Manfredi A, *Art. 8 GDPR e monetizzazione delle informazioni del minore. Tra consenso e contratto zero price* (2024) 2 EJPLT.
DOI:

EJPLT
ISSN 2704-8012



Art. 8 GDPR e monetizzazione delle informazioni del minore. Tra consenso e contratto zero price

Art. 8 GDPR and monetisation of the information of the minors. Between consent and zero-price contract

ALESSANDRO MANFREDI
Dottorando di ricerca
Università Magna Græcia di Catanzaro.

Abstract

Attraverso il saggio, l'autore intende delineare gli offuscati contorni dell'articolo 8 del GDPR. I minori, in quanto categoria vulnerabile in sede di trattamento dei dati personali, sono maggiormente connessi ai rischi ricollegabili all'uso delle piattaforme virtuali, le quali fanno ampio uso della c.d. contrattazione a prezzo zero. Attraverso il saggio verrà analizzato il rapporto tra capacità di agire del minore e consenso al trattamento dei dati, raffrontandolo alla sempre più concreta patrimonializzazione dei dati personali. Infine, verranno osservati i limiti di età delineati dal GDPR.

Through this essay, the author intends to outline the blurred boundaries of Article 8 of the GDPR. Minors, as a vulnerable category when it comes to the processing of personal data, are more connected to the risks associated with the use of virtual platforms, which make extensive use of so called zero-price contracts. The article analyses the relationship between the legal capacity of minors and their consent to the processing of data and compares it with the increasingly tangible capitalisation of personal data. Finally, it will consider the age limits set by the GDPR.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: GDPR; Consenso al trattamento dati del minore; monetizzazione.

Summary: 1. Introduzione. – 2. Il consenso del minore al trattamento dei dati e la capacità di agire. – 3. Dato personale e valore patrimoniale. – 4. Frammentarietà dei limiti di età. – 5. Conclusioni.

1. Introduzione.

Le nuove generazioni dimostrano una notevole capacità di adattamento al mondo digitale. Tale capacità permette loro di utilizzare determinati strumenti tecnologici già in giovane età, aprendo loro la strada all'utilizzo di varie tipologie di servizi digitali. Come è noto, i *social network*, le app di messaggistica, le c.d. gaming apps e le altre applicazioni di uso comune fra i minori sono spesso fornite gratuitamente al fine di attrarre utenza. La gratuità di accesso a tali contenuti porta comunque alla creazione di complessi e paralleli circuiti di monetizzazione, spesso utilizzati ai fini del mantenimento dei vari software e servizi immessi sul mercato. Ciò avviene principalmente mediante strumenti di profilazione, sfocianti, ad esempio, in diverse tipologie di online advertising oppure nell'uso di advertising supported software (attraverso il tipico fenomeno del pay per click [1]).

Tali attività potrebbero produrre particolari rischi per questa sostanziosa fascia di utenza, essendo i minori una categoria vulnerabile esposta in modo continuativo ai suddetti servizi [2]. I rischi afferenti alle attività di tutela dei minori rendono necessaria un'analisi delle norme del Regolamento 2016/679 (in tema di protezione dei dati personali delle persone fisiche), al fine di osservare come vengano trattati i dati personali dei minori, in particolare durante la fruizione dei servizi della società dell'informazione. I suddetti servizi si distinguono per l'ampio uso della c.d. contrattazione a prezzo zero (o zero price), ovvero prestazioni di natura negoziale in cui è possibile accedere a un servizio in modo apparentemente gratuito [3].

Come si avrà modo di analizzare, il trattamento dei dati personali del minore presuppone la valutazione di diversi aspetti: anzitutto si tocca il profilo della

[1] Per pay per click (pagamento per click) si intende un modello di pubblicità basato su fruizione, ovvero, mediante monetizzazione per interazione. Tale modello consente agli inserzionisti pubblicitari di pagare la dovuta tariffa solo nel momento in cui un utente interagisce con la pubblicità stessa. Il modello prevede l'uso di banner pubblicitari utilizzati per attrarre i click degli utenti che fruiscono di uno determinato sito web/applicazione, il pagamento della tariffa al sito ospitante avviene nel momento in cui l'utente accede all'annuncio pubblicitario attraverso il banner.

[2] I. A. CAGGIANO, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione,* in Familia, 2018, 1, pp. 6 - 7

[3] V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in AA. VV, *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, 2019, pp. 35-49.
Tale modello di contrattazione prevede che l'utente acceda al servizio gratuitamente attraverso la stipulazione di un contratto per la prestazione di un servizio senza pagamento di un corrispettivo. Inevitabilmente, come si avrà modo di analizzare, tale forma di contrattazione tra le parti è sospesa, nella sua identità, tra atti di liberalità e contratti a titolo apparentemente gratuito in cui la controprestazione è individuabile direttamente nei dati personali, oppure indirettamene nelle operazioni ad essi correlate (come, ad esempio, il marketing basato sulla creazione di profili di personalità).

liceità del trattamento, ma non meno rilevante è quello dei rapporti con l'istituto della capacità di agire.

