

CIRCOLARE N. 5-2020

“Minori e tutela della privacy con il Gdpr”

1. LO STATUTO SPECIALE DELLA PRIVACY MINORILE

1. PRINCIPI GENERALI

4. IL RUOLO DEI GARANTI

5. IL RUOLO DEI TITOLARI/RESPONSABILI DEL TRATTAMENTO: CODICI DI CONDOTTA

6. TRASPARENZA

7. OBLIO

8. DECISIONI AUTOMATIZZATE

9. RESPONSABILE DELLA PROTEZIONE DEI DATI

10. SICUREZZA

11. LEGITTIMO INTERESSE

12. MARKETING

13. SERVIZI DI PREVENZIONE E CONSULENZA DEDICATI A MINORI

14. CONSENSO DIGITALE



Tutti i diritti riservati - Il documento è tutelato dalle norme sul diritto d'autore. Il suo utilizzo, come quello di tutte le altre [Circolari di Federprivacy](#) è riservato ai soci iscritti all'associazione. La traduzione, l'adattamento totale o parziale, la riproduzione, redistribuzione e/o diffusione con qualsiasi mezzo non sono consentite, salvo espressa autorizzazione da chiedere scrivendo a press@federprivacy.org



1. LO STATUTO SPECIALE DELLA PRIVACY MINORILE

Il Gdpr detta uno statuto speciale del diritto dei minori alla privacy e alla protezione dei dati. Si tratta di un gruppo di norme, che compongono un corpo definito e specifico.

È corretto, pertanto, distinguere la disciplina della privacy e protezione dei dati per gli adulti dalla diversa e autonoma disciplina della privacy e protezione dei dati per i minori.

Vediamo, in questa circolare, come si struttura nel Gdpr la disciplina della privacy minorile.

Si premette, peraltro, che lo statuto speciale del diritto della privacy minorile si muove nel quadro di un "*rischio accettato*" dall'ordinamento.

Il legislatore si dimostra consapevole dei rischi, cui va incontro il soggetto vulnerabile in ragione dell'età, ma, anziché eliminare la fonte del rischio, opta per ritenere lecito il trattamento dei dati dei minori, apponendo una serie di condizioni e precauzioni.

Avendo a mente la ratio delle norme, la presente circolare compie alcune scelte interpretative nell'ottica della minimizzazione del rischio a carico dei minori d'età e di massimizzazione del grado di protezione degli stessi.

2. PRINCIPI GENERALI

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.

Ciò vale qualunque sia la base giuridica del trattamento ed ovviamente anche nel caso in cui occorra il consenso del rappresentante legale.

Nei termini appena sinteticamente riportati, si esprime il Considerando 38 al Gdpr, che può essere illustrato analiticamente nei seguenti punti:

- ➔ Il considerando 38 si rivolge a una determinata categoria di interessati
- ➔ La categoria è individuata su base anagrafica
- ➔ A tale base anagrafica viene abbinata la valutazione di maggiore squilibrio rispetto al titolare/responsabile del trattamento
- ➔ La valutazione dello squilibrio poggia su una considerazione di immaturità del minore rispetto alla autodeterminazione nei rapporti giuridici
- ➔ L'immaturità viene descritta come deficit intellettuale, che conduce necessariamente ad un deficit volitivo
- ➔ Il deficit intellettuale è descritto quale insufficiente consapevolezza
- ➔ La diminuita capacità di intendere ha per oggetto i rischi del trattamento, le conseguenze del trattamento e le misure di salvaguardia nonché i diritti in relazione al trattamento dei dati personali
- ➔ Il minore, dunque, rischia di non rendersi conto della possibilità che, nel corso o a causa di un trattamento, vengano messi a repentaglio la riservatezza, l'integrità e la disponibilità del dato a lui riferibile
- ➔ Il minore, inoltre, rischia di non rendersi conto della possibilità che, nel corso o a causa di un trattamento, egli possa subire un danno materiale o immateriale



