Martínez Calvo J, 'I dati personali come corrispettivo contrattuale: appunti di diritto europeo' (2024) Special Issue EJPLT.
DOI:

EJPLT
ISSN 2704-8012

I dati personali come corrispettivo contrattuale: appunti di diritto europeo

Personal data as contractual consideration: notes on European law

JAVIER MARTÍNEZ CALVO
Professore Associato Associato di Diritto civile
Università di Saragozza

Abstract
La considerazione dei dati personali dei consumatori come corrispettivo nei contratti per la fornitura di contenuti e servizi digitali, come previsto dalla Direttiva (UE) 2019/770, solleva seri interrogativi sulla sua compatibilità con la normativa vigente in materia di protezione dei dati personali. Il Regolamento (UE) 2016/679 prevede che il consenso al trattamento dei dati debba essere dato liberamente, escludendo così qualsiasi richiesta coercitiva da parte del professionista in caso di inadempienza da parte del consumatore. Inoltre, tale consenso deve essere revocabile in qualsiasi momento, il che potrebbe costituire una violazione del contratto da parte del consumatore. Questo studio analizza la tensione tra queste normative, esplorando i possibili conflitti e cercando soluzioni per armonizzare la protezione dei dati personali con le nuove forme di transazioni nell'economia digitale.

[*] Questo articolo è stato presentato al Convegno interuniversitario "L'informazione e il diritto", 29-30-31 maggio 2024, Università Federico II, Orientale, Parthenope, Suor Orsola Benincasa, Napoli.
Comitato scientifico: Prof. Francesco Romeo (Uni Federico II Napoli). Prof.ssa Vania Maffeo (Uni Federico II Napoli), Prof.ssa Roberta Montinaro (Università degli Studi L'Orientale di Napoli), Prof. Roberto Carleo (UNI Parthenope); Prof. Agostino De Caro (Uni Molise), Prof. Giuseppe Di Chiara (Uni Palermo), Prof.ssa Lucilla Gatt (Uni Suor Orsola Benincasa), Prof. Mariano Menna (Uni Campania).

© 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/

Abstract
The consideration of consumer personal data as payment in contracts for the provision of digital content and services, as provided for in Directive (EU) 2019/770, raises serious questions as to its compatibility with current personal data protection law. Regulation (EU) 2016/679 provides that consent to data processing must be freely given, thus excluding any coercive demand by the entrepreneur in case of non-compliance by the consumer. Moreover, this consent must be revocable at any time, which could constitute a contractual breach by the consumer. This study explores the tension between these regulations, exploring possible conflicts and seeking solutions to harmonise the protection of personal data with new forms of transactions in the digital economy.

Keywords: Personal data; contractual consideration; digital contracts; consent; revocation

Summary: 1. Introduzione: la configurazione dei dati personali dei consumatori come corrispettivo contrattuale – 2. Carattere prevalente delle norme sulla protezione dei dati personali. – 3. Il consenso del consumatore come presupposto per la liceità del trattamento dei dati personali. – 3.1. Consenso libero, specifico, informato e inequivocabile. – 3.2. Consenso dei minori. – 3.3. Consenso al trattamento di dati particolarmente protetti. – 3.4. L'adempimento coercitivo come ostacolo al libero consenso. – 4. La revoca del consenso come inadempimento contrattuale. – 4.1. Il diritto dell'interessato di revocare liberamente il consenso. - 4.2. Revoca del consenso al trattamento dei dati dei minori. – 4.3. Conseguenze della revoca del consenso nell'ambito contrattuale. – 5. A titolo di riflessione finale.

1. Introduzione: la configurazione dei dati personali dei consumatori come corrispettivo contrattuale.*

I nostri modelli di consumo stanno cambiando a passi da gigante: Internet sta progressivamente diventando il canale principale per l'acquisto di beni e servizi, a scapito del commercio fisico, e i contenuti e i servizi digitali stanno diventando una parte sempre più importante del nostro carrello della spesa. Tanto che i contratti per la fornitura di contenuti e servizi digitali hanno assunto un ruolo più che significativo nell'economia dell'Unione Europea.