2. Il consenso del minore al trattamento dei dati e la capacità di agire.

La tutela del minore interessato dall'attività di trattamento dei dati è oggetto di attenzioni specifiche nell'art. 8 del GDPR. L'articolo, nei suoi tre paragrafi, identifica la base giuridica di liceità del trattamento, la cornice anagrafica, il ruolo del titolare della responsabilità genitoriale e le disposizioni relative ad eventuali contrattazioni.

L'articolo 8 cerca di fornire una limitata autonomia decisionale al minore, proteggendolo al contempo dai rischi propri dell'immaturità. A riguardo, giova asserire che il propedeutico considerando n. 38 [4] del GDPR afferma la necessità di garantire ai minori una specifica protezione, in quanto soggetti interessati meno consapevoli dei rischi e delle conseguenze poste dal trattamento dei dati. Le attività ritenute maggiormente incidenti sono sostanzialmente il marketing e il profiling. L'art. 8 stabilisce che il trattamento dei dati personali del minore è lecito quando lo stesso presta il consenso [5] relativamente all'offerta diretta di servizi della società dell'informazione. La norma così posta individua e racchiude l'unica eventualità di trattamento dati lecito posta autonomamente dal minore, cercando di rimodularne l'incapacità attraverso una conformazione alla quotidiana realtà della società dell'informazione. Ciò avviene per mezzo di un bilanciamento tra la protezione delle informazioni del minore e l'autonomia necessaria allo sviluppo della sua personalità, in ossequio al principio del *favor minoris* [6].

È pertanto opportuno individuare come tale limitata capacità di agire si coniughi con l'incapacità ex art. 2 c.c. Prima di ciò, effettuando una breve digressione dal tema trattato, è constatabile come le recenti produzioni del legislatore comunitario (soprattutto GDPR e Artificial Intelligence Act) prendano spesso spunto da istituti afferenti a ordinamenti giuridici di estrazione nordamericana. Un simile influsso – dovuto principalmente alle capacità scientifico/industriali degli apparati produttivi degli Stati Uniti - rende maggiore, superficialmente, la compatibilità di alcuni istituti dei regolamenti comunitari dedicati al digitale con gli istituti propri dei sistemi di common law [7], che spesso non tengono conto di alcune distinzioni operanti in ordinamenti

---

[4] Considerando 38 del Regolamento UE 2016/679: «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 interessate 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 a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.»

[5] Per esplicita menzione nel dato normativo dell'art. 8: «Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni…»

[6] G. M. RICCIO, G. SCORZA, E. BELISARIO, *GDPR e normativa privacy, Commentario*, 2° ed., Milano, 2022, p. 106

[7] Un esempio lampante può essere individuato nell'adozione dei principi di privacy by default e privacy by design, istituti di certa estrazione nordamericana (Canada), sul punto v. S. BONGIOVANNI, C. MOTTINO, *Il Vademecum sul regolamento europeo n.2016/679*, Milano, 2017, pp. 84-85. Altro esempio può essere

di Civil law. Facendo riferimento alle pertinenze dell'art. 2 c.c., si può ad esempio osservare come la distinzione tra capacità giuridica e capacità di agire non sia presente nei paesi di common law, orientando il tutto verso l'omnicomprensiva legal capacity.

Ritornando all'art. 2 c.c. e sul diritto comunitario, l'art. 2 c.c., come ben noto, identifica nella maggiore età la capacità di agire di un individuo, la quale costituisce un requisito di validità relativo alla conclusione di atti di natura negoziale. A livello ermeneutico, il dogma dell'incapacità del minore è andato incontro a un'opera di temperamento, portando ad una circoscrizione del suo campo di azione ad atti di natura patrimoniale, concedendo al minore un certo livello di autodeterminazione sui diritti fondamentali e sulla realizzazione diretta di alcuni dei suoi interessi [8]. La moderazione dell'art. 2 c.c. è anche conseguenza della valorizzazione dell'autodeterminazione del minore [9] e non dell'incapacità di agire del minore, quale strumento di tutela dello stesso, riconoscendone di fatto una certa autonomia. Il riconoscimento di una maturità sufficiente a compiere determinati atti è da tempo presente in diverse esperienze giuridiche europee. Tra le principali esperienze si possono citare, ad esempio, les actes de la vie courante del Code Civil Francese, l'individuazione della maturità del minore (condiciones de madurez) del Código Civil spagnolo oppure l'individuazione degli spazi di capacità nelle amministrazioni di sostegno proprie del Betreuung tedesco e del Sachwalterschaft austriaco. Nelle predette esperienze si palesa, con le dovute differenze, un'opera di gradazione dell'autonomia del soggetto vulnerabile, graduata in base al livello di maturità raggiunto e alle diverse circostanze con cui potrebbe confrontarsi[10], valorizzando di fatto il livello di autodeterminazione.

In tale contesto vi potrebbe rientrare il consenso al trattamento dei dati da parte del minore di età, in quanto, il consenso, inquadrato quale elemento di liceità per il trattamento dei dati, nonché presupposto per l'esercizio di un

rintracciato nella definizione di accountability, intesa in italiano quale responsabilizzazione/responsabilità e differente dalla responsabilità di gergo tecnico inglese di responsability. Definizioni e termini spesso utilizzati in coppia nelle c.d. norme standardizzate (es. ISO) nell'accezione di "accountability and responsability".