- Il minore, inoltre, potrebbe non conoscere gli accorgimenti pratici per contrastare rischi e danni
- Il minore, inoltre, potrebbe non conoscere i rimedi giuridici per prevenire i rischi e ottenere un ristoro dei danni subiti
- Il considerando 38 descrive la categoria dei minori al fine di individuare gli stessi quali destinatari di norme speciali
- Il considerando 38 dettaglia la ratio delle norme speciali nella "*specifica protezione*"
- Per quanto sopra, la specifica protezione deve compensare la insufficiente consapevolezza e, pertanto, deve contenere azioni positive per emancipare il minore dalla condizione di squilibrio
- A monte e a valle di quanto sopra dedotto vi è la realistica constatazione che non è praticabile la prescrizione del divieto di assoluto di trattamento di dati dei minori di età. Peraltro, l'ordinamento prevede specifici divieti di trattamento dei dati dei minori
- A monte e a valle di quanto sopra dedotto vi è la realistica constatazione che non sarebbe praticabile, né socialmente accettata, una scelta normativa per cui sia sempre necessario l'intervento del rappresentante legale in relazione ai trattamenti dei dati dei minori di età. In tal caso, l'intervento di un adulto (ad esempio, per esprimere il consenso in nome e per conto del minore) sarebbe di per sé giuridicamente risolutivo. Peraltro, l'ordinamento prevede specifici casi in cui il trattamento dei dati dei minori deve essere autorizzato dal consenso del rappresentante legale (si veda la soglia anagrafica per i trattamenti di dati connessi alla fruizione di servizi della società dell'informazione)
- A monte e a valle di quanto sopra dedotto vi è la realistica constatazione che direttamente ai minori si rivolgono alcuni titolari di trattamento ed, in particolare, i fornitori di servizi della società dell'informazione
- In relazione a ciò, la scelta del Gdpr è di parzialmente emancipare i minori rispetto ai trattamenti dei loro dati
- Il Gdpr ha scelto di delimitare il campo di azione della rappresentanza legale dei minori, emancipando questi ultimi, in un determinato, seppure amplissimo, ambito (servizi della società dell'informazione), a esprimere l'accordo all'utilizzo dei propri dati (lasciando, però, alle legislazioni nazionali la materia delle condizioni soggettive necessarie a esprimere l'accordo "*contrattuale*")
- Tutte le disposizioni del Gdpr, che si preoccupano della tutela dei minori (rispetto alla trasparenza, rispetto al consenso, agli standard di sicurezza e così via), presuppongono un rapporto diretto tra minore e titolare/responsabile
- Tutte le disposizioni del Gdpr, che si preoccupano della tutela dei minori (rispetto alla trasparenza, rispetto al consenso, agli standard di sicurezza e così via), sono altrettante disposizioni che implicitamente riconoscono che il Gdpr ha ampliato la capacità di agire del minore
- Urge una disciplina specifica di questa ampliata capacità di agire del minore, anche con riferimento alle situazioni di possibile conflitto tra il minore e il rappresentante legale in relazione a vicende, nelle quali il minore pretende di autodeterminarsi anche contro gli intendimenti del suo rappresentante legale (quest'ultimo sempre assoggettato all'obbligo di cura, istruzione ed educazione del minore)



A conferma di quanto dedotto in relazione al Considerando 38, si deve aggiungere che, ai fini dell'inquadramento generale del tema, si deve tenere conto altresì della definizione dei minori quali " *soggetti vulnerabili*".

Ad esempio nelle "[Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del Regolamento \(UE\) 2016/679](#)", adottate dal WP29 il 4 aprile – 4 ottobre 2017, si legge che " *i minori possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati...*". Anche in tale contesto, le autorità riconoscono, dunque, che il minore, in quanto tale, difetta delle capacità naturalistiche per curare e difendere i propri interessi.

Questo, peraltro, porta nuovamente non alla esclusione normativa della capacità di autodeterminazione da parte del minore, ma ad una definizione delle condizioni di trattamento dei dati dei minori, emancipati, per certi effetti ed in certi ambiti (servizi della società dell'informazione), ad esprimere il consenso, quale base giuridica del trattamento del dato.

