Thiene e S. Corso (a cura di), *La protezione dei dati sanitari.* Privacy *e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, 2023, 13; Ead., in R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta (a cura di), *op. cit.*, *sub* art. 9, reg. Ue n. 679/2016, *I. Profili generali*, 243.

[24] In base all'art. 4, n. 13, i dati genetici sono «i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta

sono naturalmente mobili al punto che spesso non è facile neppure tracciare con sicurezza una demarcazione netta tra dati comuni e dati sensibili[27].

Con specifico riguardo alle *app* per la salute e il benessere delle donne, le informazioni inserite potrebbero apparire di primo acchito neutrali rispetto all'intimità sensibile della persona. Uno sguardo più consapevole aiuterebbe a mettere in luce che si tratta di dati potenzialmente idonei a svelare lo stato di salute, l'orientamento sessuale e finanche le convinzioni religiose. Il nocciolo duro della *privacy*, quindi[28]. Per questo, in linea con le indicazioni della nostra giurisprudenza di legittimità[29], sarebbe preferibile prediligere un'interpretazione estensiva dei confini delle singole categorie particolari di dati, finalizzata a ricomprendere anche le informazioni capaci di rivelare *indirettamente* gli aspetti esistenziali più riservati[30].

3. Le regole per il trattamento di categorie particolari di dati personali: il primato del consenso

Tra le dieci eccezioni al divieto di trattamento, espressamente previste dall'art. 9 GDPR, particolare rilevanza per il tema che stiamo trattando assume il consenso dell'interessato, espressione del potere di autodeterminazione della persona nelle scelte esistenziali e baluardo a difesa della sfera intima e privata.

---

persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione».

[25] In base all'art. 4, n. 14, i dati biometrici sono «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

[26] In base all'art. 4, n. 15, i dati relativi alla salute sono: «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». Per approfondimenti cfr. P. GUARDA, *I dati sanitari*, in V. CUFFARO, R. D'ORAZIO, e V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 591 ss.

[27] Cfr. G. FARES, *The processing of personal data concerning health according to the EU Regulation*, in ID. (a cura di), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, Torino, 2021, 17 ss., spec. 19 ss. Sulle "zone grigie" di interpretazione della definizione, v. W. SCHÄFKE-ZELL, *Revisiting the definition of health data in the age of digitalized health care*, in *International Data Privacy Law*, 12, 1, 2022, 33 ss.

[28] G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella società dell'informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, 1997, 375; V. ZENO-ZENCOVICH, in E. GIANNANTONIO, M. LOSANO e V. ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, *sub* art. 22, 201, 203. V. anche S. RODOTÀ, *Tecnologie e diritti*, cit., 84; ID., Privacy *e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, 1991, 524.

[29] Confermando l'orientamento più rigoroso già sostenuto da Cass. 19.5.2014, n. 10947, in *Foro it.,* 2015, I, 121, le sezioni unite hanno ritenuto che l'indicazione contenuta nel bonifico bancario *pagamenti ratei arretrati bimestrali e posticipati l. n. 210 del 1992*, configuri un dato personale idoneo a rivelare lo stato di salute del beneficiario dell'indennizzo: Cass., sez. un., 27.12.2017, n. 30981, in *Giur. it*., 2018, 2639 con nota di A. RICCI.

[30] F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm.*, 2017, I, 1232 ss.

In tutte le ipotesi di *Health App* per la salute e il benessere delle donne il consenso autorizzativo, che ha struttura necessariamente unilaterale, costituisce la base giuridica che legittima la raccolta e il trattamento dei dati, anche quelli più riservati, delle utenti.

Il Regolamento (UE) 2016/679 dedica, nel suo complesso articolato, particolare attenzione alle caratteristiche che deve presentare il consenso.

In base a quanto previsto dall'art. 4, n. 11, deve configurarsi come una manifestazione di volontà *libera, specifica, informata e inequivocabile* dell'interessato[31]. A queste indicazioni si aggiungono quelle specificamente previste per i dati c.d. sensibili dall'art. 9, par. 2, lett. *a*: il consenso deve essere *esplicito* e reso per una o più *finalità specifiche*[32]. Al riguardo in modo incisivo si parla di consenso *granulare*, in quanto destinato a svolgere una funzione non solo permissiva, ma anche regolativa delle fattispecie circolatorie[33]. Questo si traduce in concreto nella necessità per il titolare del trattamento di creare differenti richieste di consenso, precedute ovviamente dalla relativa informativa, a seconda delle diverse finalità della raccolta di dati[34].

Tutte queste cautele, già presenti nella Direttiva 1995/46, hanno accompagnato naturalmente l'introduzione nel nostro sistema del Fascicolo Sanitario Elettronico, avvenuta con d.l. n 179 del 2012, convertito con l. n. 221 del 2012. Al riguardo merita segnalazione, perché sembra preannunciare una diversa sensibilità in materia di protezione dei dati sanitari tra salute pubblica e diritto alla riservatezza, una novità introdotta durante il periodo pandemico[35], e cioè l'eliminazione della necessità del consenso per l'alimentazione del Fascicolo Sanitario Elettronico, avvenuta con l'abrogazione del comma 3-*bis* dell'art. 12 dell'appena menzionato d.l. n. 179 del 2012 da parte del d.l. 19 maggio 2020, n. 34[36].