[8] Tra cui si annoverano: P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Napoli, 1975, pp. 247 - 332 e ss.; P. PERLINGIERI, *Rapporti personali nella famiglia*, Napoli, in Rass. dir. civ., ESI, 1982, pp. 23 ss.; F. D. BUSNELLI, *Capacità ed incapacità di agire del minore*, in Fam. pers. succ.,1982, pp. 59 ss.; F.D. BUSNELLI, F. GIARDINA, *La protezione del minore nel diritto di famiglia italiano*, in Giur. it., 1980, pp. 14 – 15; E. QUADRI, *L'interesse del minore nel sistema della legge civil*e, in Fam. dir., 1999, p.83; E. LA ROSA, *Tutela dei minori e contesti familiari. Contributo allo studio per un diritto dei minori*, Milano, 2005, pp. 57 e ss.

[9] Art. 12 della Convenzione di New York sui diritti del fanciullo del 20 novembre 1989, nella quale si statuisce: «States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child. »

[10] Per approfondimenti sul tema si rimanda v. M. L. CHIARELLA, *Paradigmi della minore età*, Soveria Mannelli, 2008, pp. 45 e ss.

diritto personalissimo [11], consentirebbe al minore un certo livello di autodeterminazione ricollegato ad un suo diritto fondamentale[12].

L'individuazione del consenso quale strumento di liceità del trattamento dei dati emerge altresì dal freno scaturente dall'art. 7, par. 4, del GDPR [13]. L'art. 7, par. 4, afferma come nel dover valutare l'effettiva libertà di prestazione del consenso [14], si debba tener conto dell'eventualità in cui l'esecuzione di un contratto, compresa la fornitura di un servizio, non sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto. Articolo che non pone un divieto di carattere generale a tali forme di trattamento. Infatti, la norma si limita ad inserire un ulteriore elemento di valutazione della liceità complessiva del consenso.

Già da tempo, per mezzo di attenta dottrina, è stato possibile individuare tale peculiarità nella norma, identificandola quale *praesumptio iuris tantum* e non *praesumptio iuris et de iure.* Quanto proposto escluderebbe l'assolutezza del divieto, accorpandolo, di fatto, ad altri fattori, tra i quali vi rientrerebbero la concorrenza, la fungibilità del servizio e l'eventuale mancanza di una negoziazione individuale [15]. Ciò consentirebbe il mantenimento dell'impianto di tutela basato sul consenso, affiancandolo all'uopo all'utilizzo di ulteriori mezzi, differenti dal consenso, qualora i dati da trattare fossero necessari alla conclusione di un contratto (come specificato nelle linee guida dell'EDPB [16]).

---

[11] Ritengono che il consenso sia fondamento di legittimità per il trattamento stesso S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy, in Europa e diritto privato*, 2004, p. 2 ss.; S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in Riv. dir. civ., 2001, vol. 6, pp. 621 ss; risultando particolarmente dirimente se rapportato alla tutela dei dati personali intesa quale specificazione autonoma del diritto alla riservatezza, oggetto di dibattito in dottrina. Sul punto v. M. C. BIANCA, *Note Introduttive*, in AA. VV. *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy»,* a cura di C. M. BIANCA, F. D. BUSNELLI, Padova, 2007, pp. XIX ss.

[12] L'attenzione verso la riservatezza del minore, è conseguenza della sovrapposizione di una posizione di protezione di rilievo costituzionale, ossia la riservatezza, con la specificità del minore quale soggetto giuridicamente meritevole di specifiche tutele. Da tale sovrapposizione discendono una serie di conseguenze, come si avrà modo di analizzare, in ordine allo sviluppo della personalità del minore, le quali potrebbero interferire con altre disposizioni parimenti riconosciute (come, ad esempio, la potestà genitoriale). A riguardo v. V. GAGLIARDI, *Art. 50: Notizie o immagini relative a minori*, *ivi,* pp. 905 ss.

[13] Art. 7 par. 4 del Regolamento 2016/679: «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.»

[14] Brevemente, il consenso al trattamento dei dati può essere inteso quale atto fondamentale e inequivocabile, posto dall'interessato, che permette al titolare del trattamento di effettuare operazioni di processing dei dati, segnando per cui una separazione tra un trattamento lecito e un trattamento illecito. Il consenso è un atto strettamente correlato alla dignità e alla libertà personale, oltre che specchio di una riflessione libera, specifica e informata, da parte dell'interessato che deve prestarlo. Inoltre, la prestazione del consenso non è esente da ripensamenti, in quanto il Regolamento concede all'interessato la possibilità di revocare il consenso in qualsiasi momento. Per una ricognizione approfondita del consenso al trattamento v. F. CAGGIA in AA. VV., *I dati personali nel diritto europeo*, *cit.,* pp. 249 ss.; F. BRAVO in AA. VV. *La protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101,* a cura di G. FINOCCHIARO, Bologna, 2019, pp. 140 ss.;

[15] G. ALPA, G. RESTA, *Le persone e la famiglia. Vol. 1: Le persone fisiche e i diritti della personalità,* Torino, 2019, pp. 543 e ss.