3. IL RUOLO DEI GARANTI

La insufficiente capacità di intendere del minore di età, che pure nell'ambito dei servizi della società dell'informazione è legittimato a un rapporto diretto con il titolare/responsabile del trattamento, deve essere compensata con speciali disposizioni.

L'elaborazione dello statuto speciale "*privacy e protezione dati*" del minore vede protagoniste, innanzi tutto, le autorità di controllo (i garanti), alle quali l'articolo 57, lett. b, Gdpr affida, tra gli altri, il seguente compito:

"b) promuovere la consapevolezza e favorire la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;".

Alle singole autorità di controllo è assegnato il potere-dovere di dare seguito concretamente a questo incarico, che rappresenta una delle priorità nella costruzione del Gdpr.

5. IL RUOLO DEI TITOLARI/RESPONSABILI DEL TRATTAMENTO: CODICI DI CONDOTTA

L'esigenza di specificità della disciplina della privacy e della protezione dei dati dei minori è trasversale ed è prescritta anche nelle norme sulle fonti di autoregolamentazione, tra le quali spiccano per importanza i codici di condotta.

In materia, l'articolo 40 Gdpr descrive l'obiettivo di tali codici, ovvero precisare l'applicazione del regolamento, ed esemplifica l'ambito dei temi suscettibili di precisazione.

Tra questi si esemplifica alla lettera g): "*l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;*".

I codici di condotta possono, dunque, avere disposizioni dedicate ai seguenti temi:

- 1) informazione al minore;
- 2) protezione del minore;
- 3) modalità di acquisizione del consenso del rappresentante ex lege del minore.



A questo proposito si evidenzia che:

- a) l'informazione è una attività ispirata al fine di compensare il deficit intellettuale del minore;
- b) l'informazione deve essere svolta con metodo educativo, e cioè facendo acquisire la competenza a capire;
- c) la protezione del minore implica l'acquisizione di una posizione di garanzia da parte del titolare/responsabile, con la conseguenza che le modalità di protezione devono essere individuate come singole e precise condotte e non come generiche finalità;
- d) le condotte, che realizzano la protezione del minore, concernono qualsiasi aspetto della disciplina della privacy e della protezione dei dati. Nel codice di condotta potranno trovare posto norme relative alle condizioni di liceità, all'esercizio dei diritti, alle precauzioni relative alla sicurezza e così via;
- e) a proposito delle condizioni di liceità, il codice di condotta può scrivere specifiche modalità della prestazione del consenso da parte del rappresentante legale del minore.

6. TRASPARENZA

Interventi delle Autorità di controllo e Codici di condotta rappresentano rinvii del Gdpr ad atti di futura adozione, i quali determineranno i loro effetti una volta adottati.

Ci sono, peraltro, disposizioni di natura precettiva, la cui operatività è immediata.

Tra queste si rilevano le norme sulla trasparenza.

Ai sensi del Considerando 58 Gdpr *"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."*

Il citato Considerando informa l'articolo 12 Gdpr, nella parte in cui prescrive al titolare del trattamento di adottare *"misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 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"*.

Le prescrizioni, anche per il vero un po' ridondanti, riguardano sia la forma sia il linguaggio di:

- a) atti di informazione (cosiddette *"informative"*)
- b) comunicazioni in risposta alla richiesta di esercizio dei diritti
- c) comunicazioni della violazione dei dati (data breach).

Per il rispetto della trasparenza, quanto alla forma, si prescrivono: concisione, trasparenza (la ripetizione è nella disposizione stessa), intelligibilità, facile accessibilità.

Per il rispetto della trasparenza, quanto al linguaggio, si prescrivono: semplicità e chiarezza.

L'articolo 12 si impunta e pretende una particolare osservanza di questi requisiti *"in particolare nel caso di informazioni destinate specificamente ai minori"*.

Peraltro, la disposizione deve essere letta sistematicamente con tutto l'impianto del GDPR, nel quale non si rinviengono norme che autorizzino il minore ad esercitare direttamente i diritti attribuiti all'interessato.

Da ciò consegue che i diritti dei minori sono sempre esercitati dai rappresentanti legali, anche con riferimento ai trattamenti dei dati nel corso di fornitura di servizi da parte di soggetti erogatori di servizi della società dell'informazione.