---

[31] Nella giurisprudenza sovranazionale v. Corte giust. UE, 1°.10.2019, causa C-673/17 (*Planet49*), in *Dir. fam. e pers.*, 2020, 133 ss.; Corte giust. UE, 11.11.2020, causa C-61/19 (*Orange Romania*), in *Foro amm.*, 2020, 2073.

[32] Cfr. G. De Cristofaro, *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in T. Pertot (a cura di), *Rechte an Daten*, Tubinga, 2020, 158.

[33] La necessità di un consenso granulare declinato per ogni tipo di finalità è sottolineata in modo molto opportuno dal Comitato Nazionale per la Bioetica, *"Mobile-Health" e applicazioni per la salute: aspetti bioetici, 28 maggio*, cit., p. 109.

[34] Cfr. S. Orlando, *Per un sindacato di liceità del consenso* privacy, in *Persona e mercato*, 4, 2022, 527 ss.

[35] La diffusione del Fascicolo Sanitario Elettronico rientra tra gli obiettivi del Piano Nazionale di Ripresa e Resilienza: per approfondimenti cfr. G. Lofaro, *La sicurezza dei dati sanitari nelle* smart technologies *quale strumento di realizzazione del diritto alla salute tra telemedicina ed intelligenza artificiale*, in www.dirittifondamentali.it, 16 giugno 2022, 120 ss.

[36] S. Corso, *Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in A. Thiene e S. Corso (a cura di), cit., 91 ss. È una sensibilità che muove verso declinazioni del principio di solidarietà, in ambito giuridico-tecnologico, secondo un paradigma diverso, appunto, da quello rappresentato dal consenso dell'interessato. Cfr. M. Ciancimino, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in *Dir. fam. e pers.*, 2022, 68. V. anche il contributo di S. Corso, in questo *focus*. Più in generale, sul principio di solidarietà, specialmente nel diritto privato, G. Alpa, *Solidarietà. Un principio normativo*, Bologna, il Mulino, 2022. Il problema è peraltro legato alla sostenibilità delle tecnologie emergenti, della quale il sistema si deve fare carico. I. Garaci e R. Montinaro (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, 2023. Così, pure, «Oltre alla dimensione individuale, viene in rilievo negli strumenti giuridici sovranazionali una nuova dimensione, quella collettiva o sociale». R. Montinaro, *La sostenibilità dell'innovazione digitale. Un'introduzione*, *ivi*, 16.

Il presente contributo non è la sede per analizzare le altre nove clausole derogative, idonee a rimuovere il divieto di trattamento dei dati relativi alla salute (e non solo). Sono ovviamente frutto di un bilanciamento e sono concepite per favorire finalità di ricerca scientifica (art. 9, par. 2, lett. *j*); scopi di cura, ossia la finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale (art. 9, par. 2, lett. *h*); motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici (art. 9, par. 2, lett. *i*)[37].

È interessante, tuttavia, richiamare il contenuto del provvedimento del nostro Garante per la protezione dei dati personali del 7 marzo 2019, n. 55, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*[38]. Nel Documento viene definitivamente chiarito che, a differenza di quanto accadeva prima dell'entrata in vigore del Reg. UE n. 679 del 2016, non è più necessario che il professionista sanitario, soggetto al segreto professionale secondo quanto previsto dall'art. 9, par. 3 GDPR, acquisisca il consenso del paziente per i trattamenti di dati finalizzati alla finalità di cura oggetto della prestazione richiesta. Questa nuova regola, fondata sulla deroga di cui alla lettera *h* del par. 2, vale in ogni circostanza indipendentemente dal fatto che la cura venga erogata all'interno di una struttura sanitaria pubblica o privata o nell'ambito di un'attività libero professionale.

Per le ragioni di ordine sistematico che abbiamo cercato di mettere in luce in queste pagine, la previsione va interpretata in senso rigorosamente restrittivo, con la conseguenza che i trattamenti dei dati non strettamente necessari alla finalità di cura dovranno fondarsi sulle altre condizioni di liceità indicate dall'art. 9 GDPR, come sul consenso dell'interessato che ancora oggi sembra svolgere un ruolo da protagonista per la raccolta dei dati sensibili. È lo stesso provvedimento del 2019 a contenere un'utile elencazione, a titolo esemplificativo, di trattamenti in ambito sanitario che richiedono ancora il consenso esplicito dell'interessato: 1) trattamenti dei dati connessi all'utilizzo di *app* mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari, per finalità diverse dalla telemedicina; 2) trattamenti dei dati finalizzati alla fidelizzazione della clientela, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario; 3) trattamenti di dati effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali; 4) trattamenti di dati effettuati da professionisti sanitari per finalità commerciali o elettorali[39].

È evidente che questa esclusione *a fortiori* riguarderà le *app* per il benessere e la salute delle donne, che continuano a richiedere il consenso *esplicito* dell'interessato reso per una o più *finalità specifi-*

[37] G. Fares, *The processing of personal data concerning health according to the EU Regulation*, cit., 21. Si v., in arg., anche lo studio di M. Tzanou (a cura di), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Responses*, Londra, 2021.

[38] Consultabile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942.

[39] Gli effetti sulle *app* per il benessere e la salute del provvedimento n. 55 del 2019 sono analizzati da I. Rapisarda, *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app *mediche*, cit., 198-199; R.M. Colangelo, App *mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice* privacy *novellato e chiarimenti del Garante*, cit., 278-279.

