LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI IMPRESA E MANAGEMENT

TESI DI LAUREA MAGISTRALE

Cattedra di Legal Issues in Marketing

DISCIPLINA DEL CONSENSO E TUTELA DEL MINORE ALLA LUCE DEL REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI PERSONALI N. 2016/679 (GDPR)

RELATORE
Prof. Francesco Di Ciommo

CORRELATORE
Prof. Roberto Pardolesi

CANDIDATA
Mariangela Miranda
Matr. 701741

ANNO ACCADEMICO 2018/2019

INDICE

INTRODUZIONE

La tutela dei dati personali dei minori rappresenta una delle principali innovazioni introdotte dal legislatore comunitario nel Regolamento europeo sulla libera circolazione e protezione dei dati personali.

All'analisi di tale normativa è dedicato il presente lavoro, il quale mira ad offrire, nei primi due capitoli, un quadro generale dell'opera, soffermandosi, in particolare, sul consenso al trattamento dei dati. Nel dettaglio, il primo capitolo si caratterizza per l'analisi della riforma e le ragioni della sua emanazione: le principali novità di cui i principi fondamentali su cui si fonda la normativa, i diritti degli interessati, il principio di *accountability*, la figura del Data Protection Officer e il binomio *privacy-by-design* e privacy-by-default. Il secondo capitolo mira, invece, a svolgere un'analisi dettagliata della disciplina del consenso al trattamento, soffermandosi sull'*informativa* agli interessati. Al riguardo, viene meglio sviluppata la fattispecie della profilazione tipizzata dall'art. 22 GDPR.

Terminata la trattazione teorica della disciplina della circolazione e protezione dei dati personali, la parte finale dell'elaborato, rappresentata dal terzo capitolo, è interamente dedicata alla tutela dei soggetti minori. Si analizzano, in particolare, i casi affrontati nei Tribunali di Roma e di Mantova, i cui Giudici hanno ordinato due genitori alla rimozione delle foto dei figli dal *social network* Facebook e condannati al pagamento di una somma di denaro in loro favore.

Infine, segnalata la recentissima sentenza del Tribunale di Rieti del 6-7 marzo del 2019[1] avente anch'essa ad oggetto la necessaria autorizzazione dei genitori per la pubblicazione online delle foto dei figli minori di quattordici anni.

[1] Per una analisi complessiva della sentenza in esame, www.canestrinilex.com/risorse/vietato-publbicare-foto-di-minorenne-si-social-senza-consenso-di-entrabmi-i-genitori-tr-rieti-2019/.

CAPITOLO 1

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR): I CAMBIAMENTI NEL MONDO DELLA PRIVACY

1.1 PREMESSA

L'impatto dell'evoluzione tecnologica dell'ultimo trentennio ha inciso significativamente sulla vita dell'uomo post-moderno, il quale è sempre più integrato nella rete e nella tecnologia di cui fa un uso quotidiano e continuo[2]. Nella realtà digitale, divenuta un vero e proprio ambiente dove il singolo esplica la propria personalità, "*non si ha più una persona virtuale contrapposta alla persona reale, ma un intreccio che restituisce la persona reale come connotata dal digitale*"[3]. L'avvento di Internet e dei social network ha trasformato profondamente, non soltanto, il tessuto economico e produttivo, ma anche le relazioni umane e sociali che, sempre più spesso, nascono e si sviluppano online, inducendo a cedere, comunicare e trasmettere porzioni più o meno rilevanti di informazioni al fine di usufruire di servizi o acquistare beni, sia da enti pubblici che da privati[4]. La rete e i servizi che essa offre consentono una diffusione potenzialmente *illimitata* nel tempo, nella qualità e nella quantità, dei dati personali relativi ad un determinato soggetto[5] facilitando, non solo, la libera circolazione di quest'ultimi all'interno dell'Unione europea, ma anche il trasferimento degli stessi verso Paesi terzi ed organizzazioni internazionali ad un livello globale prima inimmaginabile[6]. Un simile scenario, se da un lato ha il vanto di abbattere le barriere fisico/geografiche, favorendo un'interconnessione costante tra individui situati in luoghi diversi, nonché semplificando ed agevolando il reperimento di qualsiasi dato, dall'altro è suscettibile di determinare un serio ed elevato pericolo per la libertà e la dignità del singolo, le cui informazioni personali sono sempre più esposte alla m*ercè* di chiunque possegga gli strumenti per connettersi alla rete. Ciò spiega i motivi per cui in un'epoca, come quella moderna, connotata dalla comunicazione digitale globale, il diritto fondamentale alla protezione dei dati personali ha assunto un ruolo determinante per la difesa della libertà dell'individuo,

[2] G. Conti, *La protezione dei dati personali per titolari e responsabili del trattamento*, Santarcangelo della Romagna, Maggioli, 2019, p. 15
[3] S. Rodotà, Il mondo della rete. Quali i diritti, quali i vincoli, Laterza, Roma-Bari, 2014, p. 14
[4] F. Modafferi, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, United Kingdom, 2015, p. 28
[5] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Giappichelli, Torino, 2016, p. 8
[6] G. Conti, *op. cit.,* p. 15

richiedendo sistemi giuridici di tutela sempre più affinati. L'esigenza di tutela nei riguardi dei propri dati personali, nata come risposta alla tecnologia legata al trattamento automatizzato dei dati, è oggi diventata la più importante barriera allo straripare della società digitale[7]. La rapidità dell'evoluzione tecnologica e della globalizzazione, infatti, sollevano nuove e importanti sfide per la protezione delle informazioni a carattere personale, sfide che richiedono di essere autonomamente gestite ed affrontate a livello, non solo, nazionale ed europeo ma, addirittura, globale[8].

1.2 DALLA TUTELA DELLA RISERVATEZZA ALLA PROTEZIONE DEI DATI PERSONALI

L'evoluzione tecnologica delle comunicazioni elettroniche, che contraddistingue la società digitale, facilitando la globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali, ha contribuito a connotare di contenuti inediti il più tradizionale diritto alla riservatezza, ampliandolo fino a farvi ricomprendere anche il diritto alla protezione dei dati personali, elevato a diritto fondamentale ed elemento essenziale del rispetto della persona e della sua vita familiare[9].

Avvertite – o forse semplicemente riscoperte – queste nuove esigenze di protezione dell'individuo, il Legislatore europeo è intervenuto con un'opera organica, il "*General Data Protection Regulation"* (da qui in poi semplicemente "GDPR")[10], al fine di garantire che tutti gli Stati membri dell'Unione detenessero un uniforme, ed elevato, livello di protezione delle persone fisiche, i cui dati personali, ora come non mai, vengono commercializzati e scambiati nell'ambito di sistemi di economia digitale, all'interno dei quali sempre più transazioni si fondano sul paradigma offerta di servizio contro dato personale[11]. È bene però, sin da subito, evidenziare come il GDPR non tuteli il diritto alla *privacy* in senso stretto, talché appare già in questa sede opportuno delineare il confine tra il diritto alla protezione dei dati personali e il diritto alla privacy intesa, in senso stretto,

[7] F. Pizzetti, *op. cit.,* p. 8
[8] G. Conti, *op. cit.,* p. 16
[9] F. Pizzetti, *op. cit.,* p. 7
[10] Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, il Reg. (UE) n. 2016/679 è entrato in vigore il 24 maggio 2016 ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018. Trattandosi di un Regolamento, non necessita di recepimento da parte degli Stati dell'Unione ed è stato attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.
[11] G. Conti, *op. cit.,* p. 16

come *riservatezza*. I due concetti, lungi dall'essere perfettamente coincidenti, al contrario hanno contenuti non eguagliabili, in quanto posti a presidio di beni giuridici differenti, seppur di uguale rilevanza[12]. Il diritto alla riservatezza, riconosciuto dall'ordinamento italiano, tanto nelle disposizioni costituzionali quanto in quelle ordinarie[13], nonché nelle leggi speciali, consiste, infatti, nella tutela di quelle situazioni e vicende strettamente personali e familiari che non devono essere oggetto di interesse socialmente apprezzabile da parte di terzi[14]. Per *diritto alla privacy*, dunque, è da intendersi, generalmente, il diritto alla riservatezza della sfera personale, privata, dell'individuo o della famiglia.

Rinvenendo la propria genesi in tempi assai risalenti - secondo la maggior parte degli studiosi e storici il periodo è riconducibile ai secoli XVIII e XIX - rispetto al più recente diritto alla protezione dei dati personali[15], la nozione di *privacy* sembrerebbe scaturire da uno specifico evento: la pubblicazione, nel 1890, di un articolo intitolato *The Right to Privacy*[16] scritto ad opera di due giovani avvocati bostoniani in opposizione agli sconfinamenti della stampa giornalistica la quale, ai tempi in cui i due scrissero, poneva quotidianamente alla *mercè d*ell'intera comunità le vicende private relative alla vita familiare dell'é*lite bo*stoniana.

È pur vero, tuttavia, che, per quanto abbia radici profonde nel tempo, il "*diritto ad essere lasciati soli*" è il frutto dei nostri tempi[17]. La genesi e il successivo sviluppo e/o trasformazione di un determinato diritto, infatti, è profondamento correlato al contesto in cui opera, ed in qualche misura influenzato dalle tecnologie, dal sistema sociale e dall'epoca storica in cui prende forma e nella quale - vuoi per effetto della consuetudine, vuoi per effetto della legge, vuoi per effetto della giurisprudenza - comincia a produrre effetti giuridici[18]. Tuttavia, pochi sono quei diritti plasmati in modo così evidente a seguito di un'innovazione tecnologica così chiaramente individuata, come è avvenuto per il *Right to privacy*[19]. È in questo quadro di profondo mutamento sociale, infatti, che la tradizionale nozione di *privacy*, definita come il "*diritto ad essere lasciati indisturbati*" e

[12] G. Conti, *op. cit.,* p. 24
[13] Il diritto alla riservatezza trova espressa tutela nell'art. 15 della Costituzione italiana che stabilisce che la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
[14] A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, Torino, 2018, p. XIII
[15] Pietra miliare della materia è rappresentato da: The Right to Privacy di Samuel D. Warren e Louis D. Brandeis in "Harvard Law Review", Vol. 4, No. 5. (Dec. 15, 1890)
[16] L. Brandeis, S. Warren, *op. cit*.
[17] R. Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2019, p. 6
[18] F. Pizzetti, *op. cit.,* p. 47
[19] F. Pizzetti, *op. cit.,* p. 48

fondata sul criterio dell'esclusione degli altri dalla propria sfera privata, si è evoluta nel diritto di ciascuno a controllare come gli altri trattino i suoi dati personali[20].

Diritto alla riservatezza e protezione dei dati personali si sono così intrecciati nell'arco del tempo[21]. Come sapientemente evidenziato da Stefano Rodotà, dalla tutela statica e negativa della riservatezza, che, costruita sul modello della proprietà privata, si esauriva nell'*esclusione* delle interferenze altrui – in un *"right to be let alone"* – si è giunti alla protezione dei dati personali, provvista altresì di una tutela dinamica, composta di regole rigorose che delineano le modalità del trattamento e conferiscono poteri di controllo e di intervento alla persona interessata[22].

Le due dimensioni diventano così interconnesse: la tutela della privacy protegge un interesse individuale, il controllo dei dati garantisce un interesse anche collettivo[23]. Nel corso del tempo, l'esigenza di protezione della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, in questo modo riflettendo l'attuale contesto storico, nell'ambito del quale il singolo cede continuamente, e nelle forme più diverse, le informazioni personali che lo riguardano[24]. Complice il progresso tecnologico, che consente di vivere ogni momento della propria vita online, perennemente connessi alla rete[25].

Invero, sebbene il diritto alla protezione dei dati personali non trovi riconoscimento formale all'interno della Carta costituzionale italiana, essendo di più recente elaborazione rispetto a quello della riservatezza, ciò non esclude la sua configurazione come diritto fondamentale dell'individuo.

Un referente normativo in tal senso si rinviene nella "Carta dei diritti fondamenti dell'Unione europea" - anche nota come "Carta di Nizza"[26] - la quale solennemente accorda ad ogni persona fisica il diritto che i propri dati personali siano trattati nel rispetto della legge e delle regole generali che disciplinano le attività di trattamento[27] [28]. Quelli

---

[20] M. Soffientini (a cura di), *Privacy*, IPSOA, Milano, 2018, p. 4
[21] R. Panetta, *op. cit.,* p. XXXIX
[22] S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2013, p. 397
[23] R. Panetta, *op. cit.,* p. XIII
[24] S. Rodotà, *op. cit.*
[25] M. Soffientini, *op. cit.,* p. 4
[26] Proclamata una prima volta il 7 dicembre 2000 a Nizza e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo, da Parlamento, Consiglio e Commissione, con l'entrata in vigore del "Trattato di Lisbona", la Carta di Nizza ha assunto il medesimo valore giuridico dei Trattati. Essa risponde alla necessità di definire un gruppo di diritti e di libertà di eccezionale rilevanza che fossero garantiti a tutti i cittadini dell'Unione europea.
[27] G. Conti, *op. cit.,* p. 25
[28] L'art. 8 della Carta di Nizza, rubricato "Protezione dei dati di carattere personale", stabilisce che: "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati*

stabiliti dalla Carta di Nizza rappresentato principi fondamentali a presidio di valori giuridici universali, i quali assumono ancor più rilevanza se solo si pensa che in una società iperconnessa, profondamente assoggettata a beni e servizi che proiettano l'individuo e i propri dati personali in una dimensione vasta e dinamica, la presenza di regole si rende indiscutibilmente vitale[29]. Senza le regole e senza il diritto saremmo destinati ad implodere; allo stesso tempo, nella veste di interessati saremmo destinati a diventare schiavi dei nostri dati personali e dei diversi titolari del trattamento, in un'economia che vede il nuovo "oro" nelle informazioni riferibili a ciascun individuo[30]. In quest'ottica, si inserisce il GDPR, frutto anche della citata evoluzione dal diritto alla *privacy* al diritto di disporre dei propri dati personali, composito mosaico di disposizioni giuridiche mediante le quali il Legislatore europeo ha attualizzato il panorama legislativo in materia, aggiornandolo alla realtà dei social network e dei motori di ricerca, e qualificandolo come uno dei più sofisticati sistemi di protezione nel mondo[31].

1.3 DALLA DIRETTIVA "MADRE" AL GDPR: LE RAGIONI DELLA RIFORMA

Abrogando e sostituendo la Direttiva 95/46/CE, la quale per anni ha rappresentato la pietra angolare della legislazione europea in materia di dati personali[32], il GDPR ha introdotto un quadro normativo sostanzialmente identico in tutto il territorio dell'UE, ponendo in questo modo fine alle asimmetrie giuridiche fino a quel momento prodotte dalle singole legislazioni nazionali frutto del recepimento della "Direttiva Madre" e delle azioni diversificate messe in campo dalle diverse Autorità di controllo[33].
L'avvento del nuovo Regolamento ha definito un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri, con l'obiettivo di uniformare ed armonizzare tale disciplina entro - e non solo - i confini comunitari, eliminando così "barriere" che si erano create nel corso del tempo con normative nazionali frammentarie e diverse tra loro, le

devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."
[29] R. Panetta, *op. cit.,* p. 6
[30] R. Panetta, *op. cit.,* p. 7
[31] A. Pisapia, *op. cit.,* p. XIV
[32] E. Tosi (a cura di), *Privacy Digitale*, Giuffrè, Milano, 2019, p. 59
[33] R. Panetta, *op. cit.,* p. 7

quali, non solo, ostacolavano la libera circolazione dei dati tra una Nazione e l'altra ma, inoltre, penalizzavano lo sviluppo di un mercato unico digitale[34].

L'intervento del legislatore comunitario, attuatosi con l'adozione del GDPR, si è reso necessario in ragione della difformità venutasi a creare tra i diversi Stati membri, oltre che allo scopo di fornire una risposta normativa rispetto alla continua, ed incessante, evoluzione dei concetti di privacy e data protection.

Invero, diverse sono state le ragioni che hanno indotto il Legislatore europeo a prediligere lo strumento normativo rappresentato dal regolamento[35] in luogo di una mera direttiva: *in primis* l'esigenza di garantire un livello di protezione dei dati personali coerente tra tutti gli Stati membri. Ciò al fine di evitare divergenze tra le singole legislazioni nazionali e facilitare la libera circolazione dei dati nel mercato interno[36].

Come efficacemente evidenziato da studiosi del settore, infatti, il processo di parificazione degli standard di protezione dei dati è efficace solo se questo corre attraverso un tracciato comune per tutti gli Stati membri e i cittadini comunitari[37].

Per tale motivo l'adozione del Regolamento è apparso lo strumento efficace per garantire alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti, giuridicamente vincolanti per i soggetti interessati, nonché gli stessi obblighi, responsabilità e sanzioni equivalenti per coloro che processassero tali dati[38].

Com'è noto, infatti, tale strumento normativo, limitando i poteri statali nella fase di recepimento, garantisce l'equiparazione dei sistemi nazionali e l'uniformità legislativa nel mercato interno[39]. Quella assunta dalle istituzioni europee che, in tal modo hanno inteso dare un segnale forte ai Paesi dell'Unione e agli operatori stranieri con interessi economici in Europa, si è rivelata una scelta coraggiosa e vincente rappresentando, al tempo stesso, l'unica risposta possibile alle esigenze del mercato europeo, sempre più caratterizzato dalla necessità di accedere ad un mercato unico digitale (c.d. *Digital Single Market*), e sempre più condizionato dalle ridotte *chances* di competere con mercati più

[34] A. Ciccia Messina, N. Bernardi, *Privacy e regolamento europeo*, IPSOA, Milano, 2018

[35] Nell'ambito degli atti aventi effetti giuridici, caratterizzanti il panorama normativo a carattere europeo, il regolamento si connota per aver portata generale e astratta in quanto rivolto a destinatari non determinati; per essere obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri senza bisogno di alcun intervento normativo statale.

[36] A. Pisapia, *op. cit.,* p. XIV

[37] R. Panetta, *op. cit.,* p. 7

[38] A. Pisapia, *op. cit.,* p. XV

[39] A. Pisapia, *op. cit.,* p. 21

grandi, come quello statunitense o cinese/asiatico, ma meno frammentati dal punto di vista giuridico/regolamentare[40].

1.4 L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE AL GDPR

Se è fuor di dubbio che lo strumento del Regolamento sia funzionale a conseguire un elevato livello di unificazione in materia di protezione dei dati personali, d'altra parte è pur vero che è la stessa disciplina comunitaria in oggetto a prevedere, seppur in taluni casi, e nei limiti stessi posti dallo stesso Regolamento[41], che gli Stati membri dispongano di un certo margine di manovra, consentendo loro di intervenire, non attraverso il recepimento, bensì mediante l'armonizzazione con altre leggi insistenti sulla medesima[42]. Muovendosi entro tali confini, il Parlamento italiano, nel mese del novembre 2017, ha delegato il Governo all'adozione di un decreto di armonizzazione dell'ordinamento nazionale al GDPR al fine di consentire un miglior adattamento della normativa comunitaria alle specifiche peculiarità del sistema giuridico italiano, nonché allo scopo di rispondere all'esigenza di salvaguardare i meccanismi di tutela, predisposti dall'Autorità Garante per la protezione dei dati personali, fino a quel momento vigenti.
Dal lavoro di un'apposita Commissione ministeriale, scandito da diverse bozze, è derivata una legge delega, la quale ha consentito al Governo di approvare in via definitiva il d.lgs. 10 agosto 2018, n. 101. Tale insieme normativo, pur presentando rispetto al previgente Decreto legislativo n.196/2003 (c.d. «Codice della Privacy») aspetti di continuità, non apporta modifiche al Regolamento, tuttavia, interviene in diverse e cruciali aree: dal trattamento dei dati particolari ai diritti dei minori e dei defunti, fino alla ridefinizione delle norme penali a supporto del corretto adempimento degli obblighi derivanti dalla materia[43]. Ciò detto, nel prosieguo della trattazione verranno analizzati gli aspetti peculiari del GDPR, seppur con un inevitabile processo semplificativo e di sintesi.