Ne consegue, altresì, che in ipotesi di data breach il titolare del trattamento deve dare comunicazione al rappresentante legale, anche nel caso di violazione dati in occasione di trattamenti dei dati nel corso di fornitura di servizi da parte di soggetti erogatori di servizi della società dell'informazione.

Ne consegue, infine, che certamente il minore può essere destinatario diretto delle informazioni di cui all'articolo 13 e 14, ma che ciò ha un senso con riferimento alle situazioni in cui la condizione di liceità sia il consenso del minore ai sensi dell'articolo 8 Gdpr. In tutti gli altri casi, l'atto di informazione deve essere rivolto al rappresentante legale del minore.

Per il dettaglio delle prescrizioni relative a forma e linguaggio delle informazioni e delle comunicazioni, si rinvia alle "[Linee guida sulla trasparenza ai sensi del regolamento 2016/679](#)", adottate dal WP29 il 29 novembre 2017-11 aprile 2018.

7. OBLIO

Un'altra disposizione di natura precettiva, la cui operatività è immediata, concerne il diritto alla cancellazione dei dati.

A proposito di tale diritto, il Considerando n. 65 al Gdpr, si sofferma sull'oblio determinato da revoca del consenso e spiega che *"tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet"*.

Si prescinde dal dare valutazioni di politica legislativa ed a maggior ragione etiche, ma è oggettivo constatare che il legislatore europeo mostra qui di preoccuparsi del caso in cui:

- a)** un minore abbia acconsentito al trattamento dei suoi dati (in relazione all'offerta diretta di servizi della società dell'informazione)
- b)** il minore, divenuto maggiorenne, abbia ripensamenti.

A riguardo di tale vicenda, il legislatore invita a una considerazione prioritaria e senza ostruzionismi dell'esercizio del diritto alla cancellazione.

Beninteso, non si tratta di situazioni in cui il consenso del minore sia stato indebitamente acquisito; al contrario, la norma sul diritto all'oblio (nella parte relativa alla revoca del consenso) presuppone un valido consenso.

Insomma, quel che è implicitamente ammesso dal Considerando 65 è che il consenso del minore sia nella sua essenza, ontologicamente, qualcosa di più debole del consenso espresso da un adulto, tanto che all'ormai maggiorenne si deve garantire uno scivolo rispetto all'oblio. Sulla base di queste considerazioni, una buona prassi, che potrebbe diventare anche una norma dei codici di condotta, è la richiesta di conferma del consenso, da rivolgere da parte dei titolari di trattamento all'interessato, in occasione del compimento della maggiore età dell'interessato medesimo.

Un'altra opzione, sostanzialmente equivalente, potrebbe essere la predeterminazione della data del compimento della maggiore età dell'interessato quale termine del trattamento.

8. DECISIONI AUTOMATIZZATE

Un'altra disposizione di natura precettiva, la cui operatività è immediata, concerne la disciplina delle decisioni interamente automatizzate. A proposito di tale istituto il Considerando n. 71 al Gdpr afferma che: *"Tale misura non dovrebbe riguardare un minore"*.



L'uso del verbo al modo condizionale denota tutta l'ambiguità del legislatore europeo, da cui derivano le altrettanto ambigue argomentazioni leggibili nelle "[Linee guida in materia di processi decisionali automatizzati e profilazione definite in base alle previsioni del Regolamento \(UE\) 2016/679](#)", adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017-6 febbraio 2018, nelle quali, a proposito dei trattamenti che coinvolgono minori, si trovano i seguenti argomenti decisamente complicati da tradurre in buone prassi:

- a) le decisioni interamente automatizzate con effetti giuridici non sono vietate in assoluto (ma non si rinviene un catalogo delle ipotesi in cui tali decisioni siano ammesse)
 - b) tuttavia, se si mettono in atto le decisioni interamente automatizzate, allora non bisogna affidarsi all'articolo 22 Gdpr (che, però, è la norma ad hoc sulle decisioni interamente automatizzate, vietate dalla regola generale)
 - c) peraltro, l'esclusione dell'affidamento all'articolo 22 vale "*di norma*"; cosicché pare di capire che ci sono eccezioni in cui si possono fare decisioni interamente automatizzate sui minori ricorrendo ai presupposti dell'articolo 22 (ma di queste ipotesi si dà un solo esempio e cioè decisioni finalizzate alla tutela del benessere, concetto talmente vago da essere onnicomprensivo)
 - d) è ammessa, invece, anche a riguardo dei minori una decisione interamente automatizzata senza effetti giuridici (categoria per la quale non è facile sciorinare una casistica)
 - e) non a caso, si evidenzia, poi, in maniera criptica che una decisione basata unicamente sul trattamento automatizzato, la quale influenzi le scelte e il comportamento di un minore, potrebbe potenzialmente avere un effetto giuridico o in modo analogo significativo sullo stesso, a seconda della natura delle scelte e dei comportamenti in questione.
- Il tenore di quanto riportato non consente affatto una ricostruzione dell'istituto unicamente sulla base delle norme e, pertanto, si insiste sulla determinante necessità di avere al più presto linee guida delle Autorità di controllo e codici di condotta.

9. RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (Data Protection Officer) deve essere obbligatoriamente nominato nei casi previsti dall'articolo 37 Gdpr.

Peraltro, anche in ambiti estranei a quelli elencati in maniera generica dal citato articolo 37, il Garante per la protezione dei dati personali ha autorevolmente dichiarato che la designazione di tale figura resta comunque raccomandata, anche alla luce del principio di "*accountability*" che permea il Regolamento ([Faq sul Responsabile della Protezione dei Dati in ambito privato](#)).

Tale ultima raccomandazione è da prendere attentamente in considerazione a proposito del trattamento di dati personali di minori, qualunque sia il tipo di informazioni trattate e qualunque sia la base giuridica del trattamento.

A proposito della nomina obbligatoria del Responsabile della protezione dei dati va rammentato che a tale adempimento sono soggetti tutti i titolari/responsabili tenuti all'applicazione del Gdpr.

Tra essi sono compresi anche i titolari/responsabili non stabiliti nell'Unione Europea, assoggettati al Gdpr alla luce del criterio dell'indirizzamento (targeting) del trattamento (articolo 3, par. 2 Gdpr).



A tale ultimo proposito si ricorda che:

a) il Comitato europeo per la protezione dei dati non ha ritenuto che la funzione di rappresentante nell'Unione (da nominarsi di norma a carico del titolare/responsabile non stabilito ai sensi dell' art. 27 Gdpr) sia compatibile con il ruolo di responsabile della protezione dei dati (EDPB, [Linee-guida 3/2018 sull'ambito di applicazione territoriale del Gdpr](#));

b) per garantire l'accessibilità del Responsabile della protezione dei dati, il Gruppo di lavoro Articolo 29 ha raccomandato la collocazione del RPD nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'UE.

Tuttavia, il medesimo WP29 non ha escluso che un RPD possa essere in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE in alcuni casi ove titolare del trattamento o responsabile del trattamento non siano stabiliti nel territorio dell'Unione europea. (WP 29, [Linee guida sui responsabili della protezione dei dati](#)).

10. SICUREZZA

Un altro ambito di natura precettiva, la cui operatività è immediata, concerne la disciplina della sicurezza dei trattamenti di dati.

A tale proposito il Considerando n. 75 sottolinea che i rischi derivanti da trattamenti di dati personali sono da presidiare con particolare riferimento ai casi in cui *"sono trattati dati personali di persone fisiche vulnerabili, in particolare minori"*.

La classe anagrafica degli interessati è parametro da tenere in considerazione nell'analisi dei rischi, nella stesura della valutazione di impatto, nella predisposizione delle misure preventive (ex ante) e di attenuazione dei danni (ex post).

L'appartenenza dei minori alla categoria dei soggetti vulnerabili evidenzia la necessità (unitamente ad altri parametri) di redigere la valutazione di impatto privacy (art. 35 Gdpr).

A tale proposito le *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato"* ai fini del Regolamento (UE) 2016/679", adottate dal WP29 il 4 aprile-4 ottobre 2017, inseriscono tra i criteri del rischio elevato il seguente:

"7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento,".