ISSN 2284-4503

che[40]. Al riguardo non si ripeterà mai abbastanza che il consenso costituisce *davvero* un valido presupposto per fondare il trattamento dei dati (in particolare quelli sensibili come quelli relativi alla salute e alla vita sessuale), solo se è preceduto da un'informativa facilmente comprensibile e chiara nel definire gli elementi essenziali del trattamento, con apposita specificazione delle finalità perseguite con la collezione di informazioni spesso di giovanissime utenti[41].

4. La tutela dei dati personali delle adolescenti

È un dato di fatto che le *app* per il benessere e la salute delle donne sono diffuse soprattutto tra le adolescenti[42] che, di fronte alle nuove tecnologie, vantano abilità e competenze spesso sconosciute al mondo degli adulti[43].

Il Comitato nazionale per la Bioetica nel 2015 ha messo in luce, in modo tempestivo e opportuno[44], le criticità sul piano bioetico, a cui va aggiunto il rischio che a condizionare le ragazze nella scelta del tipo di *app* non siano considerazioni legate al riconoscimento di una validità sul piano scientifico, ma altri fattori tra cui il seguire acriticamente l'indice di gradimento espresso da precedenti fruitrici.

Qui affrontiamo il tema dallo specifico punto di vista del diritto alla protezione dei dati personali delle adolescenti.

Innanzitutto è necessario chiarire chi deve autorizzare il trattamento dei dati (comuni e sensibili) delle persone minori di età. Troviamo la risposta sempre all'interno del Regolamento (UE) 2016/679[45]. Con esclusivo riguardo ai servizi offerti dalla società dell'informazione[46] (e quindi non per l'ambiente

[40] R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, 774, secondo cui questo requisito «assume una funzione delimitante dello spazio e della misura dell'interferenza altrui nella sfera privata».

[41] «Ne consegue anche l'esigenza di offrire, proprio nei confronti dei minori, informazioni semplici, concise, che includono anche riferimenti educativi che sollecitino la presa di coscienza dei problemi, con un linguaggio adatto»: Comitato Nazionale per la Bioetica, *"*Mobile-Health*" e applicazioni per la salute: aspetti bioetici*, cit., 106. Anche per il GDPR «i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente» (considerando 58).

[42] Sono al secondo posto tra le *app* scaricate dalle adolescenti: B. CORBIN, *Digital Micro-Aggressions and Discrimination: FemTech and the "Othering" of Women*, cit., 345.

[43] A questa disinvoltura non corrisponde sempre una consapevolezza sul valore dei propri dati personali: cfr. I. GARACI, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale***,** in *Nuove leggi civ. comm.*, 2021, 801-802, secondo cui il minore è diventato un consumatore più precoce rispetto al mondo analogico, ma rimane un consumatore particolarmente vulnerabile. Importanti suggerimenti su come aiutare i più giovani a tutelarsi di fronte ai rischi connessi allo sviluppo del mondo digitale sono contenuti nel vademecum del Garante per la protezione dei dati personali*, La Scuola a prova di* privacy, edizione 2023, consultabile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9887111.

[44] Comitato Nazionale per la Bioetica, *"*Mobile-Health*" e applicazioni per la salute: aspetti bioetici*, cit., 110.

[45] Per approfondimenti sulla condizione del minore nella prospettiva del reg. Ue 2016/679 cfr. E. DE BELVIS, *Dati personali, rapporti familiari e tecnologie digitali*, Napoli, 2022. Si vedano, inoltre, i contributi contenuti nel volume curato da A. ANNONI e A. THIENE, *Minori e* privacy*. La tutela dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Napoli, 2019.

[46] Per la definizione di servizio della società dell'informazione l'art. 4, n. 25 del GDPR rinvia alla definizione molto ampia prevista dall'art. 1, par. 1, della Direttiva (UE) 2015/1535, che fa riferimento a «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un

off line)[47] l'art. 8 fissa a sedici anni l'età in cui il minore acquista la capacità per dare il consenso al trattamento dei propri dati personali[48]. Al di sotto di questa soglia di età il trattamento è lecito solo se e nella misura in cui il consenso è prestato dal titolare della responsabilità genitoriale[49].

La previsione accorda agli Stati membri la possibilità di abbassare fino a tredici anni l'età per l'accesso autonomo alla società digitale[50].

Il terzo paragrafo dell'art. 8 GDPR precisa che le regole appena richiamate non pregiudicano le disposizioni generali del diritto dei contratti degli Stati membri. Il riferimento va alle norme sulla validità e sull'efficacia del contratto stipulato da un minore di età. Questo in concreto significa che vi è una diversificazione tra le regole per il consenso al trattamento dei dati da un lato, e quelle relative al consenso contrattuale dall'altro[51].

Non possiamo addentrarci nella questione[52]; ricordiamo solo che, per superare la granitica previsione contenuta all'art. 2 del cod. civ. e riconoscere uno spazio di autonomia ai c.d. grandi minori anche sotto il profilo negoziale, l'unica soluzione sembra ancora oggi quella di fare ricorso all'evanescente categoria degli atti minuti della vita quotidiana, fingendo una procura tacita dei genitori[53]. Questa

---

destinatario di servizi»: P. ARGANELLI, App*,* Privacy *e minori. La tutela dei minori in internet tra autodeterminazione informativa e fruizione dei contenuti digitali*, in *De Iustitia*, 2021, 2, 93.