---

[40] R. Panetta, *op. cit.,* p. 12
[41] Sul punto, il Considerando n.10 del GDPR stabilisce che gli Stati membri *"dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento"* né si esclude che *"il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisazione le condizioni alle quali il trattamento dei dati personali è lecito."*
[42] R. Panetta, *op. cit*., p. 12
[43] *Ibidem.*

1.5 IL GDPR: INQUADRAMENTO GENERALE

L'insieme normativo, in cui il nuovo Regolamento europeo si articola, si compone di ben 99 articoli, preceduti da 173 "Considerando", i quali chiariscono il contesto e le ragioni della nuova disciplina in materia di protezione dei dati personali[44]. Etichettate come disposizioni generali, le norme di apertura al Regolamento - articoli da 1 a 4 - sono volte ad individuare, e delimitare, l'oggetto, le finalità e l'ambito di applicazione del medesimo.

Per quanto concerne l'*oggetto*, quest'ultimo viene chiaramente ricondotto dall'art. 1 ad una duplice tematica: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei medesimi dati[45]. I due ambiti, dunque, appaiono ordinati secondo un pari grado di importanza, senza che l'uno possa prevalere sull'altro. Esplicativo in tal senso risulta il Considerando 5, il quale evidenzia che l'integrazione economica e sociale, conseguente al funzionamento del mercato interno, ha condotto a un considerevole aumento dei flussi trasfrontalieri di dati personali e, per l'effetto, anche di dati scambiati in tutta l'Unione tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese, con la conseguenza che la portata della condivisione e della raccolta di dati è aumentata in modo significativo[46].

Con riferimento alle *finalità* del Regolamento, anche quest'ultime possono essere distinte secondo un duplice ordine di idee: 1) elevare la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale a un diritto fondamentale[47]; 2) contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica che consenta il progresso economico e sociale, il rafforzamento e la convergenza delle economie nel mercato interno nonché il benessere delle persone fisiche[48].

---

[44] E. Tosi, *op. cit.,* p. 59

[45] E. Belisario, G. M. Riccio, G. Scorza (a cura di), *GDPR e normativa privacy commentario*, IPSOA, 2018, p. 4

[46] Evidenzia il Considerando 6 come «La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali (…)».

[47] Lo enuncia espressamente il Considerando 1, ai sensi del quale «La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale.».

[48] Come chiarisce il Considerando 2, il GDPR è «inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al

Invero, sebbene raffrontando l'art. 1 del Regolamento[49] con l'art. 1 della previgente Dir. 95/46/CE[50] possa sembrare che sussista una sostanziale sovrapponibilità tra l'oggetto e le finalità dei due testi, da un'analisi critica emergerà la *natura bivalente* della nuova disciplina: l'esigenza di tutela dei dati personali abbraccia quella di favorire la libera circolazione di quest'ultimi. Non da meno, l'espressione *"protezione della vita privata"*, frequentemente utilizzata nel contesto della Direttiva viene sostituita all'interno del Regolamento dall'espressione *"protezione dei dati personali"*, dicitura dalla peculiare rilevanza la quale estende l'ambito di tutela oltre la nozione di privacy intesa, tradizionalmente, soltanto come riservatezza, allargando il proprio raggio d'azione alla componente della privacy che riguarda l'identità personale, dunque la protezione dei dati personali. Del resto, anche il raffronto tra le disposizioni di cui all'art. 1 del Regolamento e il corrispondente punto dedicato alle finalità della disciplina nel Codice Privacy (art. 2)[51] rivela l'assenza, nella previgente disciplina italiana, di qualsivoglia riferimento alla libera circolazione dei dati a fronte di una concentrazione sulla tutela della riservatezza, dell'identità personale e della protezione dei dati personali[52].

Venendo all'ambito di applicazione, giova evidenziare che il Regolamento europeo si applica esclusivamente alle persone fisiche, così come chiaramente si legge nell'articolo iniziale dell'impianto normativo in oggetto. Dall'espressione utilizzata nell'art. 1, infatti, "*protezione dei diritti e delle libertà fondamentali delle persone fisiche",* si deduce che il GDPR non disciplina il trattamento dei dati personali relativi a persone giuridiche. In particolare, come dichiarato nel Considerando 14[53] ne sono esenti le

---

rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.».

[49] L'art. 1 GDPR sancisce quanto segue: «1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.»

[50] L'art. 1 Dir. 95/46/CE stabilisce che: «1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
2. Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1.»

[51] Ai sensi dell'art. 2, *Codice Privacy*: «Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.»

[52] E. Belisario, G. M. Riccio, G. Scorza, *op. cit.,* p. 9

[53] Considerando 14 del GDPR: «È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al

imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto. Tuttavia, è il comma 2, lett. c) a precisare che il Regolamento non si applica ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Il Considerando 18[54] specifica che tali attività potrebbero, ad esempio, comprendere l'uso dei social network, senza quindi una connessione con attività commerciali o professionali. Riguardo l'ambito di *applicazione materiale*, invece, l'art. 2, comma 1 lo identifica in *"tutti i trattamenti di dati personali che siano interamente o parzialmente automatizzati o, anche, non automatizzati purché siano contenuti in un archivio o destinati a figurarsi."* Sotto quest'aspetto, il Considerando 15[55] chiarisce che la protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se questi sono contenuti o destinati a essere contenuti in un archivio[56], al fine di evitare l'insorgere di gravi rischi di elusione.

Tale concetto di *neutralità tecnologica* costituisce una misura da inquadrarsi nel meritorio e condivisibile obiettivo del Legislatore europeo di scongiurare il rischio, quanto mai elevato, di elusione della disciplina comunitaria, attraverso il ricorso a soluzioni tecnologiche - o anche niente affatto tecnologiche - eventualmente qualificabili come estranee all'ambito di applicazione del Regolamento[57]. Infine, la normativa europea apporta diverse novità riguardo *l'ambito territoriale* di applicazione del Regolamento. Ciò allo scopo di estendere il più possibile la tutela accordata, prevedendo la sua applicabilità ogniqualvolta sia rintracciabile un collegamento, sia pure indiretto, con l'ordinamento dell'Unione Europea e dei suoi Stati membri[58]. Più nel dettaglio, secondo

---

trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.»

[54] Considerando 18 del GDPR: «Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.»

[55] Considerando 15 del GDPR: «Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.»

[56] *Ibidem.*

[57] E. Belisario, G. M. Riccio, G. Scorza, *op. cit.,* p. 11

[58] E. Belisario, G. M. Riccio, G. Scorza, *op. cit.,* p. 19

la disciplina dettata dall'art. 3, la normativa in esame si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nel territorio dell'Unione, indipendentemente dal fatto che il trattamento sia effettuato all'interno dell'Unione.[59] È, quindi, sufficiente che *lo stabilimento* del Titolare o del Responsabile del trattamento *si trovi nel territorio UE*, per applicare il GDPR.

Il secondo comma dell'art. 2 introduce una seconda novità, in base alla quale il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dal fatto che vi sia un pagamento correlato, oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione[60]. Non da ultimo, ai sensi del terzo comma del medesimo articolo, il GDPR trova applicazione rispetto al trattamento dei dati personali effettuato da un titolare del trattamento che è stabilito nell'Unione europea, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro[61]. Ne consegue che, per determinare l'applicabilità della nuova disciplina comunitaria a un determinato trattamento, l'interprete dovrà innanzitutto indagare se il titolare o il responsabile hanno uno stabilimento nell'UE e se il trattamento è svolto nel contesto dell'attività di quello stabilimento o in un luogo posto al di fuori dell'UE ma soggetto al diritto di uno stato membro in virtù del diritto internazionale pubblico[62]. Solo se ricorrono tali condizioni, potrà ritenersi che il GDPR trovi applicazione, a prescindere dal fatto che il trattamento abbia ad oggetto i dati personali di persone fisiche presenti nel tracciato europeo o in Paesi terzi (es. India).

Al contrario, laddove tali condizioni non ricorrano, l'interprete dovrà concentrare la sua attenzione, non sul titolare (o responsabile), ma sull'interessato per verificare che esso si trovi all'interno dell'UE e, in caso positivo, se il trattamento avvenga nell'ambito di

[59] M. Soffientini, *op. cit.,* p.15
[60] *Ibidem.*
[61] Considerando 25 del GDPR: «Laddove vige il diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento dovrebbe applicarsi anche a un titolare del trattamento non stabilito nell'Unione.»
[62] E. Belisario, G. M. Riccio, G. Scorza, *op. cit.*, p. 20

un'offerta di beni e servizi verso un Paese membro o di un'attività di monitoraggio di detti interessati.

1.6 LE PRINCIPALI NOVITÀ INTRODOTTE DAL GDPR

1.6.1 I PRINCIPI

I principi fondamentali su cui si fonda la nuova normativa sono enunciati nel capo II (artt. 5-11). Nel dettaglio, la disciplina si sviluppa su due piani differenti: disposizioni generale sui principi (art. 5) e disposizioni specifiche sui principi (artt. 6-11).
L'art. 5[63], rubricato *"Principi applicabili al trattamento dei dati personali",* esplica una serie di principi la cui valenza si estende ad ogni tipo di trattamento - e ad ogni sua fase- avente ad oggetto i dati personali. I principi su cui si incardina tale disposizione sono rappresentati da: a) liceità, corretta e trasparenza; b) minimizzazione dei dati; c) esattezza; d) limitazione della conservazione; e) integrità e riservatezza; f) responsabilizzazione[64].

[63] L'art. 5 GDPR rubricato "Principi applicabili al trattamento di dati personali" prevede che:
«1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)»

[64] È interessante notare come questo aspetto sia sostanzialmente allineato a quanto già previsto dall'art. 11 del Codice Privacy, il quale prevedeva che:
«1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Ciò posto, per quanto concerne, in primo luogo, quello di *liceità*, di cui all'art. 6, trattasi di un principio il quale posta che, per giuridicamente connotarsi come lecito, il trattamento dei dati personali deve fondarsi sul *consenso* dell'interessato o su altra base giuridica prevista come obbligatoria dal Regolamento o dalla normativa europea o da quella statale[65]. Ne consegue che la base giuridica del trattamento potrebbe essere anche estranea ad una disposizione regolamentare, come ad esempio la necessità per il titolare di adempiere all'obbligo legale al quale è soggetto (si pensi ad un notaio nel trattamento dei dati dei suoi clienti) o la necessità di esecuzione di un contratto di cui l'interessato è parte[66].

Con particolare riferimento a quello di *correttezza*, invece, giova evidenziare come tale principio venga già riconosciuto nel contesto ordinamentale italiano. Esemplificative in tal senso risultano le due disposizioni codi cistiche: "Il debitore e il creditore deve comportarsi secondo le regole della correttezza" (art. 1175 c.c.); "Il contratto deve essere eseguito secondo buona fede" (art. 1375 c.c.).

Nell'ottica del GDPR il principio in parola richiede che il trattamento dei dati si svolga in maniera leale e onesta. Si tratta, in buona sostanza, di una forma di lealtà e buona fede da osservarsi in tutte le fasi relative al trattamento di dati personali: in tali fasi vanno certamente ricomprese anche quelle decisorie e preparatorie, e non soltanto, quindi, le operazioni di trattamento strettamente intese[67].

Al fine di essere trasparente - principio di *trasparenza* - il trattamento deve avvenire con modalità predefinite e rese note all'interessato che sarà quindi pienamente consapevole, non solo, della tipologia di dati raccolti, ma anche delle modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i suoi dati personali[68]. Inoltre, tale principio, alla

---

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.».

[65] Considerando 40 del GDPR: «Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.»

[66] Considerando 44 del GDPR: «Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.»

[67] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 94-95

[68] Come evidenzia il Considerando 39: «Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.».

base degli artt. 12 e ss., impone che le informazioni e le comunicazioni relative al trattamento dei dati siano facilmente accessibili e comprensibili. In particolare, nell'*informativa* resa agli interessati andrà chiaramente comunicato il dato relativo all'identità del titolare e le finalità del trattamento, nonché le ulteriori informazioni relative al diritto degli interessati di ottenere conferma e comunicazione del trattamento di dati personali che li riguardano[69]. La *trasparenza*, dunque, non attiene solamente al contenuto dell'informazione relativa al trattamento, ma anche alle modalità con cui esso è formulato e veicolato[70].

1.6.2 I DIRITTI DEGLI INTERESSATI

Il Capo III del Regolamento UE n. 2016/679 si occupa dei "diritti dell'interessato", che vengono modificati sia nella struttura che nelle modalità di esercizio, specificate nell'art.12 dello stesso[71]. Il Regolamento così consolida il quadro dei diritti, e lo amplia rispetto a quelli già conosciuti nel *Codice Privacy*, con l'introduzione di nuovi, tra i quali: il diritto alla portabilità dei dati e il diritto all'oblio.
Proprio a questi ultimi verrà dedicata una disamina specifica nel corso della successiva trattazione.

a) Il diritto all'oblio
Disciplinato dall'art. 17, il diritto all'oblio conferisce all'interessato il potere di ottenere dal titolare del trattamento la cancellazione dei propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento non sia altrimenti conforme al GDPR[72].
Come meglio sarà chiarito nel prosieguo della trattazione, il Considerando n. 65 evidenzia come il diritto all'oblio assuma particolare rilevanza nell'ipotesi in cui l'interessato, che abbia prestato il proprio consenso, abbia la qualità soggettiva di minore - quindi,

[69] E. Tosi, *op. cit.*, p. 79
[70] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 93
[71] Art. 12 del GDPR specifica: *Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni (...) relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*
[72] G. Conti, *op. cit.*, p. 99.

astrattamente, non nella piena consapevolezza dei rischi derivanti dal trattamento - e voglia successivamente eliminare dalla rete i dati personali che lo riguardano[73].
Tuttavia, seppur affidando all'interprete il compito di effettuare una compensazione tra interessi contrapposti, è il medesimo art. 17, al comma 3, ad individuare - ed elencare - una serie di eccezioni all'operatività dei primi due commi, stabilendo che la disciplina da questi ultimi dettata non troverà applicazione nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento.
Da tale disamina emerge una differenza rilevante tra l'impianto normativo del Regolamento rispetto a quello della previgente Direttiva: mentre in quest'ultima il diritto all'oblio veniva, parzialmente, ricavato soltanto in via interpretativa dal generale diritto alla privacy, nel Regolamento, invece, tale diritto è sancito come diritto autonomo, trovando riconoscimento in una specifica disposizione di legge.

b) Il diritto alla portabilità dei dati

Il diritto alla portabilità dei dati costituisce una delle principali novità in tema dei diritti dell'interessato e, in generale, dell'intero quadro normativo confluito nel Regolamento europeo. I presupposti del diritto sono dettagliati dal paragrafo 1, art. 20 GDPR[74]: il primo presupposto riguarda la condizione di liceità del trattamento, riservando la portabilità ai casi in cui il trattamento si basi sul consenso dell'interessato o su un contratto di cui

[73] A. Pisapia, *op. cit.*, p. 67.
[74] Art. 20 "Diritto alla portabilità dei dati", paragrafo 1:
«L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati».

questo è parte; il secondo presupposto concerne la modalità del trattamento, secondo cui il trattamento deve essere effettuato con mezzi automatizzati.

Trattasi, infatti, di un diritto che permette agli interessati di ricevere i dati personali, forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare. Scopo del Legislatore europeo è, in questo modo, accrescere il controllo degli interessati sui propri dati personali e di consentire la trasmissione diretta da un titolare all'altro o direttamente all'interessato.[75]

A titolo esemplificativo, godono di portabilità, i dati raccolti dalla cronologia della navigazione su un sito web o delle ricerche effettuate.

1.6.3 IL PRINCIPIO DI RESPONSABILIZZAZIONE O ACCOUNTABILITY

La chiave di volta della recente disciplina in materia di protezione dei dati personali è rappresentata, sembra ombra di dubbio, dal principio di *accountability* - anche detto di *responsabilizzazione* - il quale, a ben vedere, riflette la centralità attribuita dal Legislatore europeo, nell'impianto normativo in esame, alla figura del titolare del trattamento ma, soprattutto, alle responsabilità che su quest'ultimo gravano[76].

Più nel dettaglio, conformemente al disposto di cui all'art. 5, comma 2, il titolare è tenuto ad assicurare che il trattamento dei dati personali sia conforme alle disposizioni contenute nel Regolamento, dovendo, inoltre, esserne in grado di provarne il rispetto in qualsiasi momento. Il principio di responsabilizzazione, pertanto, si sostanzia nel rispetto degli altri principi del trattamento di cui all'art. 5, comma 1, e nella capacità del titolare di dimostrare di averli osservati[77].

La vera innovazione compiuta dal GDPR risiede proprio nella modifica di prospettiva: non è cruciale limitarsi ad effettuare un trattamento lecito, che sia quindi fondato su idonea base giuridica, ma è necessario assumersi la responsabilità che quel determinato trattamento integri i profili di tutela dettati dalla disciplina in parola[78].

Dal tenore letterale Considerando 74[79] emerge che l'accountability combina due aspetti: innanzitutto l'adozione da parte del titolare di "*misure adeguate ed efficaci*" che l'art. 24,

[75] G. Conti, *op. cit.*, p. 102.
[76] E. Tosi, *op. cit.*, p. 376.
[77] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 323.
[78] A. Pisapia, *op. cit.*, p. 100.
[79] Considerando 74 del GDPR: «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto

comma 1[80], traduce nell'adozione di *"misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento"*; in secondo luogo, la capacità, da parte dello stesso titolare, di dimostrare la conformità delle attività di trattamento con le disposizioni del GDPR, ponendo così l'accento su un aspetto di non poco conto: la possibilità di verificare concretamente, attraverso l'analisi delle misure – tecniche ed organizzative – adottate, l'approccio assunto da un determinato titolare quanto alla protezione dei dati personali dei soggetti interessati[81]. Il principio qui esposto rinviene un ulteriore referente normativo, accentuando in questo modo la sua portata, nell'art. 24[82], il quale prevede che il titolare del trattamento debba, non solo, mettere in atto, ma anche riesaminare e aggiornare adeguate misure tecniche e organizzative, al fine di garantire - ed essere in grado di dimostrare - che le operazioni del trattamento vengono effettuate in conformità con le disposizioni del GDPR[83].

Tra gli strumenti che garantiscono l'accountability si annoverano, tra gli altri, la nomina di un Data Protection Officer (di seguito anche brevemente "DPO") e il rispetto degli obblighi di *"privacy-by-design"* e *"privacy-by-default"*, di seguito esposti.

1.6.4 IL DATA PROTECTION OFFICER

Quella del "Responsabile della protezione dei dati personali", conosciuto anche come "*Data Protection Officer*" o, semplicemente, "*DPO"*, costituisce, nel panorama giuridico nazionale, un'inedita figura soggettiva in quanto non prevista neppure dal previgente "Codice della privacy".