11. LEGITTIMO INTERESSE

La posizione del minore è considerata nell'ambito delle basi giuridiche del trattamento. Ciò rileva, in particolare, ai fini dell'articolo 6, par. 1, lett. f) Gdpr, per il quale il trattamento è lecito se 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 minore età dell'interessato, dunque, non esclude la possibilità di avvalersi della base giuridica del legittimo interesse.

Peraltro, come ha insegnato il [Parere del WP29 n. 6/2014](#) (sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE adottato il 9 aprile 2014), il legittimo interesse presuppone la definizione di un bilanciamento tra gli interessi o i diritti fondamentali degli interessati e l'interesse del titolare del trattamento. Lo status dell'interessato è, infatti, rilevante ai fini del test comparativo a monte della assunzione del legittimo interesse quale base giuridica del trattamento.

Nel parere si legge che "benché in linea di principio il test comparativo debba essere effettuato prendendo in considerazione un individuo medio, situazioni specifiche devono comportare l'adozione di un approccio basato maggiormente su una valutazione caso per caso: per esempio, potrà essere pertinente esaminare se l'interessato è un minore".

Conclusivamente sul punto, della minore età si potrà tenere conto per ritenere impraticabile la base giuridica del legittimo interesse oppure se ne dovrà tenere conto per aumentare le precauzioni o le misure di tutela a favore degli interessati.

12. MARKETING

Nelle Linee guida in materia di processi decisionali automatizzati e profilazione definite in base alle previsioni del Regolamento (UE) 2016/679", adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017-6 febbraio 2018, si fa un cenno all'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utenti e alla raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore.

In quella sede si esprime la seguente opinione:

"Dato che i minori rappresentano un gruppo più vulnerabile della società, le organizzazioni dovrebbero, in generale, astenersi dal profilarli per finalità di marketing. I minori possono essere particolarmente vulnerabili nell'ambiente online e più facilmente influenzabili dalla pubblicità comportamentale. Ad esempio, nei giochi online, la profilazione può servire per individuare i giocatori che l'algoritmo ritiene più propensi a spendere soldi, oltre a fornire annunci più personalizzati. L'età e la maturità del minore possono influenzarne la capacità di comprendere la motivazione che sta alla base di tale tipo di marketing o le sue conseguenze".

Si tratta di un'affermazione che non blocca il trattamento dei dati per queste specifiche finalità, ma che spinge a un self-restraint da parte del titolare del trattamento.

A questo punto, si attende la costruzione, ad opera del diritto vivente, delle condizioni del rispetto della privacy e della protezione dei dati dei minori nei trattamenti marketing, poiché si tratta di attività non vietata, ma rispetto al quale gli standard di dettaglio non sono forniti dalla norma primaria.



Peraltro, si ritiene opportuno evidenziare che allo stato della legislazione vigente

- 1) le norme conducono a ritenere dovuto il consenso del rappresentante legale del minore per potere trattare i dati del minore di età a fini di marketing;
- 2) le norme conducono a ritenere dovuto il consenso del rappresentante legale del minore per profilare i dati dei minori.

Nel Considerando 47 al Gdpr si fa riferimento al marketing diretto quale legittimo interesse del titolare. Peraltro, quella affermazione è, allo stato, da riferire alle discipline speciali di marketing regolate con il sistema dell'opt-out. In questi casi vale quanto riferito a proposito di legittimo interesse e dati dei minori.

13.SERVIZI DI PREVENZIONE E CONSULENZA DEDICATI A MINORI

Il Considerando 38 al Gdpr individua un settore specifico e lo sottopone a una speciale condizione di liceità. Si tratta dei servizi di prevenzione o di consulenza forniti direttamente a un minore, per i quali il considerando citato riferisce che *"Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario"*.

La notazione del Considerando 38 è del tutto in linea con i principi e gli istituti del diritto positivo italiano che, allo scopo di catalizzare ogni sforzo teso alla maturazione del minore di età, intervengono con interventi specifici e in situazioni in cui, a priori, non sussistono rischi di pregiudizio alcuno.