[16] EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects: «The WP29 guidelines on consent also clarify that where "a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis". Conversely, the EDPB considers that where processing is not in fact necessary for the performance of a contract, such processing can take place only if it relies on another appropriate legal basis»

Impostazione che tra l'altro emerge da un'analisi storica evocata in dottrina. L'art. 7, par. 4, nella sua prima instaurazione, antecedente al testo definitivo del GDPR [17], presentava l'elemento del notevole disvalore tra le parti nelle operazioni di processing, rimosso in iter legislativo ordinario in favore dell'attuale formulazione [18].

La presenza del disvalore nella norma garantirebbe la possibilità di quantificare l'accessorietà del consenso rispetto alla previsione individuata dalla fattispecie, escludendo ulteriormente la generalità e l'assolutezza del divieto di cui all'art.7, par. 4. Ciò potrebbe portare ad alcune riflessioni circa l'universale applicabilità dell'impianto basato sul consenso in tema di data protection [19] e ad un suo settoriale superamento.

È comunque necessario precisare, come l'EDPB abbia già da sé individuato alcuni parametri afferenti all'art. 7, par. 4 utilizzabili ai fini di una verifica della liceità del consenso prestato, affermando che: «any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.»[20]. A riguardo l'EDPB nello specifico individua quattro differenti parametri di valutazione del consenso ovvero: imbalance of power, conditionality, granularity e detriment.

La condizionalità, strettamente correlata ai vincoli posti dall'art. 7, par. 4, non è considerata in senso assoluto dall'EDPB. Secondo il garante europeo, l'interpretazione normativa fornita dal, non vincolante, considerando n. 43[21] prevede che in un numero molto ristretto di casi tale condizionalità potrebbe non rendere invalido il consenso, presumendo l'eccezionalità di una siffatta eventualità. Egualmente incidente è il già menzionato squilibrio di potere, il quale, per espressione dell'EDPB, è circoscritto principalmente al rapporto tra interessato ed ente pubblico oppure verso vincoli di carattere occupazionale [22].

---

[17] Il riferimento è alla risoluzione, in prima lettura, del Parlamento Europeo del 12 marzo 2014: «Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller…) ». (Consultabile al seguente link: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html#title1)

[18] Per un'attenta e completa ricostruzione dell'iter legislativo ordinario v. G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2022, pp. 98. ss.

[19] *Ibidem*

[20] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, pp. 7-8. (Consultabile al seguente link: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en)

[21] Considerando n. 53 del GDPR: «Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione».

[22] EDPB, *op. cit.*, pp. 7 ss.

Un esempio (Cypriot Data Commissioner, 11.17.001.007.219 KEO PLC (2020)) è rinvenibile in casistica afferente ad un reclamo da parte di alcuni dipendenti di una società cipriota successivamente accolto dal Commisioner for Personal Data Protection di Cipro. I dipendenti contestavano alla società l'introduzione di un sistema di tracking aziendale (ricollegato all' Enterprise Resource Planning) attraverso smart card comprendente un terminale munito di rilevamento della scheda e di una telecamera utilizzata al fine di individuare eventuali irregolarità nell'uso delle stesse. Relativamente alla prestazione del consenso la DPA di Cipro ha individuato come nei termini previsti dall'art. 7 par. 4 del GDPR: «Due to an employment

Quanto prescritto dall'art. 7, par. 4, deve essere letto in combinato disposto con l'art. 8, par. 3 del GDPR, nel quale si prevede che le disposizioni relative al par. 1 dell'art. 8 (consenso autonomo del minore) non pregiudichino le disposizioni generali del diritto dei contratti degli Stati membri. Quindi, l'art. 8 acquisirà particolare validità nel caso in cui il trattamento dei dati personali non riguardi l'uso di dati indispensabili alla conclusione di un contratto.

Da quanto affermato emerge inevitabilmente un'incongruenza, in quanto, ci si potrebbe spesso ritrovare in una circostanza di validità del consenso con contratto non siglabile. Eventualità che potrebbe manifestarsi con una certa frequenza durante la fruizione di servizi digitali, risultando pertanto inevitabile l'intervento del titolare della responsabilità genitoriale (in base alle disposizioni previste dai vari Paesi membri) il quale andrà a concludere il contratto lasciando la prestazione del consenso al minore [23]. L'eventualità menzionata porrebbe un ragionevole freno alla limitata capacità di agire concessa al minore, creando un cortocircuito negli obiettivi normativi del legislatore comunitario. Infatti, la definizione di servizi della società dell'informazione legata al consenso del minore, rintracciabile per richiamo dell'art. 4 n. 25 del GDPR nella Direttiva del 9 settembre 2015, n. 1535 [24], evidenzia come i suddetti servizi siano prestati normalmente dietro retribuzione. Per cui, potrebbe rendersi inefficace la limitata autonomia concessa al minore, il quale attraverso la sola prestazione del consenso al trattamento dei dati potrebbe non essere in grado di avvalersi autonomamente di alcuni servizi digitali.