La quarta sezione del GDPR (artt. 37-39) illustra in modo chiaro e puntuale le qualità, il raggio d'azione e le dinamiche aziendali associate a alla figura in oggetto.

misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche».

[80] Art. 24 "Responsabilità del titolare del trattamento", paragrafo 1: «Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.»

[81] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 324.

[82] Art. 24 del GDPR, *ibidem.*

[83] A. Pisapia, *op. cit.*, p. 100.

In particolare, l'art. 37 individua i tre casi in cui la nomina è obbligatoria, e cioè nelle ipotesi in cui il trattamento venga svolto (1) da un'autorità pubblica o da un organismo pubblico, con riferimento all'attività principale; (2) da un titolare o responsabile che svolge trattamenti tali da richiede un monitoraggio regolare e sistematico di interessati su larga scala; (3) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. Al di fuori delle tassative ipotesi sopra indicate – e salvo ulteriori, specifiche, previsioni provenienti da leggi nazionali o dall'UE – la nomina di un DPO è facoltativa, seppur consigliata.

Riguardo i requisiti soggettivi, appare chiaro dall'art. 37, comma 5, che il DPO debba essere designato *"in funzione delle qualità professionali, in particolare dalla conoscenza specialistica della normativa e della prassi in materia di protezione dei dati"* e con le *capacità di assolvere* i compiti a questo assegnati dallo stesso Regolamento (art. 39 GDPR). Parrebbe evidente, quindi, che il profilo professionale idoneo a tal ruolo si incontri in un punto mediano tra le funzioni Legal, IT e Compliance[84].

Ai sensi dell'art. 38, comma 3, appare di rilevante importanza, inoltre, la garanzia di non poter essere sollevato dall'incarico per cause imputabili allo svolgimento del suo ruolo, riflettendo il carattere autonomo della figura in esame rispetto alle dinamiche aziendali (ad esempio conflitti con l'AD). Il DPO, dunque, gode di una sorta di immunità nell'esercizio delle sue funzioni: a dimostrazione di ciò la sua responsabilità, salvo casi di dolo o colpa, non può eccedere il valore del contratto di nomina[85].

Al fine di evitare ogni eventuale conflitto d'interessi e garantire al DPO l'indipendenza richiesta dalla normativa, è proferibile, quindi, assegnare l'incarico a un professionista esterno alla struttura aziendale[86].

Tra i compiti del DPO, indicati a titolo esemplificativo ma non esaustivo nell'art. 39, rientrano quelli di: a) informare e fornire consulenza al titolare o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservazione del regolamento,

[84] F. Pizzetti, *Modalità e requisiti necessari per la nomina a DPO* in *Intelligenza Artificiale, Protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Torino, 2018, p. 96 ss.
[85] R. Panetta, *op. cit.*, p. 24
[86] A. Pisapia, *op. cit.*, p. 107

di altre disposizioni europee e nazionali applicabili per la protezione dei dati; c) qualora richiesto, fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati (ex art. 35) e sorvegliarne lo svolgimento; d) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per tutte le questioni riguardanti la materia in esame, a partire dalle ipotesi di esercizio dei diritti, fino al caso in cui sia avvenuta una violazione di dati personali (c.d. data breach) a seguito di un incidente di sicurezza fisica e informatica[87].

1.6.5 PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Privacy by design e privacy by default sono generalmente indicate come due pilastri della costruzione del Regolamento europeo[88].

Nel dettaglio, con l'espressione "*data protection by design*", si intende l'obbligo in capo al titolare, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura e delle finalità del trattamento, di mettere in atto misure tecniche e organizzative adeguate, per integrare nel trattamento le necessarie garanzie volte a tutelare i diritti degli interessati[89]. In altri termini, la "privacy-by-design" costituisce una nozione omnicomprensiva del rispetto dei principi di *data protection* attraverso la protezione fin dalla fase di progettazione di un trattamento di dati personali[90]. L'applicazione di tecniche idonee a rispettare i principi della data protection introduce il concetto della "*data protection by default*", che è definito dal paragrafo 2 dell'art. 25[91]. Privacy-by-default significa che la tutela della protezione del dato deve assurgere a impostazione predefinita[92], dovendo il titolare adottare misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

---

[87] R. Panetta, *op. cit*., p. 25
[88] A. Ciccia Messina, N. Bernardi, *op. Cit.*, p. 85
[89] M. Soffientini, *op. cit.*, p.97
[90] A. Ciccia Messina, N. Bernardi, *op. cit.*, p. 41
[91] Art. 25 "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", paragrafo 2: «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.».
[92] A. Ciccia Messina, N. Bernardi, *op. cit.*, p. 86

In particolare, le misure di protezione dei dati by default devono garantire che i dati personali, per impostazione predefinita, non siano resi accessibili ad un numero indefinito di persone fisiche senza l'intervento dell'interessato (ad esempio, rendendo di default pubblico un profilo di un social network con possibilità generalizzata per tutti di accedere a foto, informazioni personali e consentendo l'indicizzazione del profilo nei social network senza il consenso dell'interessato[93]). Dunque, attraverso un'applicazione corretta di suddetti principi si vuol garantire che il dato sia protetto fin dalla sua progettazione, ovvero quando questo viene raccolto dal titolare, e che sia garantita la tutela e il rispetto della vita privata per impostazione predefinita[94].

CAPITOLO 2
L'INFORMATIVA AGLI INTERESSATI E IL CONSENSO AL TRATTAMENTO

2.1 PREMESSA

L'art. 6, par. 1 del GDPR, in maniera del tutto speculare alla precedente Direttiva[95], dispone che il trattamento dei dati personali debba trovare il proprio fondamento in una idonea base giuridica[96]. Secondo quanto prescrive la citata disposizione normativa, il trattamento dei dati è lecito se l'interessato ha espresso il proprio consenso al trattamento (art. 6, par. 1, lett. *a*).

A tale fonte di legittimazione seguono, nell'ordine, una base di tipo contrattuale (lett. *b*), l'adempimento di un obbligo legale (lett. *c*), la salvaguardia di interessi vitali dell'interessato o di altra persona fisica (lett. *d*), il perseguimento da parte del titolare di un interesse pubblico o connesso all'esercizio di pubblici poteri (lett. *e*) e, da ultimo, l'interesse legittimo del titolare o di terzi, sempre che non prevalga l'interesse "fondamentale" dell'interessato (lett. *f*).

[93] G. Conti, *op. cit.*, p. 134
[94] *Ibidem.*
[95] Il riferimento è all'art. 7, par. 1, lett. *a*, della Direttiva 95/46/CE.
[96] Mondini Rusconi Studio Legale, *Big Data: Privacy, gestione, tutele*, Altalex, Milano, 2018, p. 214

Dall'analisi testuale dell'articolo in esame il consenso appare requisito equipollente alle altre, e differenti, basi giuridiche pur previste dalla citata disposizione: la normativa non sembra stabilire una gerarchia nel catalogare le basi di liceità del trattamento[97].

Sul punto giova evidenziare che, mentre nell'ambito del vecchio sistema previsto dal previgente Codice della privacy (D.lgs. 196/2003), il consenso rivestiva un'importanza significativa, nell'impianto generale del GDPR, invece, la sua valenza pare essere stata ridimensionata in quanto il consenso rappresenta solo una fra le altre cause di legittimazione del trattamento[98].

Al contempo, è pur vero che, sebbene il consenso sia parificato alle altre cause di legittimità del trattamento, tale base giuridica, nel contesto regolamentare, si connota di peculiari profili di novità.

Su questi ultimi, ed in particolare, sul binomio "informativa-consenso", che *insieme* costituiscono il fondamento della liceità del trattamento[99], ci si soffermerà nel corso della trattazione oggetto del presente capitolo.

2.2 IL CONSENSO AL TRATTAMENTO

2.2.1 DEFINIZIONE

La definizione del consenso per il trattamento di dati personali è riportata all'art. 4, par. 1, n. 11 del GDPR, il quale reca l'indicazione dei requisiti essenziali di validità: costituisce "*consenso dell'interessato*" qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento[100].

Dunque, affinché possa considerarsi validamente espresso, il consenso dell'interessato deve presentare specifiche caratteristiche che, pertanto, devono ricorrere

[97] R. Panetta, *op. cit.*, p. 107
[98] G. Conti, *op. cit.*, p. 72
[99] R. Panetta, *op. cit.*, p. 108.
[100] Sul tema del consenso al trattamento dei dati si veda il recente contributo di I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 67 ss., nonché l'ampio saggio di S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. Dir. priv.*, 2016, 513 ss. ove si ritrovano ampi riferimenti alla dottrina degli ultimi decenni in questa materia.

cumulativamente e non alternativamente affinché il consenso possa ritenersi validamente espresso[101].

In base a tale disciplina, quindi, il consenso deve essere:

a) *libero*: per libertà si intende *consapevolezza* degli elementi sui quali il consenso si esercita e mancanza di *condizionamenti*. Occorre che l'interessato sia in grado di operare una scelta, senza il rischio di aver subito intimidazioni, raggiri e/o coercizioni[102].

Il consenso, dunque, può definirsi "libero" quando è il risultato di una scelta autonoma dell'interessato; al contrario, secondo il Considerando n. 42, non può definirsi tale quando l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizi.

In quest'ottica, è opportuno che il trattamento, effettuato per ottemperare a un obbligo legale da parte del titolare del trattamento soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri da parte di una pubblica amministrazione, trovi il proprio fondamento nella legge e non si basi sul consenso dell'interessato che, nelle predette ipotesi, difficilmente potrà considerarsi liberamente espresso[103]. Tale affermazione trova conforto anche nella posizione del nazionale Garante per la protezione dei dati personali che osserva "*il consenso può essere ritenuto effettivamente libero solo se si presenta come manifestazione del diritto all'autodeterminazione informativa e, dunque, al riparo da qualsiasi pressione e se non viene condizionato all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto"*[104].

Come pure, secondo l'art. 7.4, non è libero il consenso quando *"l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto."*

Dunque, qualora il consenso non sia necessario all'adempimento di obblighi di legge o per dare esecuzione al contratto, l'interessato deve poter scegliere se prestarlo o meno[105]. Ne consegue che il consenso al trattamento dei propri dati personali è libero solo e, nella misura in cui, non è condizione per ottenere un bene e/o un servizio essenziale[106];

---

[101] G. Conti, *op. cit.*, p. 72.
[102] Gruppo di lavoro art. 29, *Opinion on Consent*, 15/2011, p. 13.
[103] Considerando n. 45 del GDPR
[104] Caso BNL Provvedimento del 28 maggio 1997, cit.
[105] In tal senso P. Manes, Il consenso al trattamento dei dati, CEDAM, Padova, 2001, p. 82
[106] Osservazione riconducibile a S. Patti, *Il consenso dell'interessato al trattamento dei dati personali* in *Riv. dir. civ.*, 1999, p. 461

b) *specifico*: tale requisito richiede che il consenso sia circostanziato, ossia riferibile ad un determinato trattamento o ad operazioni di esso specificatamente individuate[107].

Il consenso deve, pertanto, essere prestato per finalità specifiche al fine di assicurare la trasparenza delle attività di trattamento[108]. Come efficacemente sottolinea il Considerando 32: *"qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste".* Inoltre, qualora il trattamento dei dati preveda più operazioni, esso deve esigere una o più richieste di consenso, a seconda che la finalità delle altre operazioni sia la stessa o siano finalità diverse (*consenso modulare*)[109].

Se, infatti, si vincolano a un solo consenso due (o più) finalità distinte, si priva l'interessato della possibilità di scegliere quale consentire e quale no, gli si impone cioè di accettarle tutte in blocco oppure di rifiutarle, e questa è un'evidente violazione del principio di libertà[110]. Ne deriva che, in caso di integrazioni o modifiche delle operazioni di trattamento, si impone che all'interessato venga richiesto nuovamente di prestare il consenso[111];

c) *informato*: si intende tale il consenso preceduto da valida *informativa*, la cui finalità è di porre l'interessato nelle condizioni di essere pienamente a conoscenza del trattamento dei propri dati personali e dei relativi diritti[112].

L'interessato, quindi, deve essere informato delle modalità di trattamento, delle finalità e dei propri diritti[113], in quanto solo un soggetto informato sui trattamenti che lo riguardano può scegliere liberamente se sottoporsi o meno al trattamento[114]. Tale requisito, oltre ad essere strettamente connesso con gli altri analizzati in precedenza, risulta decisivo per garantire effettivamente la libertà e la specificità nella manifestazione dell'atto[115]. Può considerarsi, dunque, una sorta di pre-condizione alla validità del consenso[116], in quanto solo un consenso preceduto da tale attività informativa diviene giuridicamente

---

[107] A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale* in *Quaderni de "Il Foro napoletano", 33*, Edizioni Scientifiche Italiane, 2019, p. 63
[108] G. Conti, *op. cit.*, p. 74
[109] R. Panetta, *op. cit.,* p. 130
[110] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 215.
[111] A. Vivarelli, *op. cit.*, p. 64.
[112] Mondini Rusconi, *op. cit.*, p. 214.
[113] C. Lo Surdo, *Dati personali e strumenti di tutela del soggetto 'interessato'*, in *Danno e responsabilità*, n. 2, 2003, p. 121 ss.
[114] G. Conti, *op. cit.*, p. 73.
[115] A. Vivarelli, *op. cit.*, p. 72.
[116] P. Manes, *op. cit.*, p. 93.

rilevante[117]. In sostanza, informativa e consenso costituiscono un unico binomio dal momento che il secondo trae le sue radici dal primo[118].

Come meglio sarà chiarito al par. 3 del presente capitolo, l'informativa costituisce uno degli adempimenti generali posti in capo al Titolare del trattamento quale strumento attraverso cui gestire il potere del cittadino di limitare e controllare la circolazione delle informazioni che lo riguardano[119];

d) *inequivocabile*: perché il consenso possa essere ritenuto inequivocabile, deve esserci certezza che l'interessato l'abbia effettivamente prestato[120]. La normativa richiede esplicitamente una dichiarazione o un atto positivo con il quale l'interessato esprime il suo assenso al trattamento dei propri dati[121].

L'espressione inequivoca, quindi, esclude il silenzio, l'inattività e la preselezione dei moduli cartacei e online come atti validi alla prestazione del consenso.

In generale, qualsiasi consenso carpito traendo vantaggio dai comportamenti che l'utente pone in essere automaticamente o per ragioni potenzialmente diverse da quelle per cui il consenso è richiesto si pone ovviamente al di fuori del perimetro dell'inequivocabilità[122]. Deve considerarsi perfettamente valido anche un consenso espresso attraverso un comportamento concludente, purché sia "inequivocabile"[123];

e) *espresso*: per qualificarsi come tale il consenso deve sempre derivare da un atto inequivocabile, anche in forma online o elettronica (ad esempio mediante *flag*), essere acquisito via e-mail o anche con l'upload di un documento scannerizzato recante la sottoscrizione di un documento a firma dell'interessato[124].

Al fine di meglio precisare l'ambito di applicazione dell'espressione *"azione positiva inequivocabile"*, è opportuno chiarire che non si reputano ammissibili né caselle pre-spuntate né quelle c.d. "di rinuncia" e non è tollerata, inoltre, l'inattività: continuare ad usufruire del servizio o della navigazione su un sito web non sono indici sintomatici di una volontà di acconsentire[125];

f) *esplicito*: l'art. 9 del GDPR stabilisce che *"è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o*

[117] A. Vivarelli, *op. cit.*, p. 73.
[118] A. Pisapia, *op. cit.*, p. 61.
[119] A. Pisapia, *op. cit.*, p. 60.
[120] M. Soffientini, *op. cit.*, p. 156.
[121] Mondini Rusconi, *op. cit*, p. 215.
[122] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 218-219
[123] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 221
[124] G. Conti, *op. cit.*, p. 73
[125] R. Panetta, *op. cit.*, p. 135

l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, tranne nel caso in cui l'interessato non abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche."

Il generale principio della libertà di forme incontra un parziale limite in tre ipotesi nelle quali si richiede che il consenso sia almeno "esplicito". Deve considerarsi esplicito il consenso non desumibile da comportamento concludente, quando ricorre una delle seguenti ipotesi:

1. trattamento di dati sensibili (art. 9, par. 2, lett. a);
2. decisione unicamente basata su trattamento automatizzato (art. 22, par. 2, lett. c);
3. trasferimento di dati personali verso Paese terzo od organizzazione internazionale "non adeguati" (art. 49, par. 1, lett. a).

Dunque, a differenza della precedente disciplina, abrogata dal D.lgs. n. 101/2018, il consenso per i dati sensibili deve essere "esplicito". Ne deriva che nell'ipotesi in cui il trattamento riguarda le "categorie particolari di dati personali" (art. 9) è, pertanto, onere del titolare che tratta questi dati particolari acquisire e documentare i processi relativi ad una corretta acquisizione del consenso[126].

2.2.2 CONDIZIONI PER IL CONSENSO

L'art. 7 del GDPR disciplina le condizioni del consenso e prevede che ciascun titolare del trattamento deve distinguere i casi in cui è necessario acquisire il consenso dell'interessato dai casi in cui non sia necessario in quanto presente una diversa base giuridica di trattamento[127].

Il primo comma del suddetto articolo specifica: *«qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali».*

Il legislatore trasforma così con chiarezza l'esercizio del diritto (*rectius* della libertà), spettante all'interessato, in onere (o meglio in obbligo) del titolare del trattamento, cioè

[126] G. Conti, *op. cit.*, p. 42.
[127] M. Soffientini, *op. cit.*, p. 156.

del soggetto che esplica l'attività economica in discussione in funzione della tutela del soggetto a cui i dati personali si riferiscono[128].

Dunque, l'obbligo di basare il trattamento sul consenso, nei casi di legge, incombe esclusivamente sul titolare, in capo al quale sono allocati i poteri decisori sulle finalità e conseguentemente sui mezzi del trattamento. Inoltre, il titolare può delegare a responsabili e personale dipendente le connesse attività di raccolta del consenso, tuttavia incombe ugualmente sulla sua figura l'onere della prova[129] circa l'espressione del consenso[130].

Il paragrafo 2[131] dell'art. 7 enuncia la chiara indicazione della richiesta di consenso: ai fini della sua validità, risulta necessario non solo che il consenso sia espresso, ma che sia anche documentato per iscritto[132]. In questo senso, il Considerando 32 precisa che il consenso può essere raccolto attraverso una dichiarazione orale al fine di dimostrare la prova dell'intervenuto consenso o, in alternativa, attraverso una dichiarazione scritta che deve essere chiara e riconoscibile rispetto ad altre questioni[133].

Occorre che la richiesta di consenso sia presentata, quindi, in modo chiaramente distinguibile, comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, assicurando la piena consapevolezza da parte dell'interessato dell'equivalenza del proprio comportamento ad un consenso al trattamento dei dati[134].

In realtà, il GDPR non impone particolari forme per raccogliere il consenso dell'interessato, ma lascia il titolare libero di scegliere la modalità più opportuna per acquisire e per documentare il consenso degli interessati[135].

In stretta relazione con il diritto al consenso va considerata la richiesta di revoca: prestazione del consenso e revoca del medesimo costituiscono cioè due espressioni del medesimo diritto riconosciuto all'interessato.

---

[128] N. Zorzi Galgano, *op. cit.*, p. 68.

[129] Art. 7 "Condizioni per il consenso", paragrafo 1: *«Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali».*

[130] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 210.

[131] Art. 7 "Condizioni per il consenso", paragrafo 2: *«Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante».*

[132] A. Vivarelli, *op. cit.*, p. 67.