Il legislatore dell'UE non è rimasto impassibile di fronte all'espansione di questo fenomeno e si è messo al lavoro per cercare di dotare i contratti di fornitura di contenuti e servizi digitali di un quadro giuridico unitario che garantisca una maggiore certezza giuridica ai consumatori. A tal fine, da qualche tempo è stata emanata la Direttiva (UE) 2019/770 relativa a

* L'articolo è stato svolto nell'ambito del Gruppo di Ricerca Consolidato del Governo di Aragona "Ius Familiae" (RP. Carlos Martínez de Aguirre Aldaz), del Progetto di Ricerca del Ministero della Scienza, Innovazione e Università spagnolo (PID2023-153228NB-I00) "Nuevas vulnerabilidades: equilibrios y desequilibrios en el ordenamiento jurídico-privado" (RRPP. Mª Victoria Mayor del Hoyo/ Sofía de Salas Murillo), del Progetto di ricerca della Generalitat Valenciana CIGE/2023/71 "Cuestiones controvertidas en relación con el ejercicio de la capacidad jurídica por los y las menores de edad" (RP. Pedro Chaparro Matamoros) e dell'Instituto Universitario de Investigación en Empleo, Sociedad Digital y Sostenibilidad dell'Università di Saragozza (IEDIS).

determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (di seguito: Direttiva (UE) 2019/770) che, insieme alla sua gemella, la Direttiva (UE) 2019/771 relativa a determinati aspetti dei contratti di vendita di beni (di seguito: Direttiva (UE) 2019/771), ha cercato di fare chiarezza su questa nuova realtà che sta gradualmente trasformando la nostra concezione del mercato.

Una delle novità più importanti introdotte dalla Direttiva (UE) 2019/770 è stata la configurazione dei dati personali del consumatore come vero e proprio corrispettivo contrattuale nei contratti di fornitura di contenuti e servizi digitali, che ha permesso di ampliare il quadro di tutela del consumatore digitale online. Il problema è che ciò può entrare in conflitto con le disposizioni della legge sulla protezione dei dati personali, il che è particolarmente evidente per quanto riguarda il rilascio e la revoca del consenso al trattamento dei dati personali, che è proprio l'aspetto su cui mi concentrerò nelle pagine seguenti.…

2. Carattere prevalente delle norme sulla protezione dei dati personali.

Il GEPD aveva già messo in guardia dai problemi che possono derivare dalla configurazione del trasferimento dei dati personali come corrispettivo contrattuale nel parere sulla proposta di direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali del 25 giugno 2017, in cui evidenziava le difficoltà di conciliare le nuove norme con la legislazione vigente in materia di protezione dei dati personali; e ha proposto di disciplinare in modo unitario la materia nel 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 (di seguito: Regolamento (UE) 2016/679).

Tuttavia, il legislatore dell'UE ha scelto di ignorare i suddetti avvertimenti e raccomandazioni ed è andato avanti con l'elaborazione del testo che avrebbe dato origine alla Direttiva (UE) 2019/770, che ha portato a una situazione di dualità normativa nella regolamentazione dei contratti per la fornitura di contenuti e servizi digitali in cambio del trasferimento di dati personali. E, come ho già detto, questo ha condotto a una certa discordanza normativa.

Il problema principale che si presenta è che la disciplina del Regolamento (UE) 2016/679 sui dati personali non si concilia bene con la sua configurazione di corrispettivo contrattuale, cosa che, come ho già anticipato, è particolarmente evidente in relazione al rilascio e alla revoca del consenso al trattamento dei dati personali.

La Direttiva (UE) 2019/770 ha cercato di anticipare le difficoltà di conciliazione che possono esistere tra il contenuto del suo dispositivo e le disposizioni contenute nella legislazione sulla protezione dei dati personali. Lo ha fatto dichiarando la natura prevalente della normativa sulla protezione dei dati. Ciò emerge chiaramente dai considerando 37, 48 e 69:

Il primo di questi prevede che "(…) la presente direttiva fa salvi il regolamento (UE) 2016/679 (12) e la direttiva 2002/58/CE (13) del Parlamento europeo e del Consiglio. Tale quadro si applica ai dati personali trattati in

relazione ai contratti disciplinati dalla presente direttiva. Di conseguenza, i dati personali dovrebbero essere raccolti o altrimenti trattati esclusivamente nel rispetto del regolamento (UE) 2016/679 e della direttiva 2002/58/CE. In caso di conflitto tra la presente direttiva e il diritto dell'Unione in materia di protezione dei dati personali, quest'ultimo dovrebbe prevalere".