Per chiarezza non ci si riferisce all'articolo 8 Gdpr, che è del tutto estraneo alla logica appena descritta. Ci si riferisce, invece, ad alcuni ambiti in cui enti pubblici sono incaricati di attività di carattere protettivo dei minori di età, che sono ad accesso diretto dei minori medesimi.

Rientrano in questo settore, ad esempio, le disposizioni in materia di cyberbullismo che consentono al minore ultraquattordicenne di esercitare i diritti previsti a propria tutela contro atti lesivi nei suoi confronti (art. 2, c. 1, l. n. 71 del 2017).

Quando, dunque, è in gioco la difesa dei diritti e degli interessi del minore, l'ordinamento, prendendo atto delle modalità evolutive della maturazione di un ragazzo e di una ragazza, riconosce progressivi spazi crescenti di autonomia al minore, anche in parziale e misurata deroga alla regola della incapacità d'agire e del necessario intervento del rappresentante legale.

Evidenziata la coerenza del Considerando 38 nel sistema dell'ordinamento italiano, occorre d'urgenza l'individuazione di cosa possa essere inserito nella categoria *"servizi di prevenzione o di consulenza forniti direttamente a un minore"*.

Ci si attende, dunque, un intervento chiarificatore, che ovviamente potrà anche essere suscitato da proposte e iniziative degli enti esponenziali che si propongono la difesa dei minori quale compito statutario.

14.CONSENSO DIGITALE

L'articolo 8 del Gdpr si occupa delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione.

Rispetto a questa disposizione è necessario mettere in evidenza che si tratta di una norma speciale relativa alla disciplina dei servizi della società dell'informazione.

In sostanza, non si tratta di una norma generale sul trattamento dei dati dei minori.



Altrimenti detto, per studiare il trattamento dei dati dei minori è un errore partire dall'articolo 8 Gdpr e generalizzare le regole, da esso desumibili, a tutti i trattamenti, che abbiano per oggetto i dati dei minori.

L'articolo 8 Gdpr, dunque, in relazione ai trattamenti di dati, basati sul consenso, realizzati nell'ambito della fornitura di servizi della società dell'informazione:

- a) introduce una prima fascia anagrafica al di sotto della quale i dati del minore non possono essere trattati, se non con il consenso del rappresentante legale;
- b) fissa una seconda fascia anagrafica, nella quale il consenso al trattamento dei dati - relativo all'offerta diretta di servizi della società dell'informazione ai minori - può essere formulato dal minore.

Per una ricostruzione della normativa, ed in una prospettiva di minimizzazione dei possibili pregiudizi per una categoria di soggetti vulnerabili, si ritiene che la nozione di "offerta di servizi" sia distinta dalla nozione di "marketing" e che, pertanto, i trattamenti per finalità di marketing siano esclusi dalla disciplina dell'articolo 8 Gdpr.

Per servizio della società dell'informazione si intende un servizio di cui all'articolo 1, paragrafo 1, lettera b), della direttiva 2015/1535, e cioè

"b) 'servizio': qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per: i) 'a distanza': un servizio fornito senza la presenza simultanea delle parti; ii) 'per via elettronica': un 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; iii) 'a richiesta individuale di un destinatario di servizi': un servizio fornito mediante trasmissione di dati su richiesta individuale."

I dettagli della disciplina del consenso digitale sono esposti da Gruppo di lavoro Articolo 29 nelle "[Linee guida sul consenso ai sensi del Regolamento \(UE\) 2016/679](#)", adottate il 28 novembre 2017 -10 aprile 2018, cui si rinvia.

Nell'ordinamento italiano l'adeguamento al Gdpr è stato effettuato mediante inserimento, da parte del d. lgs 101/2018, dell'articolo 2 – quinquies nel Codice della Privacy, ai sensi del quale si è stabilita in 14 anni l'età soglia per il consenso digitale.

Tale abbassamento rispetto alla soglia del Gdpr (16 anni) è stata, talvolta, giustificata con il raffronto rispetto ad altre norme dell'ordinamento italiano che danno rilevanza al consenso del minore ultraquattordicenne.