[133] Art. 7, par. 2, *ibidem.*

[134] A. Vivarelli, *op. cit.*, p. 69.

[135] G. Conti, *op. cit.*, p. 75.

Il diritto di revoca è sancito dal paragrafo 3[136] della disposizione in esame, la quale stabilisce il diritto dell'interessato di revocare il proprio consenso, precedentemente prestato, in qualsiasi momento.

Il titolare del trattamento è tenuto, quindi, ad informare l'interessato al momento in cui sta per raccogliere il consenso della possibilità di revocarlo[137]. Se l'interessato revoca il consenso, i trattamenti operati in virtù del consenso originariamente prestato sarebbero comunque leciti nel rispetto del principio del legittimo affidamento delle parti[138].

È opportuno distinguere le ipotesi in cui il trattamento non sia iniziato da quelle in cui, sulla base di un consenso validamente prestato, si sia dato inizio all'elaborazione dei dati[139]. Nel primo caso, è ammissibile una revoca *ad libitum*: come previsto dalla disposizione in parola *"il consenso è revocato con la stessa facilità con cui è accordato",* il che si traduce nel diritto di esercitare la revoca in assenza di giusta causa, quindi senza giustificati motivi. L'interessato può revocare il proprio consenso senza incontrare alcun limite e, soprattutto, senza dover indicare i motivi della sua ritrattazione, ancorando quest'ultima alla sussistenza di una giusta causa[140].

Nel caso in cui, invece, si sia dato avvio alle operazioni di trattamento, il consenso poi revocato deve ritenersi pienamente legittimo[141]. La revoca vale, quindi, soltanto *pro futuro*: non pregiudica la liceità del trattamento basata sul consenso prima che questo sia stato revocato, opera dunque *ex nunc* senza effetti retroattivi[142].

Il punto 4, dell'art. 7, recita *«Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».*

La norma fa riferimento al caso in cui si verifichino entrambe le seguenti condizioni: 1) l'utente è posto di fronte a un *aut aut*: o presta il consenso o non potrà fruire del

---

[136] Art. 7 "Condizioni per il consenso", paragrafo 3: *«L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato».*

[137] R. Panetta, *op. cit.*, p. 132.

[138] Nella normativa precedente il potere di revoca non era espressamente previsto come nel GDPR: Della direttiva 95/46/CE non vi era una norma *ad hoc*, mentre nell'ordinamento italiano si assumeva che il consenso fosse revocabile.

[139] La ricostruzione è riconducibile a S. Patti, *op. cit.*, p. 465 ss.

[140] A. Vivarelli, *op. cit.*, p. 77.

[141] G. Conti, *op. cit.*, p. 76.

[142] A. Pisapia, *op. cit.*, p. 63.

servizio; 2) il consenso ha ad oggetto, tra l'altro, un trattamento di dati non necessario – in quanto non strettamente funzionale – alla prestazione del servizio[143]. Si pensi al caso in cui, al fine di accedere ad un servizio, il titolare richieda all'interessato un consenso a ricevere comunicazioni commerciali dirette da parte del gestore, ma anche alla trasmissione di questi a operatori terzi ai fini, ad esempio dell'invio di comunicazioni commerciali, oppure ad acconsentire alla pubblicazione di proprie immagini e fotografie su siti e spazi web[144]. È ragionevolmente plausibile che, ove il consenso sia stato prestato in tali condizioni, il legislatore europeo ritenga che non sia stato prestato liberamente, ma "forzata" da parte del titolare pena l'esclusione del servizio.
Dunque, sulla base di un consenso viziato, i dati così acquisiti non devono ritenersi utilizzabili essendo il trattamento considerato illegittimo.

2.2.3 IL CONSENSO AL TRATTAMENTO PER LA PROFILAZIONE

Il problema del libero consenso si fa ancor più delicato in relazione ad uno dei trattamenti più insidiosi: quello della *profilazione*[145].
Ai sensi dell'art. 4 del GDPR, la profilazione viene definita come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nel relativo impiego al fine di valutare determinati aspetti personali relativi a una persona fisica e, in particolare, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti*".
L'attività di profilazione consiste, quindi, in quell'insieme di attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento o in determinate categorie omogenee (*cluster*).
Dal punto di vista commerciale, la profilazione permette di inviare pubblicità mirata e fornire servizi personalizzati al fine di rispondere esattamente ai desideri di ciascun consumatore. Tuttavia, secondo il Considerando n. 24, per stabilire la presenza di un'attività qualificabile come profilazione occore verificare che gli utenti siano tracciati su internet e che, eventualmente si siano adoperate tecniche di trattamento dei dati personali che consistono nella categorizzazione della persona fisica, in particolare per

[143] E. Tosi, *op. cit.,* p. 73.
[144] G. Conti, *op. cit*., p. 74.
[145] E. Tosi, *op. cit.*, p. 75.

adottare decisioni che la riguardano o analizzarne oppure prevederne le preferenze, i comportamenti e le posizioni personali.

L'art. 22 del GDPR precisa: *«L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».* Tale previsione non si applica nel caso in cui il trattamento sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, nel caso in cui sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e infine nel caso in cui si basi sul *consenso esplicito* dell'interessato.

In tale ultima ipotesi, è necessario che il titolare indichi analiticamente nel documento contenente l'informativa in che cosa si articola l'attività di profilazione nonché esponga in maniera chiara e comprensibile le conseguenze delle stesse[146].

Il Considerando 71, infatti, precisa: *«Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori».*

Sul delicato tema della profilazione era intervenuto, già nel 2015, il Garante italiano, il quale attraverso Linee guida ad hoc - in materia di dati personali per profilazione *on line*[147] - stabiliva le indicazioni da includere nell'informativa, le modalità di formalizzazione del consenso preventivo separato e ben distinto per le finalità di profilazione e il rispetto del diritto di opposizione[148].

Pertanto, qualora il titolare del trattamento intenda svolgere attività di marketing o di profilazione è necessario che la manifestazione del consenso sia, anche graficamente, separata dal consenso principale al fine di permettere all'interessato di esprimere consapevolmente e liberamente le proprie scelte[149].

---

[146] G. Conti, *op. cit.*, p. 108.
[147] Provvedimento 19 marzo 2015, n. 161, in *GUUE* n. 103 del 6 maggio 2015.
[148] A. Pisapia, *op. cit.*, p. 68.
[149] *Ibidem*.

In conclusione, una finalità concettualmente unica può in concreto far capo a due soggetti diversi e autonomi e richiedere perciò due consensi: l'interessato potrà naturalmente rifiutarli entrambi, potrà fornirne solo uno, potrà fornirli entrambi, senza conseguenze pregiudizievoli[150].

2.3 L'INFORMATIVA PRIVACY: REGOLE PER LA SUA REDAZIONE

2.3.1 DEFINIZIONE

Il titolare che voglia operare con i dati personali è tenuto ad informare l'interessato sul trattamento che intende effettuare, rendendolo edotto dei diritti che lo stesso può esercitare[151].

Come ben chiarito, infatti, dal Considerando 60, affinché un trattamento possa definirsi corretto e trasparente, è necessario che all'interessato sia resa un'informativa sull'esistenza del trattamento e delle sue finalità.

L'informativa è dovuta per qualsiasi trattamento e dunque a prescindere che esso sia fondato sul consenso o su altra condizione di liceità[152]. Infatti, qualsiasi sia la base giuridica del trattamento, l'interessato deve essere informato per poter esercitare il controllo sul flusso e sulle operazioni svolte sui propri dati, incluso il diritto di opporsi.

Il GDPR distingue in due diverse disposizioni le informazioni da rendere quando la raccolta dei dati avviene presso l'interessato (art. 13) e quelle da fornire quando i dati sono stati ottenuti non presso di lui, ma presso terzi (art. 14)[153].

Gli art. 13 e 14 del GDPR, quindi, disciplinano in modo dettagliato l'informativa e prevedono che essa debba contenere una serie di elementi considerati indispensabili perché l'interessato possa esercitare i propri diritti e manifestare un valido consenso[154].

Qualora le finalità del titolare venissero modificate nel tempo sarà necessario provvedere alla modifica dell'informativa e all'acquisizione di un nuovo consenso[155].

Conformemente ai principi di correttezza ed accountability, la tempestività della conoscenza delle informazioni da parte dell'interessato è un elemento fondamentale[156].

---

[150] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 216.
[151] Mondini Rusconi, *op. cit*., p. 210.
[152] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 185
[153] R. Panetta, *op. cit.,* p. 120
[154] M. Soffientini, *op. cit.*, p. 153
[155] A. Pisapia, *op. cit*, p.61
[156] R. Panetta*, op. cit.,* p. 126

A seconda di come vengono raccolti i dati, sono ravvisabili tre tipologie di informativa:
1) informativa diretta: se i dati vengono raccolti presso l'interessato, l'informativa dovrà essere resa al momento della raccolta dei dati personali (art. 13);
2) informativa successiva: se i dati sono raccolti presso altre fonti, l'informativa dovrà essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta dei dati (art. 14);
3) informativa ulteriore: necessaria nel caso in cui il Titolare modifichi le finalità originarie del trattamento. In tal caso, il documento a completamento dell'informativa originario deve essere consegnato prima dell'inizio del nuovo trattamento che altrimenti sarebbe sfornito della base giuridica corretta per garantirne la liceità[157].
L'obbligo incombe esclusivamente sul titolare, che può delegare alle attività esecutive il responsabile del trattamento e il personale dipendente.

Ugualmente sul titolare incombe l'onere probatorio di avere fornito l'informativa, in conformità con i principi generali[158]. Dunque, l'informativa deve essere fornita prima dell'acquisizione del consenso, pena la sua invalidità[159].

2.3.2 IL CONTENUTO DELL'INFORMATIVA

Il contenuto minimo dell'informativa, in parte più esteso rispetto a quello previsto nel Codice[160], è ora tassativamente elencato all'art. 13 del GDPR, nel caso in cui i dati siano raccolti presso l'interessato (direttamente), e all'art. 14, nel caso in cui i dati siano raccolti presso terzi (indirettamente)[161].
Gli elementi più rilevanti che il Titolare deve obbligatoriamente comunicare sono:

---

[157] Per approfondimenti sulla questione si veda A. Pisapia, *op. cit.*, p. 62
[158] Art. 24 del GDPR, il quale dispone: *«(…) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.»*.
[159] A. Pisapia, *op. cit*, p. 61.
[160] Art. 13 del GDPR: *«L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:*
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile».
[161] R. Panetta, *op. cit.*, p. 123.

(i) l'identità e i dati di contatto del Titolare del trattamento (e, se del caso, quelli del rappresentante);
(ii) se designato, i dati di contatto del Data Protection Officer (DPO);
(iii) le finalità del trattamento, nonché la sua base giuridica;
(iv) gli eventuali destinatari o categorie di destinatari dei dati personali;
(v) l'intenzione di trasferire i dati personali in un paese terzo o a un'organizzazione internazionale e, se del caso, specificare attraverso quali strumenti.

Nel caso in cui si tratti di un'informativa "successiva", oltre le indicazioni di cui sopra, va specificato anche:

(i) l'origine dei dati personali e se provengono da fonti accessibili al pubblico;
(ii) le categorie di dati personali trattate.

Infine, nel caso di un'informativa "ulteriore", vanno rese ulteriori rilevanti informazioni:

(i) indicazione della nuova finalità;
(ii) durata di conservazione o in subordine, se impossibile, criteri per determinarla.

Inoltre, vanno segnalate altre tre regole:

1) se il trattamento prevede processi decisionali automatizzati inclusa la profilazione di cui all'art. 22, paragrafi 1 e 4, il titolare dovrà comunicare all'interessato che sta svolgendo questo tipo di attività, fornire informazioni significative e accessibili sulla logica utilizzata e spiegare l'importanza e le conseguenze del trattamento per l'interessato (in particolare, se gli interessati al trattamento sono minori);
2) Il titolare è tenuto ad informare l'interessato se intende trattare i dati per finalità diverse e a tal fine è necessario un nuovo consenso;
3) Se i dati vengono raccolti indirettamente, il titolare è tenuto a dichiarare la fonte da cui hanno origine i dati trattati e specificare, eventualmente, se essi se gli stessi provengano da fonti accessibili al pubblico[162].

2.3.3 LA FORMA DELL'INFORMATIVA

L'informativa va resa in linea di principio in forma scritta e preferibilmente in formato elettronico; in alternativa, oralmente, soltanto su richiesta dell'interessato e purché sia comprovata la sua identità (art. 12, par. 1). Il linguaggio deve essere semplice e chiaro e,

[162] GDPR Art. 14, par. 2, lett. *f.*

se l'informativa è scritta, il testo deve essere ben strutturato e comprensibile in tutti i suoi passaggi[163].

Il Regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, par. 7).

I doveri di semplicità e chiarezza devono essere, infine, rafforzati nell'ipotesi in cui l'interessato al trattamento sia un soggetto minorenne e, in questo frangente, l'informativa e le modalità di espressione del consenso devono essere particolarmente accessibili[164].

A tal proposito, l'art. 12, par. 1 e il Considerando 58[165] evidenziano la specifica protezione di cui hanno bisogno i minori: il titolare deve apprestare cautele maggiori nel rendere le informazioni ad essi dirette, utilizzando un linguaggio ancora più semplice (immagini, vignette, fumetti)[166].

2.3.4 VIOLAZIONE DELLA DISCIPLINA SULL'INFORMATIVA

La violazione della disciplina in tema di informativa (art. 13 e 14) è punita con l'irrogazione di una sanzione amministrativa pecuniaria fino a 20.000.000€ (venti milioni), o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

CAPITOLO 3

LA TUTELA DEI MINORI

3.1 L'EVOLUZIONE TECNOLOGICA E IL DIRITTO ALLA PRIVACY DEI MINORI

L'avvento della tecnologia in tutti i settori della vita dell'uomo moderno ha contribuito a creare diversi problemi che si caratterizzano principalmente, non solo, per la gestione dei flussi di informazioni ma anche e soprattutto per la tutela dei dati riferibili alle persone fisiche.

---

[163] R. Panetta, *op. cit.*, p. 131.
[164] G. Conti, *op. cit.*, p. 76.
[165] Lo annuncia espressamente il Considerando 58, ai sensi del quale: *«Dato che 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».*
[166] R. Panetta, *op. cit.*, p. 131.

In un sistema multitecnologico dove la riduzione delle distanze, rispetto al passato, rappresenta sicuramente un dato oggettivo della realtà contemporanea, tali dati, necessitano di particolare tutela proprio perché indicano tutte le peculiarità delle singole entità, persone fisiche o enti che siano, ed il ritardo delle legislazioni di molti Stati Occidentali nel recepire tali istanze è oggi una verità che non necessita di alcuna dimostrazione.

Addirittura, se si pensa che nel gioco tecnologico moderno ad uso capitalistico la presenza, nelle piattaforme online, delle persone fisiche minori di età è reso possibile senza non troppi ostacoli, si comprende come la tutela dei dati di tali soggetti richieda uno sforzo maggiore ad opera dei singoli Stati.

Al giorno d'oggi, il minore dispone di numerosi ambiti e strumenti per esercitare i diritti a lui riconosciuti, non solo dall'ordinamento interno ma altresì dalle Convenzioni internazionali, anche attraverso l'utilizzo di tecnologie in grado di permettere nuovi modelli di relazione[167].

L'avvento dei c.d. *social media* ha determinato una rivoluzione nelle modalità di interazione e comunicazione personale e nel caso dei minori destano preoccupazione gli sviluppi legati ad un uso indiscriminato e poco avveduto di apparecchi, si pensi ai giocattoli interattivi specificamente destinati ai bambini ovvero agli *smartwatch* sempre più spesso utilizzati da soggetti giovanissimi.

Secondo una recente statistica dell'Unicef[168], ogni giorno, nel mondo, 175 mila bambini e ragazzi si collegano ad Internet per la prima volta nella loro vita e, secondo una stima globale, i minorenni hanno un tasso di presenza sul web del 71% rispetto al 48% della popolazione totale.

Ma già in uno studio del 2015[169] venivano individuati diversi caratteri comuni ai social media: a) l'utilizzo generalizzato della tecnologia del web 2.0; b) la profilazione degli utenti del sito o della applicazione; c) la connessione dei profili con quelli di altri utenti o gruppi di utenti.

È quindi evidente che le prassi di marketing attraverso i social media, i giochi online e le applicazioni *mobile* hanno un impatto evidente sul comportamento dei minori.

---

[167] Si fa riferimento all'art.10 c.c. concernente la tutela dell'immagine, al combinato disposto degli artt.4,7,8 e 145 del d.lgs. n.196/2003 riguardanti la tutela della riservatezza dei dati personali, agli artt.1 e 16, 1 comma, della Convenzione di New York del 20-11-1989 ratificata dall'Italia con legge 27-5-1991 n.176.

[168] Dati disponibili su: *Safer Internet Day 2018*, una guida sull'uso sicuro del web per i bambini.

[169] J. A. Obar, S. Wildman, *Social Media Definition and the Governance Challenge: An Introduction to the Special Issue*, in *"Telecommunications Policy"*, vol. 39, 2015, n. 9, pp. 745-750.

Nei giochi online, ad esempio, la profilazione può servire per individuare i giocatori più propensi a spendere somme di danaro ovvero per fornire annunci personalizzati a cui non corrisponde una maturità da parte del minore nel riconoscere la ragione commerciale di una pratica di marketing.

Tutti questi elementi mettono in luce i rischi per la privacy e per l'autonomia negoziale degli utenti minori di età[170].

Il concetto di privacy, che secondo il significato originario riguardava esclusivamente l'intimità della vita privata[171], si è quindi modificato nel corso dei decenni includendo altresì il diritto alla protezione dei dati personali.

In realtà, ad una attenta osservazione, ci si accorge che il quadro normativo della tutela dei minori sui media, per quanto articolato, non sembra mai sufficiente a proteggere in modo efficace i bambini durante le loro attività in rete.

Pertanto, assume oggi una rilevanza strategica la tutela dei minori nell'utilizzo dei servizi della società dell'informazione al fine di evitare le conseguenze negative di tali attività durante la navigazione online.

Sul terreno della tutela della privacy il minore esige di essere particolarmente protetto da un'esposizione o sovraesposizione di dati per i possibili rischi sullo sviluppo della personalità, per l'esteso tracciamento della persona nel corso dell'intera vita e per i furti di dati o di identità.

Sono stati quindi gli stessi giuristi ad interrogarsi sulla necessità di rendere chiare le regole giuridiche moderne da applicare ai minori al fine di rendere effettiva la loro protezione in quanto soggetti pur sempre deboli e non capaci di discernimento in relazione a talune scelte che inevitabilmente hanno un impatto duraturo e negativo sulla loro esistenza.

Come evidenziato dal parere 5/09 WP163 del Gruppo di lavoro per la tutela dei dati ex art.29 *"i dati personali che l'utente inserisce online, insieme ai dati che ne descrivono le azioni e le interazioni con altri utenti, possono creare un profilo articolato dei suoi interessi e delle sue attività. I dati personali pubblicati sui siti di social network possono essere usati da terzi per svariati scopi, anche commerciali, e possono comportare gravi rischi come il furto di identità, il danno economico, la*

[170] G. Pedrazzi, *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy, in Informatica e diritto*, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 439.