[47] La contraddizione presente nel nostro sistema è evidente e deriva dal fatto che il legislatore europeo non aveva ovviamente la competenza a prevedere una regola generale in materia di consenso al trattamento dei dati personali dei minori. Nel nostro ordinamento in mancanza di una previsione specifica rimane, per la dimensione off line, la regola della rappresentanza genitoriale per il consenso al trattamento dei dati anche dei c.d. grandi minori: cfr. A THIENE, *Gioventù bruciata online: quale responsabilità per i genitori?,* in A. ANNONI, A. THIENE (a cura di), *Minori e* privacy*. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, cit., 50.

[48] C. CAMARDI, *Relazione di filiazione e* privacy*. Brevi note sull'autodeterminazione del minore*, in *Jus civile*, 2018, 836; F. NADDEO, *Il consenso al trattamento dei dati personali del minore,* in *Dir. inf.,* 2018*,* 50; E. LUCCHINI GUASTALLA, Il nuovo regolamento europeo dei dati personali: i principi ispiratori, in *Contr. e impr*., 2018, 116; M. ASTONE, *L'accesso dei minori di età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) e i suoi riflessi sulla protezione dei dati personali*, in *Contr. e impr*., 2019, 614 ss.

[49] A. THIENE, *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in *Fam. e dir.*, 2017, 172.

[50] In ossequio al *Children's Online Privacy Protection Act* (COPPA), che obbliga le piattaforme a chiedere l'autorizzazione dei genitori prima di raccogliere informazioni personali su bambini minori di tredici anni: C. SARTORIS, *Minors' data protection between e-learning and social network platforms*, in *European Journal of Privacy Law & Technologies*, 2020, 2, 143 (nota 9); M. MACENAITE, E. KOSTA, *Consent for processing children's personal data in the EU: following in US footsteps*?, in *Information & Communications Technology Law*, 2017, 146 ss.; E. LIEVENS, V. VERDOODT, *Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, 269 ss.

[51] P. VIRGADAMO, *Minori e nuovi* media, in A. CORDIANO e R. SENIGAGLIA (a cura di), *Diritto civile minorile*, Napoli, 2022, 364; I.A. CAGGIANO, Privacy *e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del regolamento UE 2016/676, tra diritto e tecno-regolazione*, in *Familia*, 2018, 13. Cfr., in termini più ampi, C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021.

[52] Si rinvia all'approfondita indagine di R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, secondo cui di fronte alla complessa fenomenologia dei rapporti di consumo, dove il minore è spesso protagonista, non ha più senso ragionare in termini di assoluta incapacità di agire. *Adde* I. GARACI, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale***,** cit., 806; G. VULPIANI, *L'utente minore online: tutela della* privacy *e attività negoziale*, in *Tecnologie e diritto*, 2021, 117-118.

[53] A. THIENE, *L'inconsistente tutela dei minori nel mondo digitale*, cit., 535.

teoria è stata più recentemente supportata da un'interpretazione analogica della disposizione contenuta all'art. 409, comma 2, del codice civile, riguardante gli atti necessari a soddisfare le esigenze della vita quotidiana del beneficiario dell'amministrazione di sostegno[54].

Per molte ragioni, non solo giuridiche, sarebbe stato auspicabile il mantenimento dell'indice temporale dei sedici anni per il consenso digitale al trattamento dei propri dati personali. In questo senso si era pronunciata l'Autorità garante per l'infanzia e l'adolescenza, chiamata ad esprimere un parere sullo schema di decreto legislativo recante *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento 2016/679/UE, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*[55].

Dopo un serrato confronto con psicologi, psichiatri, giuristi, tecnici della comunicazione, sociologi, pedagogisti era infatti arrivata al convincimento che «porre in capo a ragazze e ragazzi con meno di 16 anni il dovere di essere consapevoli circa le conseguenze del consenso al trattamento dei dati personali significa caricarli di un onere conoscitivo e di comprensione eccessivamente gravoso»[56].

Con decreto legislativo 10 agosto 2018 n. 101, il legislatore ha invece scelto di abbassare la soglia di età, introducendo nel c.d. Codice Privacy l'art. 2 *quinquies* (*Consenso del minore in relazione ai servizi della società dell'informazione*), secondo cui il minore che ha compiuto *i quattordici anni* può esprimere il consenso al trattamento dei propri dati in relazione all'offerta diretta dei servizi della società dell'informazione.

A bene vedere non si tratta di una scelta eccentrica, anzi per certi aspetti è coerente con precedenti valutazioni legislative, in particolare con la previsione contenuta all'art. 2 della l. 29 maggio 2017 n. 71, *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*, che prevede per i minori ultraquattordicenni la possibilità di inoltrare automaticamente al titolare del trattamento, al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione, il blocco dei contenuti (post, immagini, video, informazioni) oggetto di condotte aggressive avvenute *on line*[57].

---

[54] D. Di Sabato, *Gli atti a contenuto patrimoniale del minore*, in F. Rossi (a cura di), *Capacità e incapacità*, Napoli, 2018, 98; M. Cinque, *Il minore contraente. Contesti e limiti della capacità*, Padova, 2007, 120 ss.