Il considerando 48 stabilisce che: "Il regolamento (UE) 2016/679 o qualsiasi altra fonte di diritto dell'Unione in materia di protezione dei dati dovrebbero applicarsi pienamente al trattamento dei dati personali in relazione ai contratti che rientrano nell'ambito di applicazione della presente direttiva. La presente direttiva non dovrebbe inoltre pregiudicare i diritti, gli obblighi e i rimedi extracontrattuali di cui al regolamento (UE) 2016/679 (…)".

Infine, il considerando 69 stabilisce che: "Nel caso in cui il consumatore fornisca dati personali all'operatore economico, quest'ultimo è tenuto a rispettare gli obblighi di cui al regolamento (UE) 2016/679 (…)".

I suoi articoli evidenziano anche la natura prevalente della legislazione esistente in materia di protezione dei dati. In particolare, l'articolo 3, paragrafo 7, stabilisce che "in caso di conflitto tra le disposizioni della presente direttiva e una disposizione di un altro atto dell'Unione che disciplina uno specifico settore o oggetto, la disposizione di tale altro atto dell'Unione prevale su quelle della presente direttiva" e l'articolo 3, paragrafo 8, stabilisce più specificamente che "il diritto dell'Unione in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione ai contratti di cui al paragrafo 1. In particolare, la presente direttiva fa salvo il regolamento (UE) 2016/679 e della direttiva 2002/58/CE. In caso di conflitto tra le disposizioni della presente direttiva e del diritto dell'Unione in materia di protezione dei dati personali, prevale quest'ultimo".

Partendo dalla premessa della natura prevalente del Regolamento (UE) 2016/679 rispetto alla Direttiva 2019/770, affronterò separatamente i due aspetti più controversi della configurazione dei dati personali dei consumatori come correspettivo contrattuale: inizierò con la questione del consenso al trattamento dei dati personali dei consumatori per poi passare alla sua eventuale revoca.

3. Il consenso del consumatore come presupposto per la liceità del trattamento dei dati personali.

3.1 Consenso libero, specifico, informato e inequivocabile.

Negli ultimi anni si è assistito ad un notevole aumento dei dispositivi connessi e ad una maggiore interazione con questi, a cui è corrisposto un proporzionale aumento dei dati generati. Si tratta di una tendenza destinata a crescere: secondo le stime previsionali della Commissione Europea, entro il 2025 il volume globale di dati aumenterà del 530%, per un valore economico di 829 milioni di euro[1].

[1] Analisi contenuta nella sezione istituzionale del sito della Commissione Europea, (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en) dedicato alla strategia europea sui dati.

Il considerando 24 della direttiva (UE) 2019/770 afferma che "il diritto dell'Unione in materia di protezione dei dati personali prevede un elenco esaustivo di fondamenti giuridici per il trattamento lecito dei dati personali", per cui il trattamento dei dati personali è legittimo solo quando si applica una di queste circostanze.

Tuttavia, i motivi giuridici specifici per il trattamento dei dati personali non sono coperti dalla Direttiva (UE) 2019/770, poiché, come indicato nel suo Considerando 38, "La presente direttiva non dovrebbe disciplinare le condizioni per il trattamento lecito dei dati personali, dal momento che tale questione è specificamente disciplinata dal regolamento (UE) 2016/679. Di conseguenza, qualsiasi trattamento di dati personali in relazione a contratti rientranti nell'ambito di applicazione della presente direttiva è lecito solo se è conforme alle disposizioni del regolamento (UE) 2016/679 relativo ai fondamenti giuridici per il trattamento dei dati personali. Quando il trattamento dei dati personali si basa su un consenso, segnatamente a norma dell'articolo 6, paragrafo 1, lettera a), del regolamento (UE) 2016/679, si applicano le disposizioni specifiche di tale regolamento, comprese quelle relative alle condizioni per valutare se il consenso sia stato o meno liberamente prestato. La presente direttiva non dovrebbe disciplinare la validità del consenso prestato (…)".