[171] Su privacy e riservatezza, cfr. C. M. Bianca, *Diritto civile, I, La norma giuridica, I soggetti,* Giuffrè, Milano, 2002, p. 180. La distinzione è legislativamente espressa, chiaramente, anche dall'art.2 D.lgs. n.196/2003 (cd. Cod. privacy).

perdita di opportunità commerciali e di possibilità di impiego e pericoli per l'incolumità fisica"[172].

Su tali basi, non è affatto un errore sostenere che la tutela dei dati personali e della privacy dei minori[173] ha rappresentato un problema particolarmente rilevante con l'avvento dei social network.

La minore età, infatti, è legata a diritti rafforzati rispetto agli adulti, per cui il trattamento da parte delle aziende dei dati deve essere regolamentato in maniera differente.

I dati degli utenti vanno cioè raccolti con molta attenzione[174] e la persona fisica deve sempre essere informata sulle eventuali adesioni, questo perché occorre specificare i trattamenti che riguardano l'uso dei dati personali.

Basti pensare che nel caso dei minori sono le stesse aziende a promuovere offerte di servizi specifici che incidono sulla loro formazione potendo, il più delle volte, determinare una lesione non solo della loro identità ma anche di ulteriori diritti riconosciuti Costituzionalmente ovvero da altre fonti sovranazionali[175].

In questo quadro, come illustrato di seguito, la normativa sulla protezione dei dati dei minori di età ha da sempre avuto alla base l'idea di evitare pericoli tra loro diversi, in modo particolare quello alla salute ed alla integrità psico-fisica di soggetti facilmente influenzabili nelle loro scelte in una fase della vita dove l'attenzione allo sviluppo della

---

[172] M. Orofino, *Minori e Diritto alla protezione dei dati personali*, in Aa.Vv., *Privacy, minori e cyberbullismo*, Torino, 2018, 14 e ss., evidenzia che *"per quanto riguarda il trattamento dei dati necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri il WP sottolinea che il principio del Best Interest del minore può essere classificato anch'esso come un interesse pubblico"*.

[173] B. Saetta, *Minori e protezione dati personali*, www.protezionedatipersonali.it/minori-e-protezione-dati-personali.

[174] F. Pastore, *Il consenso per i minori: cosa cambia con il GDPR*, www.itgovernance.eu/blog/it/il-consenso-per-i-minori-cosa-cambia-con-il-regolamento-privacy-gdpr.

[175] La Costituzione italiana, entrata in vigore il 1° gennaio 1948, dedica ai minori quattro articoli: 30, 33, 34 e 37. Per quanto riguarda la Convenzione Onu, ci sono ben 42 articoli tutti dedicati ai bambini e agli adolescenti. Sono quattro i principi fondamentali della Convenzione sui diritti dell'infanzia e dell'adolescenza:

a) *Non discriminazione (art. 2): i diritti sanciti dalla Convenzione devono essere garantiti a tutti i minori, senza distinzione di razza, sesso, lingua, religione, opinione del bambino/adolescente o dei genitori.* ***b)*** *Superiore interesse (art. 3): in ogni legge, provvedimento, iniziativa pubblica o privata e in ogni situazione problematica, l'interesse del bambino/adolescente deve avere la priorità.* ***c)*** *Diritto alla vita, alla sopravvivenza e allo sviluppo del bambino (art. 6): gli Stati devono impegnare il massimo delle risorse disponibili per tutelare la vita e il sano sviluppo dei bambini, anche tramite la cooperazione tra Stati.* ***d)*** *Ascolto delle opinioni del minore (art. 12): prevede il diritto dei bambini a essere ascoltati in tutti i processi decisionali che li riguardano, e il corrispondente dovere, per gli adulti, di tenerne in adeguata considerazione le opinioni.*

personalità deve essere inevitabilmente al centro delle legislazioni nazionali e sovra nazionali.

3.2 LA LEGISLATURA PRECEDENTE AL GDPR IN MATERIA DI TUTELA DEI MINORI

Con l'avvento del Regolamento Europeo n. 679/2016, entrato in vigore il 25 maggio 2018, il quale non necessita di trasposizione nelle legislazioni nazionali in quanto di immediata applicazione[176], si ricava come la tutela della privacy, con riguardo al minore, vada intesa non solo come minimizzazione dei dati a lui relativi (art. 5, par. 1, GDPR)[177], ma anche e soprattutto nell'ottica del consenso informato attraverso la necessità di trasparenza delle informazioni che deve avvenire *"mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano"*[178].

Prima del GDPR, i principali *social network* prevedevano una età minima per iscriversi fissata a 13 anni, questo perché le principali aziende americane applicavano e continuano ad applicare il limite fissato dalla legge federale Usa (Children's Online Privacy Protection Act. c.d. COPPA[179]) secondo cui nessuna persona giuridica (tranne gli enti pubblici) può raccogliere dati relativi a minori di 13 anni.

---

[176] Per un approfondimento sul Regolamento Privacy GDPR (*General Data Protection Regulation*) n.679/2016, *"La tutela dei dati personali dei minori"* di G. CAPILLI, cap.XII.

[177] L'articolo 5, par.1, lett.c, del GDPR stabilisce che *"1. I dati personali sono: (...) lett.c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)*.

[178] Il testo completo del Considerando n. 32 GDPR stabilisce che *"Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso"*.

[179] *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. 6501–6505, §312.5. Parental consent, disponibile sul sito della *Federal Trade Commission: www.ftc.gov*.

Il COPPA prevede altresì il preavviso di trattamento ai genitori del minore ed il consenso degli stessi dimostrabile a richiesta oltre che l'obbligo di adottare misure di sicurezza ed il divieto di sollecitare dati non necessari al trattamento.
La normativa europea precedente al GDPR, invece, non prevedeva un limite espresso ma solo indiretto e ricavabile dal quadro normativo generale.
In Italia, ad esempio, la capacità di agire, e cioè la capacità del soggetto a compiere atti che incidono nella propria sfera giuridica, si acquista con la maggiore età, quindi a 18 anni, per espressa previsione dell'art. 2 del Codice Civile[180].
Tuttavia, il minore, di età compresa tra 14 e 18 anni, ha una capacità giuridica attenuata mentre il minore dei 14 anni non è imputabile e non ha capacità giuridica.
Come si vede, il legislatore italiano ha riconosciuto, in determinati casi, al minore di età il potere di decidere relativamente a propri interessi che trovano tutela nei diritti fondamentali Costituzionalmente riconosciuti.
In altre parole, l'interpretazione di cui all'art. 2 del Codice Civile necessita di distinguere gli atti a contenuto patrimoniale, rispetto ai quali non può mai venire meno un controllo da parte dell'esercente la responsabilità genitoriale, dagli atti a contenuto non patrimoniale, ove viceversa si considera sufficiente la capacità di discernimento del minore tenendo conto della sua maturità di giudizio.
Quanto invece al cd. Codice della Privacy, posto in essere nel nostro ordinamento giuridico con D.lgs. n.196/2003, nulla è indicato in via generale circa i requisiti di capacità per la prestazione del consenso privacy e quindi sulla idoneità del minore a prestarlo, in quanto l'unica norma che richiamava la capacità di agire di chi presta il consenso, l'articolo 24, è stata abrogata dal decreto legislativo n.101/2018, riferendosi tra l'altro a situazioni speciali, o secondo un'altra interpretazione, eccezionali e quindi non applicabili analogicamente[181].
In assenza di una norma generale espressa, nell'ordinamento italiano si era fatta quindi strada la tesi che il minore potesse autorizzare il trattamento dei dati, salvo l'accertamento della sua capacità naturale e cioè della capacità di intendere e di volere.

[180] A. Scarpa, *Legislazioni e Giurisprudenza per gli interessi del minore (Le riflessioni della dottrina sulla capacità di agire*, in *Dir.giur*., 1992, pag.41, ritiene l'art.2 del codice civile una norma generica anziché generale *"idonea ad avallare criteri operativi che funzionano da passprtout" e conclude ritenendo preferibile il metodo relativistico".*
[181] S. Patti, *Consenso, sub art. 23*, in Aa.Vv. *La protezione dei dati personali.* Commentario a cura di C. M. BIANCA E F. D. BUSNELLI, Padova (Cedam), 2007, p. 544 ss.

Tuttavia, la dottrina maggioritaria[182] ha da sempre sostenuto, con riferimento alla capacità dei minori di età di manifestare il consenso al trattamento dei dati, la necessità di verificare se l'attività sui dati determini o meno una esposizione del minore a pubblico, in quanto se il trattamento dei dati personali del minore infra sedicenne non determina esposizione a pubblico e gli stessi dati sono acquisiti dal titolare del trattamento per fini specifici, ad esempio per marketing, allora il consenso al trattamento dei dati deve essere necessariamente manifestato da chi ne esercita la responsabilità genitoriale.

3.3 LA TUTELA DEI MINORI E L'ART. 8 DEL GDPR

Ai sensi del Considerando n. 38 del GDPR è stabilito che *"I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente ai minori stessi".*

La specifica protezione dei minori è altresì indicata nel Considerando n. 58 del GDPR, atteso che la modalità di comunicazione delle informazioni deve avvenire attraverso l'utilizzo di un linguaggio semplice e facilmente comprensibile[183].

In altre parole, il legislatore europeo ha previsto la necessità per i minori di età di ottenere tutele giuridiche rafforzate in quanto soggetti particolarmente vulnerabili e facilmente influenzabili dalla pubblicità comportamentale[184].

---

[182] A. Vivarelli, *op. cit.,* p. 49.

[183] Nello specifico, il Considerando n. 58 al GDPR stabilisce che *"Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che 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".*

[184] Parte della dottrina, R. Panetta, *op. cit.,* pag.114, sostiene che in realtà *"ad uno sguardo più attento all'ordito normativo del GDPR, ci si rende conto di come la stessa sensibilità rispetto a questa categoria di interessati non sia stata analogamente mantenuta con riguardo ad elaborazioni di dati*

Il nuovo Regolamento europeo ha quindi previsto, come adesso vedremo mediante l'articolo 8, una regolamentazione specifica che però non tocca la capacità di agire del minore che resta disciplinata dall'ordinamento civile nazionale.

In particolare, l'art. 8 del GDPR, intitolato "*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione"* più specificamente prevede che *"Qualora si applichi l'art. 6, paragrafo 1, lettera a) ("quando l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento dei dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.*

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore a 13 anni.

Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, formazione o l'efficacia di un contratto rispetto a un minore"[185].

La norma può essere vista in parallelo con lo statunitense Children's Online Privacy Protection Act 1998 (COPPA), in vigore dal 2000 e già in precedenza richiamato, che però prevede una regolamentazione maggiormente più articolata: l'età del consenso digitale è innanzitutto fissata a 13 anni, i metodi di verifica dell'identità del genitore sono molteplici, la rappresentanza dei genitori nella prestazione del consenso è obbligatoria così come obbligatorio è per il titolare del trattamento adottare misure di sicurezza.

---

molto penetranti la personalità dell'individuo. Uno degli usi a valle più frequenti consiste nella creazione di profili personali o di utente, e persino psicometrici, come è emerso dalle risultanze dello scandalo Facebook – Cambridge Analytica. Nella stessa direzione, con effetti ancora più preoccupanti, si pone il progetto del Governo Cinese cd. "credit social score", la cui logica è di realizzare profili molto accurati dei propri cittadini partendo dai dati raccolti e di creare, poi, delle classificazioni sulla base del punteggio parametrato al comportamento del singolo cittadino desunto da quelle informazioni. Lo score che si raggiunge determina alcuni benefici se positivo o ne rimuove degli altri se negativo".

[185] Linee guida nell'interpretazione della norma sono state fornite dal *Working Party art.29, Guidelines on Consent under Regulation 2016/679, 17 EN/WP259*.

Dunque, la norma di cui all'art. 8 del Regolamento Europeo n. 679/2016, non riguarda genericamente tutti i trattamenti di dati di minori, ma per la sua applicabilità richiede l'esistenza di due requisiti:

1) che vi sia un'offerta diretta di servizi della società dell'informazione a soggetti minori di 16 anni.

   Per la definizione di *"servizio della società dell'informazione"* l'art. 4, par. 25[186], del GDPR rinvia all'art. 1, par. 1, lett. b) della Direttiva UE 2015/1535 del 09 settembre 2015 e lo descrive come *"qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi"*.

   Più in particolare, viene definito cosa si intende per *"a distanza"* (servizio fornito senza la presenza simultanea delle parti), *"via elettronica"* (servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento, compresa la compressione digitale, e di memorizzazione di dati e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici), *"a richiesta individuale di un destinatario di servizi"* (servizio fornito mediante trasmissione di dati su richiesta individuale);

2) che il trattamento dei dati dei minori sia basato sul consenso[187].

   Se, invece, il trattamento ha altra base giuridica, come ad esempio il rispetto di un obbligo di legge ovvero di legittimi interessi, la norma di cui all'art. 8 non si applica.

   In presenza di questi due requisiti, l'articolo 8 stabilisce il divieto di offerta diretta di servizi digitali ai minori di 16 anni, a meno che non sia raccolto il consenso dei genitori, accertando che il consenso sia dato dall'esercente la responsabilità genitoriale.

   Con riferimento ai *"servizi compositi"* [188], quando un servizio della società dell'informazione costituisce una parte integrante di un servizio generale la cui componente principale non è un servizio della società dell'informazione, lo stesso non rientra nella specificazione.

   Viceversa, qualora il servizio presenti due componenti economicamente indipendenti, una delle quali è la componente online e l'altra è la consegna fisica o la distribuzione

[186] Il paragrafo 25 dell'art. 4 del GDPR stabilisce il *"servizio della società dell'informazione: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio"*.

[187] R. Panetta, *op. cit.,* p. 112

[188] Con riferimento ai servizi compositi, una attenta analisi viene realizzata dall'Avvocato S. Coppola del foro di Matera in *www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-e-minori-gestire-consenso-e-privacy-sui-social-che-ce-da-sapere/.*

di merci, la prima rientra nella definizione di servizio della società dell'informazione, mentre la seconda no.

A titolo esemplificativo, se un minore acquista online suonerie per *smartphone,* la raccolta dei dati (nome, cognome, indirizzo e-mail, dettagli di pagamento) sarà necessaria all'esecuzione di un contratto e pertanto il trattamento dei dati sarà lecito ai sensi dell'art. 6 del GDPR[189].

Se, invece, il titolare intende utilizzare l'indirizzo e-mail del minore anche per l'invio di newsletter, sarà necessario raccogliere il suo consenso in quanto il trattamento dei dati personali per finalità di marketing non rientra nell'ambito del contratto[190].

In sostanza, il GDPR introduce una deroga alla regola generale fissata dal nostro ordinamento giuridico in materia di capacità di agire: compiuti i sedici anni, si raggiunge quella che è stata definita come "età digitale"[191] necessaria per il trattamento dei propri dati personali anche con riferimento alla materia della profilazione.

Inoltre, come previsto dall'art. 8 del GDPR, tale limite può essere ulteriormente abbassato dagli Stati nazionali ma non può mai scendere al di sotto dei 13 anni.

È fondamentale specificare che la norma di cui all'art.8 del Regolamento Europeo n. 679/2016 riguarda soltanto la legittimità del consenso al trattamento dei dati personali ma non incide sulla validità del contratto sottostante, il cui regime giuridico rimane disciplinato dalla legislazione nazionale o da quella del foro competente a decidere eventuali controversie relative al servizio[192].

---

[189] L'art. 6 del GDPR, intitolato *"Liceità del trattamento",* stabilisce, al 1 paragrafo, che *"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".

[190] cfr. S. Coppola, *op. cit.*

[191] Trattasi di una interessante espressione utilizzata da B. Saetta, *op. cit.*

[192] In particolare, il recente parere del Working Party art.29, *"Guidelines on consent under Regulation 2016/679"*, pubblicato in via definitiva il 10 aprile 2018 (Opinion n. 259), è chiarissimo nel precisare che il consenso di cui all'art.8 non riguarda la validità di eventuali contratti che sia necessario stipulare fra provider e user ai fini della fornitura del servizio. Il regime giuridico dei contratti resta sempre disciplinato dalla legislazione nazionale o da quella del foro competente a decidere eventuali controversie relative al servizio.

Infatti, il par. 3 dell'art. 8 del GDPR stabilisce che le norme relative ai requisiti di autorizzazione genitoriale nei confronti dei minori non pregiudicano *"le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore"*.

Di conseguenza, i requisiti per la validità del consenso all'uso dei dati relativi a minori rientrano in un quadro giuridico da considerarsi distinto dal diritto contrattuale nazionale.

Il GDPR prevede quindi dei casi esenti da consenso quando il trattamento dei dati è necessario per obblighi contrattuali, per obblighi derivanti da legge, per interessi vitali, per il servizio pubblico ovvero quando il trattamento è basato sui legittimi interessi.

La norma di cui all'art. 8 del GDPR non intende affatto precludere ai minori di 16 anni l'accesso alla rete e ai suoi servizi ma impone a chi offre un servizio della società dell'informazione di richiedere il consenso informato per poter legittimamente trattare i suoi dati personali e di accertare che l'interessato sia in grado di prestare validamente tale consenso.

A questo scopo, e solo per questo, fissa in sedici anni l'età necessaria affinché tale consenso sia valido ai fini della legittimità dei trattamenti, salvo appunto diversa decisione nazionale.

3.4 LE NOVITÀ APPORTATE DALL'ART. 8 DEL GDPR

È evidente che la principale novità introdotta dall'art. 8 del GDPR è rappresentata dalla previsione di un'età per la liceità del consenso[193].

In realtà, già nell'anno 2012, quando tale norma veniva pensata e ritenuta necessaria per la protezione dei minori, fu previsto il limite di 13 anni per la prestazione del consenso ed il Gruppo di Lavoro dell'art. 29 suggerì che l'ambito di applicazione fosse esteso al di fuori dei servizi della società dell'informazione.

Ma non seguì alcuna discussione in seno al Parlamento europeo ed il Consiglio innalzò la soglia a 16 anni adottando un approccio per così dire flessibile conferendo agli Stati Membri la possibilità di prevedere soglie più basse fino a 13 anni.

[193] In senso critico rispetto all'adozione della soglia dei 16 anni, e a favore invece della più bassa soglia dei 13, L. Bolognini, C. Bistolfi, *L'età del consenso digitale*; Boccia Artieri G. esamina la questione dal punto di vista sociologico e comportamentale in *op. cit.*

L'art. 8 ha anche previsto, in relazione al consenso del minore infra-sedicenne, la possibilità per il genitore non solo di rappresentare legalmente il figlio ma altresì di autorizzare il trattamento dei dati personali.

Un tale controllo preventivo mediante autorizzazione e non solo sostituzione (che è la regola della rappresentanza legale) era già stato ritenuto ammissibile nel nostro ordinamento, con riguardo in generale all'agire dell'incapace, in base ad una interpretazione della norma sulla rappresentanza legale del minore[194].

Un simile sistema è in grado di valorizzare la funzione educativa del genitore nella costruzione della personalità del soggetto, senza mortificare la libertà decisionale del minore in un regime intermedio tra rappresentanza e autonomia[195].

Dall'altro lato, quanto ai metodi per la verifica del consenso, la previsione legislativa nulla dice circa la possibilità di verificare se l'intervento dell'esercente la responsabilità genitoriale nella prestazione del consenso è realizzabile, non solo in caso di creazione di identità digitali ma anche al momento della richiesta di autorizzazione o sostituzione[196].

Il GDPR, che richiede solo implicitamente la verifica dell'età del minore, affronta in via approssimativa il problema della identificazione del titolare della responsabilità genitoriale, rimettendo al titolare del trattamento ed alla sua responsabilità il compito di individuare i criteri più idonei in considerazione delle tecnologie disponibili[197].