[55] I compiti e i poteri dell'Autorità garante per l'infanzia e l'adolescenza, istituita con l. 12 luglio 2011, n. 112, per assicurare la piena attuazione e la tutela dei diritti e degli interessi delle persone minori di età in conformità a quanto previsto dalle Convenzioni internazionali, sono descritti da: L. Strumendo e P. De Stefani, *Il Garante dell'infanzia e dell'adolescenza*, in L. Lenti (a cura di) *Tutela civile del minore e diritto sociale della famiglia*, nel *Trattato di diritto di famiglia* diretto da Paolo Zatti, IV, Milano, 2012, 257 ss.; G. Morani, *Un nuovo organo monocratico, autonomo e indipendente, a tutela dei minori: l'autorità garante dell'infanzia e dell'adolescenza*, in *Dir. fam. e pers.*, 2012, 490 ss.

[56] È possibile visionare il parere sul sito dell'AGIA: https://www.garanteinfanzia.org/sites/default/files/atto-governo-22-parere-autorita-garante-infanzia-adolescenza.pdf.

[57] Al momento dell'approvazione della legge il riferimento ai quattordici anni era parso ad alcuni stravagante perché non teneva conto né della tendenza dei siti di socializzazione di fissare a tredici anni l'età minima per l'iscrizione dei fanciulli in autonomia né della scelta europea di alzare la tutela a sedici anni. V. A. Thiene, *I diritti della personalità dei minori nello spazio virtuale*, in A. Thiene, E. Marescotti (a cura di), *La scuola al tempo dei* social network, cit., 34.

In definitiva, da un'interpretazione sistematica di queste previsioni si evince che nel nostro ordinamento il minore quattordicenne ha il diritto a prestare il consenso autonomamente e può esercitare tutti i diritti previsti dalla normativa privacy, in particolare il diritto di opposizione e cancellazione[58].

5. Strategie per un'efficace educazione digitale alla luce della legge 20 agosto 2019, n. 92

Non possiamo nascondere la preoccupazione che questa scelta finisca per agevolare la realizzazione degli interessi economici dei fornitori dei servizi della società dell'informazione[59], anche in considerazione del fatto che le tecniche di tutela più efficaci sono quelle che si fondano sull'autodeterminazione, e quindi su una gestione consapevole dei dati personali (propri e altrui)[60].
È evidente a tutti che persiste un problema di adattamento culturale nei confronti di questa nuova sfida[61], ancora oggi si registra una scarsa sensibilità degli utenti (a prescindere dall'età) per i profili di *privacy*. Per questo di fronte ad un'evoluzione sempre più frenetica del mondo digitale dovrà essere sostenuto l'impegno educativo delle famiglie e delle scuole per la diffusione della conoscenza delle regole e dei principi racchiusi nella normativa europea ed italiana a tutela dei dati personali[62]. Si riscontra, in particolare, una scarsa consapevolezza circa le dinamiche di tipo economico-commerciale che attraversano il funzionamento delle piattaforme, definite in modo icastico come i nuovi padroni dell'Universo[63].
Si comprendono, quindi, le difficoltà e le paure dei genitori, smarriti nel loro compito di indicatori di regole nella crescita dei figli, per il semplice fatto di non essere essi stessi a conoscenza di regole per un'educazione digitale.
Dell'urgenza di ricostruire una comunità educante intorno a questi bisogni di conoscenza e protezione dei diritti fondamentali dei minori si è fatta carico la legge 20 agosto 2019, n. 92, che ha previsto per tutte le scuole di ogni ordine e grado l'insegnamento dell'educazione civica, inteso non come presenza di una nuova disciplina scolastica, ma come percorso educativo trasversale teso a formare studenti-cittadini, in grado di conoscere e attivarsi per favorire una trasformazione, un superamento della crisi, un miglioramento personale e comunitario.

---

[58] 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 *Nuovo Diritto Civile,* 2019, 2, 68 ss.
[59] C. Irti, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 2019, 619 ss.; G. Citarella, A. Venchiarutti, *Diritti della personalità dei minori*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma, 2022, 536.
[60] A. Thiene, *I diritti della personalità dei minori nello spazio virtuale*, cit., 37.
[61] B. C. Han, *La società della trasparenza*, Roma, 2014, 9 ss.; A. Masera, G. Scorza, *Internet. I nostri diritti*, Roma-Bari, 2016, 34 ss.; E. Maestri, *Il minore come persona digitale. Regole, tutele e* privacy *dei minori sul* Web, in A. Thiene, E. Marescotti (a cura di), *La scuola al tempo dei* social network, cit., 7 ss.; S. Nardi, *La famiglia e gli affetti nell'era digitale*, Napoli, 2020, 7 ss.
[62] «L'educazione dei minori, utenti attivi di tali nuove tecnologie, risulta particolarmente urgente e rilevante sul piano bioetico: una educazione che rafforzi strumenti di autodifesa dei giovani nell'ambito dell'uso delle tecnologie»: Comitato Nazionale per la Bioetica, *"*Mobile-Health*" e applicazioni per la salute: aspetti bioetici*, cit., 110.
[63] L'espressione è contenuta nel volume di F. Rampini, *Rete padrona. Amazon, Apple, Google* & co*. Il volto oscuro della rivoluzione digitale*, Milano, 2014.