A tale proposito sono state, ad esempio, richiamate le norme che attribuiscono al minore ultraquattordicenne il diritto di prestare il proprio consenso all'adozione (art. 7, c. 2, l. n. 184/1983).

Questo orientamento sostiene che sarebbe incoerente ammettere il quattordicenne a prestare il proprio consenso per essere adottato, ma non per iscriversi a un social network.

Si permetta sul punto di motivatamente dissentire. L'estensione analogica delle norme si basa sull'eadem ratio.



Non ricorre questo presupposto allorché si comparano l'adozione e la iscrizione ad un social network: il procedimento adottivo è ontologicamente, strutturalmente e funzionalmente destinato alla protezione del minore, il quale è legittimato a dire la sua opinione rispetto a un contesto di protezione già vagliato da un punto di vista tecnico e dall'autorità giudiziaria; l'iscrizione al social network implica adesione ad entrare in un ambiente pieno di pericoli e senza che lo stesso sia stato scandagliato da alcuna pubblica autorità.

Peraltro, non si può negare la realtà, nella quale la pronta e facile accessibilità delle modalità di interazione e i prodotti immateriali forniti sulla rete elettronica mettono, in ogni luogo ed in ogni tempo, il minore direttamente di fronte allo scaffale virtuale. L'ottica del legislatore europeo è che sia meglio regolamentare, offrendo spazi vigilati di agibilità alle imprese che vogliono entrare in contatto diretto con il minore, anziché vietare tout court o non regolamentare affatto.

Riprendendo la relazione all'allora in itinere decreto legislativo 101/2018, il combinato della regolamentazione europea della legge italiana ha, quindi, stabilito che il minore debba avere almeno quattordici anni al fine di prestare un valido consenso al trattamento dei propri dati, limitatamente ai trattamenti che vengono effettuati nell'ambito dei servizi della società dell'informazione.

Ciò significa che l'ultraquattordicenne può acconsentire ai trattamenti connessi e conseguenti all'iscrizione a social network o a servizi di messaggistica.

È bene ribadire che all'infuori dell'ambito dei servizi della società dell'informazione, permane in ogni caso il limite dei diciotto anni per la prestazione di un valido consenso al trattamento dei dati personali.

In relazione a questo tema, da ultimo, si evidenzia che, per norma espressa dell'ultimo paragrafo dell'art. 8 Gdpr, le regole speciali sul consenso relativo al trattamento dei dati non incidono sulla disciplina italiana relativa alla capacità di agire contrattuale: ragione questa per cui il minore è incapace a esprimere qualsiasi "*consenso contrattuale*", anche quello necessario per concludere un contratto per la fruizione dei servizi della società dell'informazione.

A questo proposito, non rileva tanto la gratuità del servizio, quanto il fatto che si debba concludere un accordo che preveda il sorgere di obbligazioni, anche eventualmente a carico di una sola parte. Certamente l'onerosità del servizio, a carico dell'utente, è sintomatica della presenza di un contratto e ciò spinge a richiedere il consenso del rappresentante legale.

Tuttavia, potrebbe sussistere un accordo, e quindi un contratto, con profili di onerosità solo a carico di una parte.

Ciò che rileva, dunque, è la presenza di un "*accordo*" tra due soggetti, fonte di obbligazioni.

Peraltro, se si accettasse l'orientamento per cui rappresenta un contratto lo scambio di "*servizi contro dati*" (vedasi [Tribunale Amministrativo Regionale per il Lazio, sezione prima, sentenza n. 261/2020](#)), si dovrebbe ammettere che si conclude un contratto ogni volta che taluno acconsenta al trattamento del dato.

La materia non mancherà di sviluppi in giurisprudenza e presso le autorità di controllo.

Nel frattempo, si ritiene opportuno che il titolare del trattamento, nell'ambito del proprio modello organizzativo privacy, motivatamente assuma e dichiari se il trattamento dei dati del minore avvenga o non avvenga nell'ambito di un accordo contrattuale. In mancanza di un accordo, infatti, non sussiste un contratto e, quindi, neppure materia per l'applicazione dell'ultimo paragrafo dell'articolo 8 Gdpr.