Per dissipare il problema evidenziato si potrebbe valutare una possibile considerazione di tali eventualità negoziali quali negozi di minuto valore. In tal senso, il nostro ordinamento rileva una limitata capacità di agire al minore per quegli atti di natura patrimoniale di lieve valenza economica, definiti per terminologia anglosassone come necessaries, ovvero i negozi della vita quotidiana o di vita corrente. La considerazione dei negozi relativi ai servizi della società dell'informazione quali necessaries ben si sposerebbe con il principio di diritto cogente del superiore interesse del minore, in quanto gli atti di vita corrente incidono sulla crescita del minore edificando la sua identità attraverso una simbiosi tra dimensione patrimoniale e identitaria/personale [25].

Siffatta eventualità partirebbe comunque da una effettiva valutazione dei servizi della società dell'informazione quali negozi di minuto valore; cosa nell'effettivo non riscontrabile, non essendo possibile quantificare il valore che i dati personali potrebbero eventualmente assumere quando ricollegati al singolo individuo.

---

contract, the employer shall be considered to hold a dominant position and any such consent can not be characterised as an explicit agreement. »

[23] M. OROFINO, F. G. PIZZETTI, *Privacy, minori e cyberbullismo*, Torino, 2018, p. 27.

[24] Art. 1, lett. b della Direttiva 2015/1535: «"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.». Definizione di più ampia portata rispetto ai servizi di comunicazione elettronica previsti dal Codice Privacy pre-novella, descritti dall'art. 4, comma 2, lett. e), come: «servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva»; a riguardo v. F. QUADRI, *Art. 121: Servizi interessati*, in AA. VV., *La protezione dei dati personali. Commentario, cit.*, pp. 1524 ss.

[25] R. SENIGAGLIA, *Minore età e contratto, Contributo alla Teoria della capacità,* Torino, 2021, p. 217

3. Dato personale e valore patrimoniale.

La limitata capacità di agire offerta al minore si scontra con un inevitabile quesito, valutare se il dato personale, inquadrato in un tessuto sociale estremamente «datificato» [26], debba essere considerato economicamente apprezzabile.

Per provare a dare una risposta a tale quesito, è utile esporre l'esistenza di due orientamenti contrastanti riguardanti l'apprezzamento economico del dato personale. Un primo orientamento, sostenuto dalle autorità di controllo sulla protezione dei dati personali, riconosce i dati quali elementi annessi ad un diritto della personalità (la riservatezza/protezione dei dati personali), per cui di difficile coniugazione con operazioni di monetizzazione. Tra le autorità in questione rientra l'European Data Protection Supervisor (EDPS) [27], la quale, richiamandosi all'art. 8 della Carta di Nizza e all'art. 16 del TFUE, suggerisce l'impossibilità di parificare un diritto fondamentale ad una semplice transazione di tipo commerciale [28]. Inoltre, l'EDPS sottolinea come l'indicazione del dato personale quale "elemento con valore di moneta" potrebbe generare problemi di carattere positivo. In particolare, per l'EDPS, non sarebbe possibile determinare *ex ante* il valore che i dati personali acquisirebbero durante le operazioni di trattamento.

Quanto accennato trova conferma nei dettami della Direttiva 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuti e di servizi digitali, successiva alla menzionata opinione fornita dall'EDPS. Infatti, l'art. 3 della Direttiva non ravvisa nel dato personale un valore di controprestazione, aderendo di fatto a quanto auspicato dall'EDPS [29].

Impostazione, peraltro, anche sostenuta in dottrina, dove l'utilizzo economico degli attributi di personalità è stato a lungo trascurato, evidenziando una palese refrattarietà nell'attribuire un valore economico alle lesioni della personalità, in conseguenza di valutazioni etico-morali relative ai diritti della personalità e alla loro indisponibilità [30].

---

[26] La "datificazione" della società e conseguentemente del sostrato economico ad essa riferibile non è nuova in dottrina. La datificazione della società implica una continua estrazione di informazioni da qualsiasi entità esistente, portando alla creazione di una risorsa economicamente apprezzabile in quantita illimitata, inedita in ambito economico. Per cui l'effettiva ed eventuale circoscrizione della fruibilità da parte dei mercati del dato personale (e della c.d. datasfera) diventa un elemento dirimente sul futuro dei c.d. diritti epistemici. Sulla datificazione della società e sulla presenza di una «datasfera» v. V. ZENO-ZENCOVICH, *Do data markets exists?*, in Media Laws, 2019, pp. 1-17; J.S. BERGÉ, S. GRUMBACH, V. ZENO-ZENCOVICH *The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance*, in European Journal of Comparative Law and Governance, Vol. 5, Issue 2, 2018, pp. 144 ss.

[27] EDPS, autorità di supervisione del trattamento dei dati da parte delle istituzioni comunitarie

[28] Il riferimento è all'opinione 04/2017 dell'EDPS antecedente alla creazione della Direttiva 2019/770: «One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction». La quale altresì richiama ai citati art. 8 della Carta di Nizza e l'art. 16 del TFUE attraverso la citazione dell'opinione 08/2016 della stessa EDPS. (Consultabile al seguente link: https://edps.europa.eu/sites/edp/files/publication/170314_opinion_digital_content_en.pdf

[29] V. PAGNANELLI in E. CREMONA, F. LAVIOLA, V. PAGNANELLI, a cura di, *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022, pp. 4 e ss.