Tra le tematiche indicate dall'art. 3, dedicato allo sviluppo delle competenze e obiettivi di apprendimento, troviamo l'educazione digitale, il cui contenuto è precisato nel successivo art. 5. Nell'ottica del legislatore l'offerta formativa deve prevedere, tenendo conto dell'età dei minori coinvolti, *almeno* le seguenti abilità e conoscenze digitali essenziali: a) analizzare, confrontare e valutare criticamente la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali; b) interagire attraverso varie tecnologie digitali e individuare i mezzi e le forme di comunicazione digitali appropriati per un determinato contesto; c) informarsi e partecipare al dibattito pubblico attraverso l'utilizzo di servizi digitali pubblici e privati; ricercare opportunità di crescita personale e di cittadinanza partecipativa attraverso adeguate tecnologie digitali; d) conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali, adattare le strategie di comunicazione al pubblico specifico ed essere consapevoli della diversità culturale e generazionale negli ambienti digitali; e) creare e gestire l'identità digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi, rispettare i dati e le identità altrui; utilizzare e condividere informazioni personali identificabili proteggendo se stessi e gli altri; f) *conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali*; g) essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere sé e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo[64].

È evidente che il successo di questo programma richiede un approccio multidisciplinare[65] e il coinvolgimento di tutti gli attori educativi, in primo luogo le famiglie[66]. Non senza significato l'art. 7 stabilisce espressamente che, al fine di valorizzare l'insegnamento dell'educazione civica e di sensibilizzare gli studenti e le studentesse alla cittadinanza responsabile, la Scuola deve rafforzare la collaborazione con le famiglie, anche integrando il Patto educativo di corresponsabilità.

Per riaccendere il perduto incantesimo relazionale è arrivato davvero il momento di abbandonare la fallimentare rigidità e il vuoto formalismo che continua a caratterizzare i loro rapporti. È necessario *incontrarsi* sui contenuti che sono proprio quelli indicati dalla legge n. 92 del 2019: oltre all'educazione digitale, dovrà essere avviato un dialogo sui principi e valori della nostra Costituzione; sugli obiettivi della Agenda 2030 per lo sviluppo sostenibile; sul rispetto dell'ambiente;

[64] Per lo sviluppo di una piena cittadinanza digitale che consenta di diventare consumatori critici e produttori consapevoli di contenuti, molto utile la consultazione del Sillabo realizzato nell'ambito dell'iniziativa *Generazioni connesse* (*Safer Internet Centre* Italia), coordinata dal Ministero dell'Istruzione con il coinvolgimento di oltre cento organizzazioni tra istituzioni, mondo accademico e società civile. Tra gli obiettivi perseguiti vi è quello di consolidare "la capacità di riflettere autonomamente sul rapporto tra sfera pubblica e sfera privata, sul tema della riservatezza (*privacy*), come protezione della propria e il rispetto dell'altrui, e sul concetto di traccia digitale (*digital foot print*), generata in rete e attraverso diverse tecnologie" – Il Sillabo di Educazione civica digitale, corredato da materiale didattico, è consultabile al link https://www.generazioniconnesse.it/site/it/0000/00/00/sillabo-di-educazione-civica-digitale/. In letteratura E. HEINZE, *Hate speech and democratic citizenship*, Oxford, 2016.

[65] I. GARACI, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, cit., 804.

[66] R. SENIGAGLIA, *Il dovere di educare i figli nell'era digitale*, in *Persona e mercato*, 2021, 3, 517.

sull'educazione alla legalità e al contrasto alle mafie; sulla valorizzazione del patrimonio culturale e dei beni pubblici comuni.

Gli obiettivi, declinati nelle successive Linee Guida ministeriali[67], sono ambiziosi non solo per la complessità dei temi, ma anche la nuova metodologia richiesta, che deve coinvolgere i discenti e gli adulti in un percorso di insegnamento-apprendimento che valorizzi il sapere reciproco, la *differenza* di cui ciascuno è portatore per una cooperazione costruttiva. Perché l'educazione è, innanzi tutto, reciprocità, esige quindi una comunità. Nessuno può farcela da solo.

6. Nuovi orizzonti per la costruzione di uno *European Health Data Space*: cenni conclusivi

Sarebbe ingenuo, e poco credibile, ritenere che la promozione di strumenti di protezione possa esaurirsi in un'opera di alfabetizzazione mediale nell'ambito dell'istruzione scolastica, rivolta non solo ai minori, ma anche ai genitori e agli insegnanti, la cui formazione continua è divenuta sempre più preziosa.

Primi fra tutti sono i soggetti privati che presidiano le piattaforme ad avere «la responsabilità di conformare la tecnica che si sostituisce all'uomo in modo da renderla rispettosa delle specifiche fragilità della persona», al fine di rendere l'ecosistema digitale «un luogo eticamente e giuridicamente sostenibile, in cui il bilanciamento tra vantaggi e rischi si giustifichi all'insegna di una cifra assiologica discendente dallo statuto giuridico del minore di età»[68].

Le ben note fragilità di una protezione dei dati personali basata sul consenso[69], come espressione dell'autodeterminazione informativa della persona[70], sono ancora più evidenti quando si tratta di minori[71], di fatto poco consapevoli dei rischi connessi alla cessione di informazioni che riguardano anche la loro sfera più intima[72]. Con specifico riferimento alle *app* per il benessere e la salute, la semplicità e rapidità di fruizione, spesso attraverso l'uso di *smartphone*, rendono di fatto irrealistico l'adempimento dell'onere informativo[73].