La questione avrebbe potuto essere disciplinata in via più specifica e meno affrettata[198], in considerazione del fatto che il problema dell'anonimato sul web e nei programmi informatici rappresenta il principale rischio da affrontare prima di valutare ogni disciplina relativa all'accesso del minore ad internet.

In una prospettiva di comparazione, il problema è stato diversamente disciplinato dalla normativa statunitense che suggerisce una serie di meccanismi di verifica: l'utilizzo di una carta di credito che prevede per ogni singola operazione una notifica al suo titolare,

---

[194] C. M. Bianca, Diritto civile, I, La norma giuridica, *op. cit.,* p. 238.

[195] C. M. Bianca, *ult. op. loc. cit.*

[196] I. A. CAGGIANO nell'articolo *"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 http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=24&idn=2&idi=-1&idu=-1.

[197] Si rammenta che l'art. 8 del Regolamento prevede che *"Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili".*

[198] I. A. Caggiano nell'articolo *"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 http://www.ejplt.tatodpr.eu/Article/Archive/index_html?ida=24&idn=2&idi=-1&idu=-1.

la connessione del genitore con il personale dell'app tramite video conferenza, la verifica della identità del genitore tramite documento di identità[199].
Tali metodi, probabilmente, saranno recepiti anche in ambito europeo ma il legislatore comunitario ha purtroppo perso una fondamentale occasione per indicare i criteri cui ispirarsi nei diversi canali di comunicazione in base al rischio per il minore.
Infine, ai sensi dell'art. 83, par. 4, lett. a) e par. 5 del GDPR, nell'ipotesi di violazione delle norme sul consenso del minore si prevede che la sanzione amministrativa pecuniaria può giungere fino a 10 milioni per il titolare o per le imprese (se superiore) fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente.
O ancora, ai sensi del paragrafo 5 dell'art. 83, la sanzione può ammontare fino a 20 milioni di euro o per le imprese (se superiore) fino al 4% del fatturato totale annuo dell'esercizio precedente.

3.5 IL DECRETO LEGISLATIVO N. 101 DEL 2018[200]

Prima dell'approvazione definitiva del decreto legislativo n.101/2018, la sua prima bozza, all'art. 6, rubricato *"Consenso del minore in relazione ai servizi della società dell'informazione"*, stabiliva che *"1) In applicazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento di propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. 2) In relazione all'offerta diretta dei servizi di cui al comma 1, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che il consenso sia prestato o autorizzato da chi esercita responsabilità genitoriale. 3) Il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, facilmente accessibile e comprensibile dal minore, le informazioni e le comunicazioni relative al trattamento che lo riguardi".*
Successivamente ai passaggi nelle commissioni parlamentari, lo schema del futuro decreto legislativo disponeva invece che *"1) Al consenso del minore al trattamento*

[199] COPPA, §312.5 (Parental consent).
[200] Trattasi del Decreto Legislativo recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati)"* pubblicato in Gazzetta Ufficiale, Serie Generale n.205 del 04 settembre 2018, entrato in vigore il 19 settembre 2018.

dei propri dati personali, in relazione ai servizi della società dell'informazione, si applicano le condizioni di cui all'art. 8, paragrafo 1, del Regolamento. In relazione a tali servizi, il trattamento dei dati personali del minore di età inferiore a SEDICI anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che il consenso sia prestato o autorizzato da chi esercita la responsabilità genitoriale. 2) In relazione all'offerta diretta dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, facilmente accessibile e comprensibile dal minore, le informazioni e le comunicazioni relative al trattamento che lo riguardi".

È evidente come in tali passaggi successivi veniva meno la possibilità per il minore di 14 anni di prestare direttamente il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione (vecchio comma 1).

Possibilità ammessa dal GDPR che, tuttavia, il legislatore aveva deciso di non esercitare eliminando la distinzione tra minore infra-quattordicenne, per il quale era necessario il consenso o l'autorizzazione genitoriale, e minore quattordicenne, in relazione al quale invece difettava tale tutela rafforzata.

Con ulteriore successiva modifica, il D.lgs. n.101/2018 ha stabilito definitivamente che *"In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi. Art. 2-sexies (Trattamento di categorie particolare di dati personali necessario per motivi di interesse pubblico rilevante)".*

In particolare, l'art. *2-quinquies* del Codice della Privacy così come adeguato dal Decreto Legislativo n.101/2018, stabilisce che il minore che ha compiuto l'età di 14 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione, ponendo pertanto il

legislatore un evidente collegamento con la disciplina del consenso in riferimento agli atti sessuali[201].

Pertanto, se il minore afferma di aver raggiunto l'età del consenso digitale, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare la veridicità della dichiarazione in quanto se un minore presta il consenso senza avere l'età sufficiente, il trattamento dei dati sarà illecito.

Il GDPR però, come già ricordato in precedenza, non prevede modalità pratiche per raccogliere il consenso del genitore e conseguentemente spetta alle società dell'informazione porre in atto le misure ragionevoli per accertare che il consenso sia prestato o autorizzato, potendo essere sufficiente la verifica della responsabilità genitoriale a mezzo posta elettronica ovvero chiedere ulteriori prove per dimostrare il consenso.

In Italia, il titolare del trattamento che vuole assicurarsi che i clienti minorenni si abbonino ai servizi esclusivamente con il consenso dei genitori o tutori, potrà chiedere all'utente se ha più o meno di 14 anni e, nel caso affermi di aver un'età superiore ai 14 anni, dovrà effettuare controlli appropriati per verificarne la veridicità.

Viceversa, se l'utente dichiara di avere un'età inferiore ai 14 anni, il titolare del trattamento può accettare tale dichiarazione senza ulteriori verifiche ma il servizio lo informerà della necessità che un genitore acconsenta o autorizzi il trattamento prima che venga erogato il servizio medesimo[202].

Solo dopo aver compiuto i 14 anni, il minore potrà manifestare il consenso al trattamento dei dati personali e rientrare nel pieno controllo del suo trattamento e, di conseguenza, confermare, modificare o revocare il consenso prestato o autorizzato dal titolare della responsabilità genitoriale.

Nel caso invece di inattività del minore, il consenso prestato o autorizzato dal genitore continuerà ad essere un presupposto valido per il trattamento.

A tal proposito, in conformità con i principi di correttezza e responsabilizzazione, il titolare del trattamento deve informare il minore di questa possibilità.

[201] R. Panetta, *op. cit.,* pag. 113.
[202] Avv. S. Coppola, *op. cit.*

3.6 LE APPLICAZIONI GIURISPRUDENZIALI DELL'ART. 8 DEL GDPR

La giurisprudenza nazionale ha avuto modo di esprimersi in più occasioni in materia di tutela dei minori nel caso di trattamento dei loro dati personali.

Prima del Decreto Legislativo n.101/2018, l'orientamento dei tribunali italiani[203] è stato conforme nel ritenere come l'inserimento di foto di minori sui social network rappresenta comportamento potenzialmente pregiudizievole per determinare la diffusione di immagini ad un numero indeterminato di persone.

Ulteriore pericolo è stato poi individuato nella condotta di soggetti che "taggano" le foto online dei minori e, con procedimenti di fotomontaggio, ne ottengono materiale pedopornografico da far circolare fra gli interessati.

Particolarmente interessante in materia è la pronuncia del Tribunale di Roma, Sez.I Civ., del 23 dicembre 2017, che non solo ha condannato la madre ad eliminare da Facebook tutte le foto del figlio sedicenne ma ha altresì statuito che, in caso di mancato rispetto dell'ordine, la stessa è tenuta a versare al figlio, a titolo di risarcimento del danno non patrimoniale subìto, 10 mila euro.

Il Tribunale di Roma ha poi inibito la madre di pubblicare contenuti tali da creare disagi al figlio, autorizzando il tutore del minore a diffidare soggetti terzi nell'ipotesi di diffusione di informazioni relative allo stesso, nello specifico condividendo post e foto, potendone ottenere la rimozione dei contenuti.

Trattasi di una sentenza storica che detta un principio di diritto forte a tutela dei minori, nel solco di numerose pronunce che negli ultimi anni hanno costretto i genitori a disattivare i profili Facebook aperti a nome dei figli o a rimuoverne le fotografie pubblicate nelle proprie pagine social.

Tanto che le disposizioni che regolano la gestione pubblica dell'immagine dei minori, da qualche anno, sono entrate anche nelle condizioni dei ricorsi per separazione consensuale e di divorzio per evitare controversie giudiziarie: i genitori, in altre parole, si mettono d'accordo da subito sull'utilizzo delle foto dei figli sui social o come sfondo dei profili Whatsapp, in genere vietandone l'utilizzo e chiedendone l'omologa da parte del tribunale.

[203] Trattasi, in particolare, della sentenza pronunciata dal Tribunale di Mantova, il 19 settembre del 2017, e dell'ordinanza del Tribunale di Roma del 23 dicembre del 2017. Per un approfondimento: www.altalex.com/~/media/altalex/allegati/2018/allegati%20free/tribunale_roma_ordinanza_23_dicembre_2017%20pdf.pdf.

Fondamentale in materia è anche la pronuncia del Tribunale di Mantova del 19 settembre 2017 che ha ordinato alla madre di rimuovere dai social le foto dei figli, statuendo che, il pubblicare *online* foto di bambini, costituisce comportamento potenzialmente pregiudizievole per gli stessi, dal momento che accresce il rischio che queste immagini vengano condivise da un numero indeterminato di persone, conosciute e non, che potrebbero farne un uso poco consono o addirittura illegale.
Anche qui il Giudice ha ordinato la rimozione delle immagini e condannato il genitore al pagamento di una somma di denaro in favore dei figli.
Infine, per essere diretta conseguenza dell'applicazione nel nostro ordinamento giuridico del GDPR, merita di essere segnalata la recentissima sentenza del Tribunale di Rieti del 6-7 marzo del 2019[204] avente anch'essa ad oggetto la necessaria autorizzazione dei genitori per la pubblicazione online delle foto dei figli minori degli anni quattordici.
In particolare, il Primo Giudicante ha osservato che la tutela della vita privata e dell'immagine dei minori rinviene tradizionalmente cittadinanza, nel nostro ordinamento giuridico, nell'art.10 c.c. (concernente la tutela dell'immagine), nel combinato disposto degli artt.4,7,8 e 145 del D.lgs. n.196/2003 (riguardanti la tutela della riservatezza dei dati personali) nonché negli artt.1 e 16, 1 comma, della Convenzione di New York del 20-11-1989, ratificata dall'Italia con legge 27-5-1991 n.176[205].
Su tali basi, riprendendo la distinzione fra i c.d. *petite enfantes* e *grands enfantes* già esistente nel diritto francese, la nuova disciplina comunitaria impone pertanto che il consenso necessario ai fini del trattamento dei dati personali del minore, e dunque anche per le immagini che possano identificarlo, sia prestato dai soggetti esercenti la responsabilità genitoriale, concordemente fra loro e senza arrecare pregiudizio all'onore, al decoro e alla reputazione dell'immagine del minore (art. 97 L. n.633/41).

[204] Per una analisi complessiva della sentenza in esame, www.canestrinilex.com/risorse/vietato-publbicare-foto-di-minorenne-si-social-senza-consenso-di-entrabmi-i-genitori-tr-rieti-2019/.
[205] L'articolo 1 della Convenzione di New York stabilisce che *"Ai sensi della presente Convenzione si intende per fanciullo ogni essere umano avente un'età inferiore a diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile"*. L'art. 16, comma 1, prevede invece che *"Nessun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione"*.

CONCLUSIONI

È indubbio che il Regolamento n. 679/2016 ha rafforzato la tutela dei minori nell'ambito del trattamento dei dati personali stabilendo precise regole in materia di prestazione del consenso.

Tuttavia, l'applicazione dell'art. 8 pone comunque problemi complessi sia con riferimento alla informativa che deve accompagnare la richiesta di consenso, sia riguardo alle modalità che il provider offerente deve adottare per verificare se la persona a cui si rivolge è capace, in autonomia, di esprimere il consenso ovvero risulta necessario invece quello di chi ne ha la responsabilità genitoriale.

Ulteriore tema di discussione riguarda l'eventuale conflitto tra l'età fissata per il consenso al trattamento dei dati e l'età prevista per l'acquisizione della capacità d'agire e, quindi, per l'esercizio dei propri diritti come, ad esempio, il diritto all'immagine.

Potrebbe, infatti, giungersi alla paradossale situazione in cui il minore almeno quattordicenne, pur potendo aprire un proprio account su un social, non potrebbe tuttavia disporre liberamente della propria immagine, diritto quest'ultimo esercitabile dai genitori esercenti la responsabilità fino al compimento del diciottesimo anno di età del figlio[206].

Sul rapporto tra social e minori, poi, parte della Comunità Scientifica è comunque divisa, nel senso che non vi è unanimità in relazione agli effetti distorsivi che l'utilizzo dei social può determinare sui singoli soggetti.

Vi è chi ritiene[207], infatti, che già all'età 13 anni si è capaci di conoscere e analizzare i servizi offerti dalla rete, tenuto sempre conto del fatto che l'uso dei social è comunque fondamentale per la formazione della personalità dei ragazzi nella società digitale.

Ne consegue che abbassare l'età di accesso a questi servizi a 13 anni, come l'art.8 del GDPR consente di fare agli Stati, rappresenterebbe il modo migliore per tutelare il *best interest* dei minori così come la Convenzione sui diritti dell'infanzia e dell'adolescenza richiede[208].

---

[206] D. Bettini in *Minori, protezione dei dati personali alla luce del GDPR, su https://www.altalex.com/documents/news/2018/04/19/minori-protezione-dei-dati-personali-alla-luce-del-gdpr*.

[207] G. Boccia Artieri esamina la questione dal punto di vista sociologico e comportamentale in *op. cit.*

[208] La Convenzione ONU sui Diritti dell'infanzia fu approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989. Tutti i paesi del mondo (ad oggi aderiscono alla Convenzione 194 Stati), ad eccezione degli Stati Uniti, hanno ratificato questa Convenzione. La Convenzione è stata ratificata dall'Italia il 27 maggio 1991 con la legge n. 176. La Convenzione è uno strumento giuridico e un riferimento a ogni sforzo compiuto in cinquant'anni di difesa dei diritti dei bambini e si compone da 54

Vi è poi, come già accennato, un problema di informativa da dare nell'ambito dell'applicazione dell'art.8, atteso che è necessario che il proponente tenga conto in modo adeguato della possibilità o meno per un minore di comprendere ciò di cui lo si informa.

A questo va aggiunto che la richiesta del consenso al trattamento dei dati impone sempre cautele particolari, sia per individuare a chi spetti fornirlo, sia per definire quando e come esso debba essere dato e in che forma.

Nel caso dell'art. 8 del GDPR, il tema è reso ancora più complesso dal fatto che, a seconda dell'età dell'interessato, esso può essere validamente dato da quest'ultimo ovvero da chi ne ha la responsabilità genitoriale.

Spetta quindi al fornitore del servizio adottare le misure necessarie per poter stabilire con ragionevole certezza sia se l'interessato ha o meno una età legislativamente adeguata, sia se la persona che eventualmente esprime il consenso a suo nome eserciti effettivamente la responsabilità genitoriale nei suoi confronti.

In ogni caso, l'art.8 è solidamente ancorato all'esigenza di tutelare il minore da chi si rivolge direttamente a lui per offrire servizi della società dell'informazione che richiedono, per essere legittimamente posti in essere, il suo consenso informato.

La norma, infatti, preserva il minore da chi offre servizi in rete senza curarsi affatto dell'età di colui al quale l'offerta è fatta e della sua capacità di comprenderne le conseguenze sotto il profilo del trattamento dei dati e degli eventuali rischi che ne possono derivare.

L'obiettivo è quello di assicurare al minore dei sedici anni (o dell'età fissata dalla legge nazionale) una tutela rafforzata in ordine ad offerte di servizi delle società dell'informazione a lui direttamente rivolte, quando queste richiedono il suo consenso.

Tutela che consiste, lo si ripete ancora una volta, nel fatto che non basta il consenso prestato dall'interessato ma occorre quello di chi ne ha la potestà genitoriale ove ne ricorrono le condizioni.

Del resto, che l'obiettivo sia la tutela del minore è reso ancora più evidente dal fatto che il già citato Considerando 38 specifica che *"il consenso del titolare della responsabilità genitoriale non deve essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente ai minori"*.

---

articoli. La creazione della Convenzione è ricordata ogni anno, il 20 novembre, con la commemorazione della Giornata internazionale per i diritti dell'infanzia e dell'adolescenza.

Altra parte della dottrina[209] sostiene invece che nonostante gli sforzi profusi a livello comunitario, la disciplina avente ad oggetto la tutela del minore è comunque parziale per non aver fatto cenno, nell'art. 22 del GDPR[210], all'esigenza di tutela dei minori rispetto alle decisioni basate su trattamenti automatizzati come la profilazione, atteso che, secondo il Considerando n. 71, una simile misura *"non dovrebbe riguardare un minore"*[211].

In altre parole, per le decisioni di cui all'art. 22, par. 1, del GDPR, non viene fatto un distinguo tra decisioni automatizzate che riguardino i minori e quelle rivolte, invece, ad un soggetto adulto.

Vi è poi la questione principale che il GDPR porta con sé all'interno dell'ordinamento giuridico italiano e cioè quella relativa alla necessità di innovare il sistema attuale che si presenta inadeguato, proponendo, nella materia della incapacità, una graduazione della stessa.

Trattasi di una questione che nasce perché è stato dimostrato che le capacità cognitive degli adolescenti hanno subìto un notevole sviluppo rispetto al passato, ed i minori oggi sono in grado di comprendere perfettamente le conseguenze e le responsabilità che derivano dai loro comportamenti ovvero dai contratti che gli stessi sottoscrivono[212].

---

[209] R. Panetta, *op. cit.,* p. 114.

[210] L'art.22 del GDPR, intitolato *"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"*, stabilisce che *"**1**. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
***2**. Il paragrafo 1 non si applica nel caso in cui la decisione:*
a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato.
***3.** Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*
***4.** Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato"*.

[211] Per il Considerando n.71 *"L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione». (...) Tale misura non dovrebbe riguardare un minore"*.

[212] L. Cunningham, *A Question of capacity: towards a Comprehensive and Consistent Vision of Children and their Stat Under law*, in *10 U.C. Davis J. Juv. L. e Pol'y* 275, 293 (2006), 278, il quale mette in evidenza come *"in the last century, a rich body of psychological literature was developed*

Occorre quindi chiedersi se i tradizionali limiti di età sono ancora attuali, posto che i minori di sedici ovvero quattordici anni hanno peculiarità e capacità diverse tra loro o addirittura rispetto a coloro che di anni ne hanno molti meno.
Questa è la ragione per la quale sarebbe stato opportuno in ambito comunitario, anziché esaltare il dato che i minori non possono autorizzare il trattamento dei loro dati personali se non sedicenni con la previsione di eventuali deroghe nei vari Paesi, limitarsi a fissare un'età al di sotto della quale il minore si presuppone non capace di discernimento uniformando in tal modo la legislazione degli Stati membri.
In ogni caso, quello della definizione dell'età minima per esprimere il consenso al trattamento dei propri dati è argomento delicatissimo che va letto alla luce della Convenzione sui diritti dell'infanzia e dell'adolescenza, del GDPR nonché del decreto legislativo n.101 del 10 agosto 2018 di adeguamento del quadro regolatorio nazionale.
La scelta della età minima per il consenso invita infatti ad operare bilanciamenti tra libertà di espressione, pensiero, associazione, e partecipazione dei minori alla vita di relazione e alla costruzione della comunità in cui vivono.
Essendo questi diritti esercitati anche in rete, occorre bilanciarli altresì con altri diritti: quello all'informazione ed alla protezione dei dati.

about the rate and process of child development. Lawmakers should draw upon research to create laws that cohesively and logically deal with children's rights and responsibilities".