[30] V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in Diritto dell'Informazione e dell'Informatica (Il), fasc.4, Giuffrè, 2018, pp. 689 ss. il quale

Diversa prospettiva è rinvenibile in recente giurisprudenza amministrativa. L'ormai nota sentenza del TAR del Lazio n. 260 del 10 gennaio 2020 - relativa alla condanna di Facebook da parte dell'AGCM per pratiche commerciali ingannevoli e aggressive - pur evidenziando l'essenza della tutela dei dati quale espressione di un diritto della personalità, riconosce il dato personale quale elemento di controprestazione contrattuale, inteso quale possibile oggetto di una compravendita [31]; concretizzando l'utilizzo delle tutele della disciplina consumeristica in tali ipotesi di scambio [32]. Altresì nel successivo intervento del Consiglio di Stato, con riferimento alla sentenza del 29 marzo 2021, n. 2631 [33], si afferma come la patrimonializzazione da parte dei social network avvenga ad insaputa dell'utenza, la quale procede con la convinzione di iscriversi senza costi alla piattaforma. Al contrario, secondo il Consiglio di Stato, i dati dell'interessato verrebbero impiegati per effettuare attività di profilazione per finalità commerciali, senza che l'utenza ne abbia un'informata contezza.

Confermando il Consiglio di Stato la natura ingannevole dell'attività di Facebook, individuata dall'AGCM prima e dal TAR poi, nella parte afferente alla pubblicizzazione della gratuità della piattaforma, si riconosce implicitamente la natura onerosa del contratto stipulato all'atto di iscrizione.

L'impostazione dettata dalla giurisprudenza potrebbe scaturire dall'effettiva impossibilità di collocare l'erogazione di servizi *social* nella categoria dei c.d. atti di liberalità, nei quali la volontà realizzativa di natura patrimoniale dell'attore non prevede un effettivo interesse economico.

La ricostruzione testé effettuata, ovviamente, non si concilia con la ricostruzione operata dalla difesa di Facebook, la quale fa coincidere il dato personale ad una *res extra commercium*. Invero si può osservare come Facebook (nel momento in cui il presente saggio è scritto) non costringa l'utente che utilizza la piattaforma a prestare il consenso al trattamento dei propri dati per finalità di natura commerciale. All'atto di creazione di un account e durante

---

richiama a V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. inf. e informatica*, 1993, pp. 545 ss.,

[31] TAR Lazio, sez. I, sent. 10.1.2020, n. 260: «Le tesi di parte ricorrente presuppongono che l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, e per tale motivo Facebook era tenuta esclusivamente al corretto trattamento dei dati dell'utente ai fini dell'iscrizione e dell'utilizzo del "social network". Tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto. A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati.»

[32] Sul punto v. C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette,* in *Giur. it.* 2021, pp 320 – 333; la quale, nell'evidenziare la necessità di equilibrare le diverse esigenze poste dalla sentenza in commento, individua come la decisione del TAR abbia il pregio di fornire diversi possibili spunti sull'uso degli strumenti propri del diritto patrimoniale, utilizzabili in complemento con gli strumenti offerti dalle norme di data protection*,* al fine di particolareggiare la tutela della protezione dei dati personali senza contraddirla.

[33] Sentenza riguardante il ricorso alla sentenza del TAR del Lazio testé menzionata. Nella sentenza del TAR del Lazio i giudici hanno confermato la sanzione di 5 milioni di euro a Facebook per pratica commerciale ingannevole, ritenendo invece insussistenti gli elementi a favore di una sanzione per pratiche commerciali aggressive. L'ingannevolezza del social, relativa alla gratuità del servizio, è stata altresì individuata dal Consiglio di Stato, attraverso la conferma della sentenza del TAR. Per un commento alla sentenza v. G. SCORZA, *Facebook non è gratis?*, in *Dir. di Internet*, 3, 2021, pp. 547 - 571

l'utilizzo del social network viene fornita all'utente, in ossequio a quanto previsto in tema di informazione dal GDPR e dal menzionato art. 7, par. 4, la possibilità di fornire il consenso per il trattamento di quei dati paralleli, non inquadrabili tra i dati fondamentali alla conclusione del contratto stesso, dai quali potrebbe effettivamente scaturire una monetizzazione. Non essendo esplicitamente menzionata dalla piattaforma un'ipotesi di uso dei dati quale diretto corrispettivo, mancherebbe un effettivo elemento di costituzione di un negozio di natura onerosa basato su dati personali. È comunque innegabile che Facebook riesca a monetizzare i dati personali per i quali l'interessato presta volontariamente il consenso, facendo decadere *de facto* un'eventuale natura liberale dell'offerta proposta dal social network. Un'interessante considerazione a tal proposito è individuabile in recente dottrina, secondo la quale si potrebbe identificare nei negozi zero price un contratto atipico a titolo gratuito, attraverso il quale si persegue un interesse economico estraneo alla fattispecie negoziale [34].

4. Frammentarietà dei limiti di età.

Altro elemento importante individuabile dall'art. 8 è la cornice anagrafica, la quale delinea, come già evidenziato, il limite oltre cui il minore non si può considerare cosciente delle proprie scelte, quindi incapace di prestare consenso al trattamento. Il limite di liceità è individuato dalla norma nei 16 anni, limite che può essere abbassato all'uopo dagli Stati membri fino ad un minimo di 13 [35].