In linea con la speciale attenzione che il GDPR riserva ai minori, meritevoli di una specifica protezione in ragione del fatto che possono essere «meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate, nonché dei loro diritti in relazione al trattamento dei dati personali»,

[67] Consultabili al link https://www.istruzione.it/educazione_civica/.

[68] R. SENIGAGLIA, *Il dovere di educare i figli nell'era digitale*, cit., 1518. Insiste sulla necessità di ripensare in senso etico i modelli di *business* anche I. GARACI, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, cit., 817.

[69] Per tutti rinvio alle riflessioni di A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 148 ss.

[70] V. NASH, *The Politics of Children's Internet Use*, in M. GRAHAM, E. H DUTTON (edited by), *Society and the Internet*, Oxford, 2014, 67 ss.

[71] P. VIRGADAMO, Minori e nuovi media, cit., 367; E. BATTELLI, Privacy *e minori: l'inadeguatezza del c.d. consenso digitale*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, cit., 554 s.; L. BOZZI, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, cit., 267.

[72] Evidenzia come la protezione del minore *on line* non si esaurisca con la regolazione del consenso al trattamento dei dati B. AGOSTINELLI, *Informazione e minori: una lettura integrata per una tutela uniforme*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, cit., 578-579.

[73] Come mette in luce in modo appropriato I. RAPISARDA, *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app *mediche*, cit., 205.

ISSN 2284-4503

specialmente con riguardo alla profilazione per attività di *marketing* (considerando 38)[74] e alle decisioni automatizzate (considerando 71), la direzione deve essere quella di definire, con un approccio olistico e proattivo[75], *by design* (ex art. 25 GDPR)[76] un più efficace sistema di tutela dei diritti fondamentali dei bambini e degli adolescenti[77]. Le imprese, soprattutto quelle che operano nel settore dei servizi della società dell'informazione, sono tenute a porre in essere strategie di sviluppo sostenibile, finalizzate a tenere sempre in considerazione il benessere (psichico e fisico dei minori di età)[78].

Non può lasciare certo indifferenti il fatto che non si sia ancora risolto il problema dell'effettivo accertamento dell'età anagrafica delle utilizzatrici[79], posto che non viene di fatto svolta nessuna attività di accertamento[80].

[74] B. CORTESE, Marketing *e minori in ambiente digitale. Alla scoperta di un* black hole *normativo nel Regolamento generale sulla protezione dei dati nell'Unione europea*, in E. DE BELVIS (a cura di), *Diritto di Famiglia e nuove tecnologie*, 2022, 255 ss.

[75] Fin dai primi commenti la dottrina ha insistito sulla necessità di effettivo adempimento da parte delle imprese dei principi dell'*accountability*, di *privacy by design* e di *privacy by default*: G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, 1 ss. V., anche E. TOSI, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno morale soggettivo*, in *Contr. e impr*., 2020, 1128, secondo cui "l'introduzione del principio di *accountability* determina l'onere di adottare un nuovo approccio *preventivo e responsabile* nella gestione della protezione dei dati da parte delle singole organizzazioni aziendali».

[76] *By design* significa che le tecnologie devono già incorporare misure di protezione dei diritti perché nello spazio digitale la tutela va necessariamente pensata in un'ottica preventiva. *Amplius* E. MAESTRI, *L'identità perduta*. Internet of things, smart devices e *privacy dei minori sul* web, in A. ANNONI, A. THIENE (a cura di), *Minori e* privacy*. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, cit., 24, secondo cui «il confine tra *off line* e *on line* potrà risultare netto solo agendo sulle scelte di *design* degli spazi virtuali su internet».

[77] Ci si riferisce all'integrazione, nella stessa tecnologia, di misure che garantiscano la protezione dei dati personali e il rispetto delle libertà e dei diritti della persona minore d'età per progettazione e per impostazione. E ciò nella complessità che è propria della condizione della persona e della situazione di vita concreta in cui versa, tenendo conto delle sue specifiche esigenze e dell'apporto che possono fornire le diverse discipline. Si pensi, ad esempio, al ruolo fondamentale che svolgono, per il diritto dei minori, le scienze umane. Sia concesso al riguardo il rinvio ad A. THIENE, *Gli affidamenti*, in R. SENIGAGLIA e A. CORDIANO (a cura di), *Diritto civile minorile*, Napoli, 2022, 299 ss.; EAD., *Giudici e servizi sociali al crocevia: il legislatore riscrive l'art. 403 c.c.*, in *Nuove leggi civ. comm*., 2022, 309 ss.

[78] Questo obiettivo di sostenibilità sociale è cruciale per I. GARACI, *Autodeterminazione e tutela del minore di età nel contesto digitale*, in A. CATRICALÀ e M.P. PIGNALOSA (a cura di), *Saggi di diritto dei consumi*, Torino, 2020, 135. Cfr. EAD., *La valutazione d'impatto sui diritti fondamentali dei minori di età nell'ambiente digitale. Riflessioni a margine della proposta di direttiva relativa alla* due diligence *delle imprese ai fini della sostenibilità e del* Digital Services Act, in I. GARACI e R. MONTINARO (a cura di), *La sostenibilità dell'innovazione digitale*, Napoli, 2023, 113 ss.