BIBLIOGRAFIA

Abriani, N. - Cottino, G., *La concorrenza sleale*, in Abriani, N. - Cottino, G. - Ricolfi, M., *Diritto industriale,* in *Tratt. dir. comm.* diretto da G. Cottino, II, Padova, 2001;

Auteri, P., *La concorrenza sleale*, in *Tratt. Rescigno*, P., XVIII, *Impresa e lavoro*, parte IV, Torino, 1982;

Ascarelli, T., *Teoria della concorrenza e dei beni immateriali,* III ed., Milano, 1960;

Balducci, D., *Cessione e conferimento d'azienda*, VIII ed., Milano, 2007;

Boscati, A., *Patto di non concorrenza*, Milano, 2010;

Buonaiuto, A.E., *Clausole accessorie al contratto di lavoro*, Milano, 2012;

Campobasso, G.F., *Diritto commerciale – Diritto dell'impresa,* VI ed., Torino, 2003;

Cendon, P., *La concorrenza*, Torino, 2005;

Cotto, A. - Fornero, L.- Odetto, G., *Cessione, conferimento, affitto e donazione d'azienda*, I ed., Torino, 2007;

Ferrentino, C. - Ferrucci, A., *Dell'azienda*, Milano, 2006;

Floridia, G., *Correttezza e responsabilità dell'impresa*, Milano, 1982;

Genovese, A., *Il risarcimento del danno da illecito concorrenziale*, Napoli, 2005;

Ghidini, G., *La concorrenza sleale*, in *Giur. sist. civ. comm. Bigiavi*, III, Torino, 2001;

Ghidini, G., *Profili evolutivi del diritto industriale. Proprietà intellettuale e concorrenza*, Milano, 2001;

Ghirotti, E., *Il patto di non concorrenza nei rapporti commerciali,* Milano, 2008

Guizzi, G., *Il mercato concorrenziale. Problemi e conflitti. Saggi di diritto antitrust,* Milano, 2010.

Jaeger, P.G., *Valutazione comparativa d'interessi e concorrenza sleale*, in *Riv. dir. ind.*, 1970;
Libertini, M., *L'imprenditore e gli obblighi di contrarre*, in Ghini, M.-Libertini, M. - Putzolu, G., *La concorrenza e i consorzi*, nel *Tratt. dir. comm. Galgano,* IV, Padova, 1981;
Nivarra, L., *L'obbligo a contrarre e il mercato,* Padova, 1990;
Pardolesi, R., *Le regole della concorrenza*, in *Diritto civile*, diretto da N. Lipari e P. Rescigno, coordinato da A. Zoppini, IV, *Attuazione e tutela dei diritti*, Parte I, *La concorrenza e la tutela dell'innovazione*, Milano, 2009;
Ravà, T., *Diritto industriale*, Parte I, II ed., Torino, 1981;
Rigato, C., *Agenti e rappresentanti*, Ravenna, 2014;
Stanzione, P., *Manuale di diritto privato,* III ed., Torino, 2013;
Turco, C., *Diritto civile, I,* Torino, 2014;
Tutolo, M., *Diritto privato*, Milano, 2006;
Vanzetti, A. - Di Cataldo, V., *Manuale di diritto industriale*, IX ed., Milano, 2009;
Villanacci, G., *I contratti della distribuzione commerciale*, Torino, 2010

SINTESI

CAPITOLO 1
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR): I CAMBIAMENTI NEL MONDO DELLA PRIVACY

L'avvento di Internet e dei social network ha trasformato profondamente, non soltanto, il tessuto economico e produttivo, ma anche le relazioni umane e sociali che, sempre più spesso, nascono e si sviluppano online, inducendo a cedere, comunicare e trasmettere porzioni più o meno rilevanti di informazioni al fine di usufruire di servizi o acquistare beni, sia da enti pubblici che da privati[213]. Ciò spiega i motivi per cui in un'epoca, come quella moderna, connotata dalla comunicazione digitale globale, il diritto fondamentale alla protezione dei dati personali ha assunto un ruolo determinante per la difesa della libertà dell'individuo, richiedendo sistemi giuridici di tutela sempre più affinati.

Dunque, avvertite – o forse semplicemente riscoperte – queste nuove esigenze di protezione dell'individuo, il Legislatore europeo è intervenuto con un'opera organica, il "*General Data Protection Regulation"* (da qui in poi semplicemente "GDPR")[214], al fine di garantire che tutti gli Stati membri dell'Unione detenessero un uniforme, ed elevato, livello di protezione delle persone fisiche, i cui dati personali, ora come non mai, vengono commercializzati e scambiati nell'ambito di sistemi di economia digitale, all'interno dei quali sempre più transazioni si fondano sul paradigma offerta di servizio contro dato personale[215]. Abrogando e sostituendo la Direttiva 95/46/CE, la quale per anni ha rappresentato la pietra angolare della legislazione europea in materia di dati personali[216], il GDPR ha introdotto un quadro normativo sostanzialmente identico in tutto il territorio dell'UE, ponendo in questo modo fine alle asimmetrie giuridiche fino a quel momento

[213] F. Modafferi, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, United Kingdom, 2015, p. 28.
[214] Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, il Reg. (UE) n. 2016/679 è entrato in vigore il 24 maggio 2016 ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018. Trattandosi di un Regolamento, non necessita di recepimento da parte degli Stati dell'Unione ed è stato attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.
[215] G. Conti, *La protezione dei dati personali per titolari e responsabili del trattamento*, Santarcangelo della Romagna, Maggioli, 2019, p. 16.
[216] E. Tosi (a cura di), *Privacy Digitale*, Giuffrè, Milano, 2019, p. 59.

prodotte dalle singole legislazioni nazionali frutto del recepimento della "Direttiva Madre" e delle azioni diversificate messe in campo dalle diverse Autorità di controllo[217].
L'avvento del nuovo Regolamento ha definito un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri, con l'obiettivo di uniformare ed armonizzare tale disciplina entro – e non solo – i confini comunitari, eliminando così "barriere" che si erano create nel corso del tempo con normative nazionali frammentarie e diverse tra loro, le quali, non solo, ostacolavano la libera circolazione dei dati tra una Nazione e l'altra ma penalizzavano lo sviluppo di un mercato unico digitale[218]. Muovendosi entro tali confini, infatti, il Parlamento italiano, nel mese del novembre 2017, ha delegato il Governo all'adozione di un decreto di armonizzazione dell'ordinamento nazionale al GDPR al fine di consentire un miglior adattamento della normativa comunitaria alle specifiche peculiarità del sistema giuridico italiano, nonché allo scopo di rispondere all'esigenza di salvaguardare i meccanismi di tutela, predisposti dall'Autorità Garante per la protezione dei dati personali, fino a quel momento vigenti. Il d.lgs. 10 agosto 2018, n. 101 è, quindi, il frutto del lavoro di un'apposita Commissione ministeriale e non apporta modifiche al Regolamento, ma interviene su diverse e cruciali aree che nel prosieguo della trattazione verranno analizzate, seppur con un inevitabile processo semplificativo e di sintesi.
L'insieme normativo, in cui il nuovo Regolamento europeo si articola, si compone di ben 99 articoli, preceduti da 173 "Considerando", i quali chiariscono il contesto e le ragioni della nuova disciplina in materia di protezione dei dati personali[219]. Etichettate come disposizioni generali, le norme di apertura al Regolamento – articoli da 1 a 4 – sono volte ad individuare, e delimitare, l'oggetto, le finalità e l'ambito di applicazione del medesimo.
Per quanto concerne l'*oggetto*, quest'ultimo viene chiaramente ricondotto dall'art. 1 ad una duplice tematica: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei medesimi dati[220].
Con riferimento alle *finalità* del Regolamento, anche quest'ultime possono essere distinte secondo un duplice ordine di idee: 1) elevare la protezione delle persone fisiche con

[217] R. Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2019, p. 7.
[218] A. Ciccia Messina, N. Bernardi, *Privacy e regolamento europeo*, IPSOA, Milano, 2018.
[219] E. Tosi (a cura di), *Privacy Digitale*, Giuffrè, Milano, 2019, p. 59.
[220] E. Belisario, G. M. Riccio, G. Scorza (a cura di), *GDPR e normativa privacy commentario*, IPSOA, 2018, p. 4.

riguardo al trattamento dei dati di carattere personale a un diritto fondamentale[221]; 2) contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica che consenta il progresso economico e sociale, il rafforzamento e la convergenza delle economie nel mercato interno nonché il benessere delle persone fisiche[222].

Venendo *all'ambito di applicazione*, giova evidenziare che il Regolamento europeo si applica esclusivamente alle persone fisiche, così come chiaramente si legge nell'articolo iniziale dell'impianto normativo in oggetto: "*protezione dei diritti e delle libertà fondamentali delle persone fisiche".* Si deduce, dunque, che il GDPR non disciplina il trattamento dei dati personali relativi a persone giuridiche. Riguardo l'ambito di *applicazione materiale*, invece, l'art. 2, comma 1 lo identifica in *"tutti i trattamenti di dati personali che siano interamente o parzialmente automatizzati o, anche, non automatizzati purché siano contenuti in un archivio o destinati a figurarsi."* Infine, la normativa europea apporta diverse novità riguardo *l'ambito territoriale* di applicazione del Regolamento, stabilendo che è sufficiente che *lo stabilimento* del Titolare o del Responsabile del trattamento *si trovi nel territorio UE*, per applicare il GDPR. Nel capo II (artt. 5-11) sono poi enunciati i principi fondamentali su cui si fonda la nuova normativa, rappresentati da: a) liceità, corretta e trasparenza; b) minimizzazione dei dati; c) esattezza; d) limitazione della conservazione; e) integrità e riservatezza; f) responsabilizzazione[223]. Per quanto concerne, in primo luogo, quello di *liceità*, di cui all'art. 6, posta che, per connotarsi giuridicamente come lecito, il trattamento dei dati personali deve fondarsi sul *consenso* dell'interessato o su altra base giuridica prevista come obbligatoria dal Regolamento o dalla normativa europea o da quella statale[224].

---

[221] Lo enuncia espressamente il Considerando 1, ai sensi del quale «La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale.».

[222] Come chiarisce il Considerando 2, il GDPR è «inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.».

[223] È interessante notare come questo aspetto sia sostanzialmente allineato a quanto già previsto dall'art. 11 del Codice Privacy, il quale prevedeva che:
«1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.».

[224] Considerando 40 del GDPR: «Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto

Con particolare riferimento a quello di *correttezza*, invece, il principio richiede che il trattamento dei dati si svolga in maniera leale e onesta. Si tratta, in buona sostanza, di una forma di lealtà e buona fede da osservarsi in tutte le fasi relative al trattamento di dati personali: in tali fasi vanno certamente ricomprese anche quelle decisorie e preparatorie, e non soltanto, quindi, le operazioni di trattamento strettamente intese[225]. Infine, il principio di *trasparenza* dichiara che il trattamento deve avvenire con modalità predefinite e rese note all'interessato che sarà quindi pienamente consapevole, non solo, della tipologia di dati raccolti, ma anche delle modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i suoi dati personali[226].

Il Capo III del Regolamento UE n. 2016/679 si occupa, in seguito, dei "diritti dell'interessato". Il Regolamento consolida il quadro dei diritti e lo amplia, rispetto a quelli già conosciuti nel *Codice Privacy*, con l'introduzione di nuovi, tra i quali: il diritto alla portabilità dei dati e il diritto all'oblio.

Il *diritto all'oblio* conferisce all'interessato il potere di ottenere dal titolare del trattamento la cancellazione dei propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento non sia altrimenti conforme al GDPR[227]. Il *diritto alla portabilità dei dati*, invece, costituisce una delle principali novità in tema dei diritti dell'interessato e, in generale, dell'intero quadro normativo confluito nel Regolamento europeo: permette agli interessati di ricevere i dati personali, forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare.

Infine, la chiave di volta della recente disciplina in materia di protezione dei dati personali è rappresentata, sembra ombra di dubbio, dal principio di *accountability* – anche detto di *responsabilizzazione* – il quale, a ben vedere, riflette la centralità attribuita dal Legislatore

---

dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.».

[225] C. Bistolfi, L. Bolognini, E. Pelino, *Il regolamento privacy europeo,* Giuffrè, Milano, 2016, p. 94-95.

[226] Come evidenzia il Considerando 39: «Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.».

[227] G. Conti, *La protezione dei dati personali per titolari e responsabili del trattamento*, Santarcangelo della Romagna, Maggioli, 2019, p. 99.

europeo, nell'impianto normativo in esame, alla figura del titolare del trattamento ma, soprattutto, alle responsabilità che su quest'ultimo gravano[228].

Il titolare, infatti, è tenuto ad assicurare che il trattamento dei dati personali sia conforme alle disposizioni contenute nel Regolamento, dovendo, inoltre, esserne in grado di provarne il rispetto in qualsiasi momento. Tra gli strumenti che garantiscono l'accountability si annoverano, tra gli altri, la nomina di un Data Protection Officer (di seguito anche brevemente "DPO") e il rispetto degli obblighi di *"privacy-by-design"* e *"privacy-by-default"*, di seguito esposti.

Quella del "Responsabile della protezione dei dati personali", conosciuto anche come "*Data Protection Officer*" o, semplicemente, "*DPO"*, costituisce, nel panorama giuridico nazionale, un'inedita figura soggettiva in quanto non prevista neppure dal previgente "Codice della privacy". Riguardo i requisiti soggettivi, appare chiaro dall'art. 37, comma 5, che il *DPO* debba essere designato *"in funzione delle qualità professionali, in particolare dalla conoscenza specialistica della normativa e della prassi in materia di protezione dei dati"* e con le *capacità di assolvere* i compiti a questo assegnati dallo stesso Regolamento (art. 39 GDPR). Il DPO, inoltre, gode di una sorta di immunità nell'esercizio delle sue funzioni: a dimostrazione di ciò la sua responsabilità, salvo casi di dolo o colpa, non può eccedere il valore del contratto di nomina[229]. Tuttavia, al fine di evitare ogni eventuale conflitto d'interessi e garantire al DPO l'indipendenza richiesta dalla normativa, è proferibile assegnare l'incarico a un professionista esterno alla struttura aziendale[230].

Riguardo i temi di *privacy by design* e *privacy by default,* questi risultano generalmente indicati come due pilastri della costruzione del Regolamento europeo[231].

Nel dettaglio, con l'espressione "*data protection by design*", si intende l'obbligo in capo al titolare, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura e delle finalità del trattamento, di mettere in atto misure tecniche e organizzative adeguate, per integrare nel trattamento le necessarie garanzie volte a tutelare i diritti degli interessati[232]. Mentre *privacy-by-default* significa che la tutela della protezione del dato deve assurgere a impostazione predefinita[233], dovendo il titolare adottare misure

[228] E. Tosi, *op. cit.*, p. 376.
[229] R. Panetta, *op. cit.*, p. 24.
[230] A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, Torino, 2018, p. 107.
[231] A. Ciccia Messina, N. Bernardi, *Privacy e regolamento europeo*, IPSOA, Milano, 2018, p. 85.
[232] M. Soffientini, (a cura di), *Privacy*, IPSOA, Milano, 2018, p. 97.
[233] A. Ciccia Messina, N. Bernardi, *op. cit.*, p. 86.

tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Dunque, attraverso un'applicazione corretta di suddetti principi si vuol garantire che il dato sia protetto fin dalla sua progettazione, ovvero quando questo viene raccolto dal titolare, e che sia garantita la tutela e il rispetto della vita privata per impostazione predefinita[234].

CAPITOLO 2
IL CONSENSO AL TRATTAMENTO E L'INFORMATIVA AGLI INTERESSATI

La definizione del consenso per il trattamento di dati personali è riportata all'art. 4, par. 1, n. 11 del GDPR, il quale reca l'indicazione dei requisiti essenziali di validità: costituisce "*consenso dell'interessato*" qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento[235].

In base a tale disciplina, quindi, il consenso deve essere:

a) *libero*: quando è il risultato di una scelta autonoma dell'interessato; al contrario, secondo il Considerando n. 42, non può definirsi tale quando l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizi.

b) *specifico*: in quanto essere prestato per finalità specifiche al fine di assicurare la trasparenza delle attività di trattamento[236]. Infatti, qualora il trattamento dei dati preveda più operazioni, esso deve esigere una o più richieste di consenso, a seconda che la finalità delle altre operazioni sia la stessa o siano finalità diverse (*consenso modulare*)[237].

---

[234] *Ibidem.*

[235] Sul tema del consenso al trattamento dei dati si veda il recente contributo di I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 67 ss., nonché l'ampio saggio di S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. Dir. priv.*, 2016, 513 ss. ove si ritrovano ampi riferimenti alla dottrina degli ultimi decenni in questa materia.

[236] G. Conti, *op. cit.*, p. 74

[237] R. Panetta, *op. cit.,* p. 130

c) *informato*: si intende che tale consenso deve essere preceduto da valida *informativa*, la cui finalità è di porre l'interessato nelle condizioni di essere pienamente a conoscenza del trattamento dei propri dati personali e dei relativi diritti[238].

d) *inequivocabile*: perché il consenso possa essere ritenuto tale, deve esserci certezza che l'interessato l'abbia effettivamente prestato[239]. La normativa richiede esplicitamente una dichiarazione o un atto positivo con il quale l'interessato esprime il suo assenso al trattamento dei propri dati[240]. L'espressione inequivoca, quindi, esclude il silenzio, l'inattività e la preselezione dei moduli cartacei e online come atti validi alla prestazione del consenso.

e) *espresso*: per qualificarsi come tale, il consenso deve sempre derivare da un atto inequivocabile, anche in forma online o elettronica (ad esempio mediante *flag*), essere acquisito via e-mail o anche con l'upload di un documento scannerizzato recante la sottoscrizione di un documento a firma dell'interessato[241].

f) *esplicito*: l'art. 9 del GDPR stabilisce che *"è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, tranne nel caso in cui l'interessato non abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche."*

In seguito, l'art. 7 del GDPR disciplina le *condizioni del consenso* e prevede che ciascun titolare del trattamento deve distinguere i casi in cui è necessario acquisire il consenso dell'interessato dai casi in cui non sia necessario in quanto presente una diversa base giuridica di trattamento[242]. Il primo comma del suddetto articolo specifica: *«qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali».* Dunque, l'obbligo di basare il trattamento sul consenso, nei casi di legge, incombe esclusivamente sul titolare, in capo al quale sono allocati i poteri decisori sulle finalità e conseguentemente sui mezzi del trattamento.

---

[238] Mondini Rusconi, *Big Data: Privacy, gestione, tutele*, Altalex, Milano, 2018, p. 214.
[239] M. Soffientini, *op. cit.*, p. 156.
[240] Mondini Rusconi, *op. cit*, p. 215.
[241] G. Conti, *op. cit.*, p. 73
[242] M. Soffientini, *op. cit.*, p. 156.