Da tale impostazione, ne consegue un certo livello di disorganizzazione che potrebbe manifestarsi, ad esempio, nel caso in cui un minore, cittadino di un paese con un determinato limite di età in tema di consenso, volesse usufruire dei servizi di un altro paese dell'Unione Europea nel quale tale limite è differentemente quantificato. Risulta pertanto difficile superare tale mancanza di uniformazione, considerando la semplice volontà della norma di rendere valido il consenso, sorvolando questa, sui differenti parametri relativi alla capacità di agire presenti nei diversi stati membri. È comunque utile sottolineare come i limiti di età individuati dal legislatore europeo risultino congrui allo sviluppo emotivo del minore [36], come precedentemente analizzato [37].

La norma evidenzia inoltre come in mancanza dei requisiti di età, il consenso possa essere prestato da chi eserciti la responsabilitàma genitoriale. A tal fine, il titolare del trattamento deve necessariamente verificare l'effettivo apporto del titolare della responsabilità genitoriale nella prestazione del consenso [38],

[34] *ivi*, p. 570
[35] Art. 8 par. 1 del Regolamento 2016/679: «Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni».
[36] I. A. CAGGIANO, *op. cit.*, pp. 17-18
[37] V. par. 2 del presente scritto.
[38] Art. 8 par. 2 del Regolamento 2016/679: «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».

fermo restando le disponibilità tecnologiche in merito [39]. La norma appare comunque astratta nel circoscrivere l'eventualità menzionata, non tenendo di fatto conto della consuetudinaria fruizione "anonima" di determinati servizi spesso utilizzati dai minori, non prevedendo, di conseguenza, specifici strumenti in merito [40].

L'impostazione prescritta è fondamentale per il minore ai fini della fruizione in semi-autonomia di alcuni servizi, ponendo di fatto un'importante differenza rispetto ad altri corpi normativi come il «Children's Online Privacy Protection Act» americano, che prevede un divieto totale di iscrizione al minore (in questo caso con limite di età di 13 anni) [41].

Con riguardo alle disposizioni del Codice Privacy successive all'introduzione del D. lgs n. 101 del 2018 [42], l'art. 2-quinquies stabilisce nei 14 anni la soglia minima relativa al consenso del minore, evidenziando tra l'altro come il consenso al trattamento dei dati degli interessati al di sotto dei 14 anni non sia precluso, concedibile da chi eserciti la responsabilità genitoriale. Infine, l'art. 2-quinquies menziona come il titolare del trattamento dei dati debba garantire al minore la dovuta informazione e le conseguenti comunicazioni con linguaggio semplice, facilmente accessibile e comprensibile, al fine di rendere significativo il consenso prestato da quest'ultimo.

5. Conclusioni.

Il binomio contrattazione zero price e consenso del minore è complesso. La complessità scaturisce dalla difficoltà di individuare il valore economico del dato personale, identificabile quale variante principale da un punto di vista negoziale. Per cui è lecito chiedersi se il dato personale abbia un concreto valore commerciale, tanto da poter essere economicamente considerato e addirittura scambiato.

Il dato personale, innanzitutto, non andrebbe inteso quale elemento patrimoniale in senso stretto, in quanto ricollegato ad un diritto della personalità, ovvero la riservatezza, il cui valore patrimoniale potrebbe derivare da una sua lesione. D'altro canto, è evidente come il dato personale sia, in concreto, economicamente apprezzato e utilizzato.

Sia la valutazione del dato personale quale *res extra commercium*, sia la valutazione del dato personale quale elemento utile ai fini di un apprezzamento economico, possono essere considerate plausibili e verosimili.

---

[39] EDPB, *op. cit.,* p. 25: «Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor. If doubts arise the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required».

[40] I. A. CAGGIANO, *op. cit.,* pp. 17-18. Da tale eventualità potrebbero altresì scaturire criticità tipiche della sicurezza informatica, individuate a più riprese dal GDPR. È comunque da specificare come dall'applicazione di una misura di sicurezza tecnica non debba conseguire necessariamente la "segretezza" del dato, bensì un congruo adeguamento tecnico volto a mitigare forme di trattamento difformi da quanto previsto dal dato normativo, come specificato da tempo in dottrina. Sul punto v. P. TROIANO, *Art. 36, Adeguamento*, in AA. VV., *La protezione dei dati personali. Commentario, cit.*, pp. 685 ss.

[41] M. OROFINO, F. G. PIZZETTI, *op. cit.*, p. 25.

[42] Decreto di adeguamento del Codice Privacy alle disposizioni del GDPR.

Per tali motivi si potrebbe delineare la valutazione economica del dato personale non quale elemento patrimoniale, bensì quale elemento monetizzabile.