[79] «L'unica soluzione che permetta di identificare l'età parrebbe essere la modifica del *code* della rete per consentire la trasmissibilità delle informazioni relative all'età dell'*user* e per rendere tracciabile l'anonimato. È pur vero che, allo stato attuale, non c'è un rapporto necessario tra un terminale (avente un dato indirizzo IP) e la persona; i governi, però, potrebbero intervenire per facilitare l'uso di tecnologie di identificazione e di autenticazione degli utenti sul *web*»: E. MAESTRI, *L'identità perduta*. Internet of things, smart devices *e* privacy *dei minori sul* web, cit., 25.

[80] I. GARACI, *Minori e pubblicità mirata*, in *Diritto mercato tecnologia*, 2022, 5.

Consapevolezza delle utilizzatrici e responsabilità proattiva dei titolari di trattamento[81] sono le chiavi per affrontare la nuova strategia europea per i dati sanitari, che punta ad un approccio dinamico del flusso circolatorio dei dati relativi alla salute[82].

Il riferimento va alla proposta di Regolamento europeo sullo spazio europeo dei dati sanitari per la costituzione di uno *European Health Data Space*[83], destinata ad applicarsi anche «ai fabbricanti e ai fornitori di sistemi di cartelle cliniche elettroniche e di applicazioni per il benessere immessi sul mercato e messi in servizio nell'unione e agli utilizzatori di tali prodotti» (art. 1, par. 3, lett. *a*)[84].

Dalla lettura dei considerando 35 e 36 emerge chiaramente l'idea della *interoperabilità* dei dati, perché le *app* per il benessere potrebbero essere collegate e fornire informazioni ai sistemi di cartelle cliniche elettroniche o a soluzioni di sanità elettronica nazionali, nei casi in cui i dati prodotti dalle applicazioni per il benessere siano utili per finalità di assistenza sanitaria[85]. Gli utenti dovrebbero essere informati circa la conformità di tali applicazioni alle prescrizioni di interoperabilità e sicurezza. A tal fine ideale sarebbe la progettazione di un *sistema di etichettatura* volontaria capace di guidare i consumatori nella scelta di applicazioni per il benessere appropriate, dotate di elevati standard di interoperabilità e sicurezza (art. 31, *Etichettatura volontaria delle applicazioni per il benessere)*.

Senza pretesa di addentrarci nella questione, non possiamo non rilevare come la disinvoltura con cui viene prevista la possibilità di un uso secondario dei dati generati dalle applicazioni per il benessere e dalle altre applicazioni digitali sia lontana dalla rigidità che ispira l'art. 9 del GDPR, che continuerà ad essere il punto di riferimento per il trattamento dei dati sensibili. Criticità che sono state tempestivamente espresse in un parere congiunto, adottato il 12 luglio 2022, dal Comitato europeo per la protezione dei dati e dal Garante europeo della protezione dei dati[86].

---

[81] Va detto che purtroppo le indagini empiriche sulle trenta principali *app* per la fertilità rivelano diverse criticità sotto il profilo della protezione dei dati personali ai sensi del GDPR: cfr. M. MEHRNEZHAD, T. ALMEIDA, *Caring for Intimate Data in Fertility Technologies*, in *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8-13, 2021, Yokohama, Japan.*

[82] COM (2022) 196 del 3.5.2022. Sui dati sanitari e la strategia europea per i dati v. S. CORSO, *Una strategia europea per i dati, anche sanitari*, in www.rivistaresponsabilitamedica.it, 7 marzo 2021.

[83] COM (2022) 197 del 3.5.2022. Per ogni riferimento cfr. S. CORSO, *Lo spazio europeo dei dati sanitari: la Commissione europea presenta la proposta di regolamento*, in federalismi.it, 10 agosto 2022.

[84] Le applicazioni per il benessere sono definite all'art. 2, par. 2, lett. *o* come «qualsiasi apparecchio o *software* destinato dal fabbricante a essere utilizzato da una persona fisica per il trattamento dei dati sanitari elettronici per scopi diversi dall'assistenza sanitaria, quali il benessere e il perseguimento di stili di vita sana».

[85] Interoperabilità significa che i sistemi devono poter dialogare tra loro con ovvie conseguenze sul piano dell'accessibilità ai dati stessi. Si pensi, ad esempio, ai vantaggi – e allo stesso tempo ai profili problematici – riscontrabili per un paziente il cui fascicolo sanitario elettronico, consultabile da un professionista sanitario, possa attingere ai dati raccolti attraverso l'uso di *app*, che siano appunto interoperabili con il fascicolo stesso. Cfr. S. CORSO, *Il fascicolo sanitario elettronico fra* e-Health*,* privacy *ed emergenza sanitaria*, in *Resp. med.*, 2020, 393 ss. In termini più ampi, M.A. SANDULLI, *Introduzione*, in A. THIENE e S. CORSO (a cura di), *La protezione dei dati sanitari.* Privacy *e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, 2023, 1 ss.

[86] Il parere è analizzato da S. CORSO, *Il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati in merito alla proposta di regolamento sullo spazio europeo dei dati sanitari*, in www.rivistaresponsabilitamedica.it, 5 settembre 2022.