Il paragrafo 2[243] dell'art. 7 enuncia la chiara *indicazione della richiesta di consenso*: ai fini della sua validità, risulta necessario non solo che il consenso sia espresso, ma che sia anche documentato per iscritto[244]. Occorre che la richiesta di consenso sia presentata, quindi, in modo chiaramente distinguibile, comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, assicurando la piena consapevolezza da parte dell'interessato dell'equivalenza del proprio comportamento ad un consenso al trattamento dei dati[245].

Il diritto di revoca è sancito, poi, dal paragrafo 3[246] della disposizione in esame, la quale stabilisce il diritto dell'interessato di revocare il proprio consenso, precedentemente prestato, in qualsiasi momento. Il titolare del trattamento è tenuto, quindi, ad informare l'interessato al momento in cui sta per raccogliere il consenso della possibilità di revocarlo[247]. L'interessato può revocare il proprio consenso senza incontrare alcun limite e, soprattutto, senza dover indicare i motivi della sua ritrattazione, ancorando quest'ultima alla sussistenza di una giusta causa[248].

Infine, il punto 4 dell'art. 7 recita *«nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».* Se il consenso, quindi, ha ad oggetto un trattamento di dati non necessario – in quanto non strettamente funzionale – alla prestazione del servizio[249], è ragionevolmente plausibile che tale consenso non sia stato prestato liberamente, ma "forzato" da parte del titolare pena l'esclusione del servizio. Dunque, sulla base di un consenso viziato, i dati così acquisiti non devono ritenersi utilizzabili essendo il trattamento considerato illegittimo.

---

[243] Art. 7 "Condizioni per il consenso", paragrafo 2: *«Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante».*

[244] A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale,* in *Quaderni de "Il Foro napoletano", 33*, Edizioni Scientifiche Italiane, 2019, p. 67.

[245] A. Vivarelli, *op. cit.*, p. 69.

[246] Art. 7 "Condizioni per il consenso", paragrafo 3: *«L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato».*

[247] R. Panetta, *op. cit.*, p. 132.

[248] A. Vivarelli, *op. cit.*, p. 77.

[249] E. Tosi, *op. cit.,* p. 73.

Il problema del libero consenso, inoltre, si fa ancor più delicato in relazione ad uno dei trattamenti più insidiosi: quello della *profilazione*[250].

Ai sensi dell'art. 4 del GDPR, la profilazione consiste in quell'insieme di attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento o in determinate categorie omogenee (*cluster*). Dal punto di vista commerciale, la profilazione permette di inviare pubblicità mirata e fornire servizi personalizzati al fine di rispondere esattamente ai desideri di ciascun consumatore. È necessario, quindi, che il titolare indichi analiticamente nel documento contenente l'informativa in che cosa si articola l'attività di profilazione, nonché esponga in maniera chiara e comprensibile le conseguenze delle stesse[251].

Pertanto, qualora il titolare del trattamento intenda svolgere attività di marketing o di profilazione è necessario che la manifestazione del consenso sia, anche graficamente, separata dal consenso principale al fine di permettere all'interessato di esprimere consapevolmente e liberamente le proprie scelte[252].

A tal proposito, il titolare che voglia operare con i dati personali è tenuto ad informare l'interessato sul trattamento che intende effettuare, rendendolo edotto dei diritti che lo stesso può esercitare[253]. È necessario che all'interessato sia resa un'*informativa* sull'esistenza del trattamento e delle sue finalità.

L'informativa è dovuta per qualsiasi trattamento e dunque a prescindere che esso sia fondato sul consenso o su altra condizione di liceità[254].

A seconda di come vengono raccolti i dati, sono ravvisabili tre tipologie di informativa:

1) *informativa diretta*: se i dati vengono raccolti presso l'interessato, l'informativa dovrà essere resa al momento della raccolta dei dati personali (art. 13);

2) *informativa successiva*: se i dati sono raccolti presso altre fonti, l'informativa dovrà essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta dei dati (art. 14);

3) *informativa ulteriore*: necessaria nel caso in cui il Titolare modifichi le finalità originarie del trattamento. In tal caso, il documento a completamento dell'informativa originario deve essere consegnato prima dell'inizio del nuovo trattamento che altrimenti

[250] E. Tosi, *op. cit.*, p. 75.
[251] G. Conti, *op. cit.*, p. 108.
[252] *Ibidem*.
[253] Mondini Rusconi, *op. cit*., p. 210.
[254] C. Bistolfi, L. Bolognini, E. Pelino, *op. cit.*, p. 185

sarebbe sfornito della base giuridica corretta per garantirne la liceità[255]. L'obbligo incombe esclusivamente sul titolare, che può delegare alle attività esecutive il responsabile del trattamento e il personale dipendente.

Il contenuto minimo dell'informativa, in parte più esteso rispetto a quello previsto nel Codice[256], è ora tassativamente elencato all'art. 13 del GDPR, nel caso in cui i dati siano raccolti presso l'interessato (direttamente), e all'art. 14, nel caso in cui i dati siano raccolti presso terzi (indirettamente)[257].

Per quanto concerne la forma dell'informativa, questa va resa in linea di principio in forma scritta e preferibilmente in formato elettronico; in alternativa, oralmente, soltanto su richiesta dell'interessato e purché sia comprovata la sua identità (art. 12, par. 1). Il linguaggio deve essere semplice e chiaro e, se l'informativa è scritta, il testo deve essere ben strutturato e comprensibile in tutti i suoi passaggi[258].

Infine, in caso di violazione della disciplina in tema di informativa (art. 13 e 14), la normativa prevede l'irrogazione di una sanzione amministrativa pecuniaria fino a 20.000.000€ (venti milioni), o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

CAPITOLO 3
LA TUTELA DEI MINORI

Il quadro normativo della tutela dei minori sui media, per quanto articolato, non sembra mai sufficiente a proteggere in modo efficace i bambini durante le loro attività in rete. Pertanto, oggi assume una rilevanza strategica la tutela dei minori nell'utilizzo dei servizi della società dell'informazione al fine di evitare le conseguenze negative di tali attività durante la navigazione online.

---

[255] Per approfondimenti sulla questione si veda A. Pisapia, *op. cit.*, p. 62

[256] Art. 13 del GDPR: *«L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:*
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile».

[257] R. Panetta, *op. cit.*, p. 123.

[258] R. Panetta, *op. cit.*, p. 131.

Con l'avvento del Regolamento Europeo n. 679/2016, entrato in vigore il 25 maggio 2018, il quale non necessita di trasposizione nelle legislazioni nazionali in quanto di immediata applicazione[259], si ricava come la tutela della privacy, con riguardo al minore, vada intesa non solo come minimizzazione dei dati a lui relativi (art. 5, par. 1, GDPR)[260], ma anche e soprattutto nell'ottica del consenso informato attraverso la necessità di trasparenza delle informazioni che deve avvenire *"mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano"*[261].

La normativa europea precedente al GDPR, invece, non prevedeva un limite espresso ma solo indiretto e ricavabile dal quadro normativo generale.

In Italia, ad esempio, la capacità di agire, e cioè la capacità del soggetto a compiere atti che incidono nella propria sfera giuridica, si acquista con la maggiore età, quindi a 18 anni, per espressa previsione dell'art. 2 del Codice Civile[262].

Quanto invece al cd. Codice della Privacy, posto in essere nel nostro ordinamento giuridico con D.lgs. n.196/2003, nulla è indicato in via generale circa i requisiti di capacità per la prestazione del consenso privacy e quindi sulla idoneità del minore a prestarlo, in quanto l'unica norma che richiamava la capacità di agire di chi presta il consenso, l'articolo 24, è stata abrogata dal decreto legislativo n.101/2018, riferendosi tra l'altro a situazioni speciali, o secondo un'altra interpretazione, eccezionali e quindi

---

[259] Per un approfondimento sul Regolamento Privacy GDPR (*General Data Protection Regulation*) n.679/2016,*"La tutela dei dati personali dei minori"* di G. CAPILLI, cap.XII.

[260] L'articolo 5, par.1, lett.c, del GDPR stabilisce che *"1. I dati personali sono: (...) lett.c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)*.

[261] Il testo completo del Considerando n. 32 GDPR stabilisce che *"Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".*

[262] A. Scarpa, *Legislazioni e Giurisprudenza per gli interessi del minore (Le riflessioni della dottrina sulla capacità di agire*, in *Dir.giur*., 1992, pag.41, ritiene l'art.2 del codice civile una norma generica anziché generale *"idonea ad avallare criteri operativi che funzionano da passprtout" e conclude ritenendo preferibile il metodo relativistico".*

non applicabili analogicamente[263]. In assenza di una norma generale espressa, nell'ordinamento italiano si era fatta quindi strada la tesi che il minore potesse autorizzare il trattamento dei dati, salvo l'accertamento della sua capacità naturale e cioè della capacità di intendere e di volere.

Il nuovo Regolamento europeo ha quindi previsto, come adesso vedremo mediante l'articolo 8, una regolamentazione specifica che però non tocca la capacità di agire del minore che resta disciplinata dall'ordinamento civile nazionale.

Dunque, la norma di cui all'art. 8 del Regolamento Europeo n.679/2016, non riguarda genericamente tutti i trattamenti di dati di minori, ma per la sua applicabilità richiede l'esistenza di due requisiti:

3) che vi sia un'offerta diretta di servizi della società dell'informazione a soggetti minori di 16 anni, dove per *"servizio della società dell'informazione"* si rinvia all'art. 1, par. 1, lett. b) della Direttiva UE 2015/1535 del 09 settembre 2015 e si intende *"qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi"*;
4) che il trattamento dei dati dei minori sia basato sul consenso[264].

Se, invece, il trattamento ha altra base giuridica, come ad esempio il rispetto di un obbligo di legge ovvero di legittimi interessi, la norma di cui all'art. 8 non si applica.

In presenza di questi due requisiti, l'articolo 8 stabilisce il divieto di offerta diretta di servizi digitali ai minori di 16 anni, a meno che non sia raccolto il consenso dei genitori, accertando che il consenso sia dato dall'esercente la responsabilità genitoriale.

Con riferimento ai *"servizi compositi"*[265], quando un servizio della società dell'informazione costituisce una parte integrante di un servizio generale la cui componente principale non è un servizio della società dell'informazione, lo stesso non rientra nella specificazione. Viceversa, qualora il servizio presenti due componenti economicamente indipendenti, una delle quali è la componente online e l'altra è la consegna fisica o la distribuzione di merci, la prima rientra nella definizione di servizio della società dell'informazione, mentre la seconda no.

---

[263] S. Patti, *Consenso, sub art. 23*, in Aa.Vv. *La protezione dei dati personali.* Commentario a cura di C. M. BIANCA E F. D. BUSNELLI, Padova (Cedam), 2007, p. 544 ss.

[264] R. Panetta, *op. cit.,* p. 112.

[265] Con riferimento ai servizi compositi, una attenta analisi viene realizzata dall'Avvocato S. Coppola del foro di Matera in */www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-e-minori-gestire-consenso-e-privacy-sui-social-che-ce-da-sapere/.*

Inoltre, come previsto dall'art. 8 del GDPR, tale limite può essere ulteriormente abbassato dagli Stati nazionali ma non può mai scendere al di sotto dei 13 anni.

È fondamentale specificare che la norma di cui all'art. 8 del Regolamento Europeo n. 679/2016 riguarda soltanto la legittimità del consenso al trattamento dei dati personali, ma non incide sulla validità del contratto sottostante, il cui regime giuridico rimane disciplinato dalla legislazione nazionale o da quella del foro competente a decidere eventuali controversie relative al servizio[266].

A questo scopo, e solo per questo, fissa in sedici anni l'età necessaria affinché tale consenso sia valido ai fini della legittimità dei trattamenti, salvo appunto diversa decisione nazionale. Infine, ai sensi dell'art. 83, par. 4, lett. a) e par. 5 del GDPR, nell'ipotesi di violazione delle norme sul consenso del minore si prevede che la sanzione amministrativa pecuniaria può giungere fino a 10 milioni per il titolare o per le imprese (se superiore) fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente. O ancora, ai sensi del paragrafo 5 dell'art. 83, la sanzione può ammontare fino a 20 milioni di euro o per le imprese (se superiore) fino al 4% del fatturato totale annuo dell'esercizio precedente.

La giurisprudenza nazionale ha avuto modo di esprimersi in più occasioni in materia di tutela dei minori nel caso di trattamento dei loro dati personali.

Prima del Decreto Legislativo n.101/2018, l'orientamento dei tribunali italiani[267] è stato conforme nel ritenere come l'inserimento di foto di minori sui social network rappresenta comportamento potenzialmente pregiudizievole per determinare la diffusione di immagini ad un numero indeterminato di persone.

Particolarmente interessante in materia è la pronuncia del Tribunale di Roma, Sez. I Civ., del 23 dicembre 2017, che non solo ha condannato la madre ad eliminare da Facebook tutte le foto del figlio sedicenne ma ha altresì statuito che, in caso di mancato rispetto dell'ordine, la stessa è tenuta a versare al figlio, a titolo di risarcimento del danno non patrimoniale subìto, 10 mila euro.

---

[266] In particolare, il recente parere del Working Party art.29, *"Guidelines on consent under Regulation 2016/679"*, pubblicato in via definitiva il 10 aprile 2018 (Opinion n. 259), è chiarissimo nel precisare che il consenso di cui all'art.8 non riguarda la validità di eventuali contratti che sia necessario stipulare fra provider e user ai fini della fornitura del servizio. Il regime giuridico dei contratti resta sempre disciplinato dalla legislazione nazionale o da quella del foro competente a decidere eventuali controversie relative al servizio.

[267] Trattasi, in particolare, della sentenza pronunciata dal Tribunale di Mantova, il 19 settembre del 2017, e dell'ordinanza del Tribunale di Roma del 23 dicembre del 2017. Per un approfondimento: www.altalex.com/~/media/altalex/allegati/2018/allegati%20free/tribunale_roma_ordinanza_23_dicembre_2017%20pdf.pdf.

Il Tribunale di Roma ha poi inibito la madre di pubblicare contenuti tali da creare disagi al figlio, autorizzando il tutore del minore a diffidare soggetti terzi nell'ipotesi di diffusione di informazioni relative allo stesso, nello specifico condividendo post e foto, potendone ottenere la rimozione dei contenuti.

Fondamentale in materia è anche la pronuncia del Tribunale di Mantova del 19 settembre 2017 che ha ordinato alla madre di rimuovere dai social le foto dei figli, statuendo che, il pubblicare *online* foto di bambini, costituisce comportamento potenzialmente pregiudizievole per gli stessi, dal momento che accresce il rischio che queste immagini vengano condivise da un numero indeterminato di persone, conosciute e non, che potrebbero farne un uso poco consono o addirittura illegale.

Anche qui il Giudice ha ordinato la rimozione delle immagini e condannato il genitore al pagamento di una somma di denaro in favore dei figli.

Infine, per essere diretta conseguenza dell'applicazione nel nostro ordinamento giuridico del GDPR, merita di essere segnalata la recentissima sentenza del Tribunale di Rieti del 6-7 marzo del 2019[268] avente anch'essa ad oggetto la necessaria autorizzazione dei genitori per la pubblicazione online delle foto dei figli minori degli anni quattordici.

Dunque, è indubbio che il Regolamento n. 679/2016 ha rafforzato la tutela dei minori nell'ambito del trattamento dei dati personali stabilendo precise regole in materia di prestazione del consenso. Tuttavia, l'applicazione dell'art. 8 pone comunque problemi complessi sia con riferimento alla informativa che deve accompagnare la richiesta di consenso, sia riguardo alle modalità che il provider offerente deve adottare per verificare se la persona a cui si rivolge è capace, in autonomia, di esprimere il consenso ovvero risulta necessario invece quello di chi ne ha la responsabilità genitoriale.

Ulteriore tema di discussione riguarda l'eventuale conflitto tra l'età fissata per il consenso al trattamento dei dati e l'età prevista per l'acquisizione della capacità d'agire e, quindi, per l'esercizio dei propri diritti come, ad esempio, il diritto all'immagine.

Vi è poi, come già accennato, un problema di informativa da dare nell'ambito dell'applicazione dell'art.8, atteso che è necessario che il proponente tenga conto in modo adeguato della possibilità o meno per un minore di comprendere ciò di cui lo si informa. A questo va aggiunto che la richiesta del consenso al trattamento dei dati

[268] Per una analisi complessiva della sentenza in esame, www.canestrinilex.com/risorse/vietato-publbicare-foto-di-minorenne-si-social-senza-consenso-di-entrabmi-i-genitori-tr-rieti-2019/.

impone sempre cautele particolari, sia per individuare a chi spetti fornirlo, sia per definire quando e come esso debba essere dato e in che forma.
Nel caso dell'art. 8 del GDPR, il tema è reso ancora più complesso dal fatto che, a seconda dell'età dell'interessato, esso può essere validamente dato da quest'ultimo ovvero da chi ne ha la responsabilità genitoriale.
Spetta quindi al fornitore del servizio adottare le misure necessarie per poter stabilire con ragionevole certezza sia se l'interessato ha o meno una età legislativamente adeguata, sia se la persona che eventualmente esprime il consenso a suo nome eserciti effettivamente la responsabilità genitoriale nei suoi confronti.
Vi è poi la questione principale che il GDPR porta con sé all'interno dell'ordinamento giuridico italiano e cioè quella relativa alla necessità di innovare il sistema attuale che si presenta inadeguato, proponendo, nella materia della incapacità, una graduazione della stessa. Trattasi di una questione che nasce perché è stato dimostrato che le capacità cognitive degli adolescenti hanno subìto un notevole sviluppo rispetto al passato, ed i minori oggi sono in grado di comprendere perfettamente le conseguenze e le responsabilità che derivano dai loro comportamenti ovvero dai contratti che gli stessi sottoscrivono[269]. Occorre quindi chiedersi se i tradizionali limiti di età sono ancora attuali, posto che i minori di sedici ovvero quattordici anni hanno peculiarità e capacità diverse tra loro o addirittura rispetto a coloro che di anni ne hanno molti meno. Questa è la ragione per la quale sarebbe stato opportuno in ambito comunitario, anziché esaltare il dato che i minori non possono autorizzare il trattamento dei loro dati personali se non sedicenni con la previsione di eventuali deroghe nei vari Paesi, limitarsi a fissare un'età al di sotto della quale il minore si presuppone non capace di discernimento uniformando in tal modo la legislazione degli Stati membri.
In ogni caso, quello della definizione dell'età minima per esprimere il consenso al trattamento dei propri dati è argomento delicatissimo che va letto alla luce della Convenzione sui diritti dell'infanzia e dell'adolescenza, del GDPR nonché del decreto legislativo n. 101 del 10 agosto 2018 di adeguamento del quadro regolatorio nazionale.

[269] L. Cunningham, *A Question of capacity: towards a Comprehensive and Consistent Vision of Children and their Stat Under law*, in *10 U.C. Davis J. Juv. L. e Pol'y* 275, 293 (2006), 278, il quale mette in evidenza come *"in the last century, a rich body of psychological literature was developed about the rate and process of child development. Lawmakers should draw upon research to create laws that cohesively and logically deal with children's rights and responsibilities".*

La scelta della età minima per il consenso invita infatti ad operare bilanciamenti tra libertà di espressione, pensiero, associazione, e partecipazione dei minori alla vita di relazione e alla costruzione della comunità in cui vivono.
Essendo questi diritti esercitati anche in rete, occorre bilanciarli altresì con altri diritti: quello all'informazione ed alla protezione dei dati.