In tal senso, l'impronta data dalla giurisprudenza amministrativa è realista, in quanto pur essendo ricollegato ad un diritto della personalità, il dato personale è indubbiamente apprezzabile nel suo valore economico. Peraltro, il provvedimento è in linea con la volontà del legislatore comunitario di mantenere un approccio liberale[43] sull'uso dei dati, in quanto il Regolamento intende parificare la protezione delle persone fisiche alla materiale circolazione dei dati [44], consentendo di conseguenza l'evoluzione e la crescita dello spazio economico europeo. Tuttavia, una patrimonializzazione del dato personale, inteso quale valido elemento di scambio, non troverebbe corrispondenza con l'effettiva monetizzazione per mezzo di profilazione. La monetizzazione effettuata dai social network spesso non dipende dalla sottoscrizione dei termini di utilizzo, portando di conseguenza ad un preciso scambio fruizione - compenso in dati, ma scaturisce da una concomitante attività di trattamento, espressione di un consenso informato a trattamenti opzionali. Appare quindi interessante la valutazione del contratto collegato ai servizi della società dell'informazione (zero price) quale contratto atipico, in cui il beneficio patrimoniale scaturisce da un'attività parallela all'erogazione del servizio. Liberando di fatto la valutazione economica del dato personale, in *tertium non datur*, sospesa tra atti di liberalità e negozi patrimoniali.

In relazione al ruolo del minore, accertato come l'art. 8 sia stato generato con il fine di garantire una concreta "maturità digitale" al minore, è riscontrabile come la gestione autonoma del consenso possa risultare ininfluente rispetto all'intento della norma.

La norma avrebbe dovuto garantire al minore la possibilità di utilizzare autonomamente i servizi digitali di uso comune, in conseguenza del discernimento in possesso dello stesso, dove invero, sin dall'entrata in vigore del Regolamento, è stata individuata l'anomala esistenza di un consenso prestato per un contratto non siglabile [45].

L'impossibilità attuale di fornire sul piano comunitario una valutazione economica al dato personale rende, di fatto, la norma debole. Non essendo possibile definire il valore del dato personale *ex ante* e per singolo utente, si

---

[43] Come evidenziato nei considerando 4 e 5 del GDPR: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica»;

«L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.»

[44] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 12 e ss.

[45] M. OROFINO, F. G. PIZZETTI, *op. cit.,* p. 27

lascerebbe di fatto al minore, in virtù della limitata capacità di agire concessa, la decisione relativa ad un'eventuale monetizzazione dei propri dati. Anche identificando il dato personale quale elemento patrimoniale – ipotesi che potrebbe portare ad una completa ridiscussione della norma - l'impossibilità di quantificare il prezzo del servizio e il valore del corrispettivo creerebbe non pochi problemi di diritto positivo, fuoriuscendo in tal caso il consenso dalla capacità di agire del minore.

Motivo per cui andrebbe valutata un'interpretazione restrittiva della definizione di servizio della società dell'informazione, inteso come da testo quale servizio «prestato normalmente dietro retribuzione», affiancandola ad ulteriori integrazioni che garantiscano una precisa identificazione delle eventualità in cui il minore potrebbe prestare il suo consenso (similmente al sistema di allegati utilizzato in diverse disposizioni comunitarie).

Per finalità di esempio, l'attività di trattamento effettuata attraverso dati forniti ad un social network differisce nettamente da una semplice visualizzazione di un sito web. In quanto, anche se in entrambi i casi fossero effettuate attività di profilazione dietro consenso dell'interessato, in ottica di gestione del rischio e per semplice differenza nella qualità dei dati erogati, la profilazione attraverso un social network manifesterebbe molti più pericoli per il minore. Tra l'altro le predette tipologie di trattamento spesso differiscono da quelle proposte da entità che incentrano la propria attività sull'erogazione di servizi a pagamento tradizionalmente intesi, concentrando, eventualmente, l'attenzione commerciale non sui dati ma su solo servizio offerto [46].

Non è perciò possibile effettuare un raggruppamento generale dei servizi della società dell'informazione, soprattutto in mancanza di una concorde valutazione comunitaria circa l'eventuale valore patrimoniale del dato personale, da cui diverse attività dipendono.

Per concludere, l'art. 8 risulta correttamente orientato, nella ratio, all'attuale realtà digitale. È comunque evidente che l'art. 8 patisca problemi di semplificazione che esulano dalle maglie dell'approccio basato sul rischio, essendo la norma di carattere permissivo e di applicazione statica.

[46] Come evidenziato in attenta dottrina, i pericoli derivanti da una disattenta prestazione del consenso, soprattutto in afferenza a precise tipologie di servizi, scaturiscono spesso da una percezione confusa del significato e della portata della protezione dei dati nella coscienza sociale. Infatti, il consenso al trattamento dei dati personali tende spesso a formarsi attraverso delle scorciatoie cognitive totalmente distaccate dal consenso informato e consapevole, ispirato alla razionalità, sfociando in comportamenti irrazionali. Da qui la conseguenza che il dato personale viene spesso scambiato per un discreto beneficio oppure per una minima ricompensa, aumentando di fatto i rischi per le fasce di utenza maggiormente meritevoli di tutela. I. A. CAGGIANO, *Results from The Legal and Ux&Hmi: A Persistent Critical Aspects on Consent and Its Real Role*, in L. GATT, R. MONTANARI, I. A. CAGGIANO, *Privacy and Consent a Legal and Ux&Hmi Approach for Data Protection*, 2021, pp. 119 ss.