Sarà quindi necessario fare riferimento al Regolamento (UE) 2016/679, che all'art. 6.1 a) considera lecito il trattamento dei dati personali quando "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità". È proprio questo l'aspetto che ci interessa in questo scritto, perché nel tipo di contratto che sto analizzando, il consenso del consumatore costituisce il presupposto per la liceità del trattamento dei suoi dati personali da parte del professionista, che in questo caso assume il ruolo di titolare del trattamento.

La validità del consenso al trattamento dei dati personali è subordinata al soddisfacimento di una serie di requisiti, come stabilito dall'articolo 4, paragrafo 11, del Regolamento (UE) 2016/679, che prevede che il consenso consiste in "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".

Come si può notare, uno dei requisiti affinché il consenso sia considerato valido è che sia dato liberamente. E nel valutare questo aspetto, l'art. 7.4 del Regolamento (UE) 2016/679 tiene in particolare conto "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". Un'idea prevista anche nel considerando 42: "il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio".

Il problema è che, in base a quanto detto, può sorgere il dubbio che nel tipo di contratti che stiamo analizzando il consenso possa essere considerato liberamente prestato. Occorre tenere presente che il corrispettivo pagato dal consumatore in cambio della fornitura di contenuti e servizi digitali consiste

proprio nel trasferimento dei suoi dati personali, per cui il rilascio del consenso al loro trattamento è inevitabile se si vuole accedere a tali contenuti o servizi.

Data la natura prevalente del Regolamento (UE) 2016/679 rispetto alla Direttiva (UE) 2019/770, il consumatore può rifiutare il consenso al trattamento dei propri dati personali, ma avrebbe comunque il diritto di acquistare i contenuti o i servizi digitali in questione?

Una risposta affermativa a questa domanda equivarrebbe a far ricadere sul consumatore la decisione sulla gratuità o onerosità del contratto, cosicché se il consumatore rifiuta di dare il consenso, il contratto, inizialmente oneroso, diventerebbe gratuito, in quanto il consumatore non verserebbe alcun corrispettivo in cambio dell'acquisizione dei contenuti o servizi digitali[2].

Forse la spiegazione potrebbe essere che, nei casi in cui il trasferimento dei dati personali del consumatore sia una delle clausole del contratto, si dovrebbe ritenere che il rilascio del consenso sia una condizione necessaria per l'esecuzione del contratto nei termini previsti dall'articolo 7 del Regolamento (UE) 2016/679. Tuttavia, questa interpretazione solleva a mio avviso seri dubbi, in quanto sembra che quando la legge dice che il trattamento deve essere necessario per la prestazione del servizio, lo faccia piuttosto in una prospettiva tecnica, per cui si riferirebbe a quei casi in cui il professionista ha bisogno di tali dati per poter fornire al consumatore il contenuto digitale o i servizi in questione.

Un altro requisito perché il consenso sia valido è che deve essere specifico, informato e non ambiguo. Ciò esclude ovviamente il consenso presunto[3] e, a mio avviso, anche quello tacito. In effetti, ritengo che questa posizione sia rafforzata dalle disposizioni del considerando 32 del Regolamento (UE) 2016/679, per cui: "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. (…)". E, a tal fine, il Considerando 42 del Regolamento (UE) 2016/679 prevede che all'interessato debba essere fornito "(…) una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali (…)". Inoltre, l'art. 7.2 del Regolamento (UE) 2016/679 stabilisce che "se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre

[2] M.I. Domínguez Yamasaki, *El tratamiento de datos personales como prestación contractual. Gratuidad de contenidos y servicios digitales a elección del usuario*, in *Revista de derecho privado*, 2020, IV, 110.
[3] A. Martínez Rojas, *Principales aspectos del consentimiento en el reglamento general de protección de datos de la Unión Europea*, in *Revista Aranzadi de derecho y nuevas tecnologías*, 2016, XLII, 62.

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".

3.2 Consenso dei minori.

Nel caso dei minori, il Regolamento (UE) 2016/679 prevede alcune regole specifiche per la validità del consenso. In particolare, l'art. 8.1 prevede che "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. 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". La giustificazione è che, come previsto dal 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".

Tuttavia, l'articolo 8, paragrafo 1, del Regolamento (UE) 2016/679 consente agli Stati membri di fissare un'età inferiore a 16 anni per consentire ai minori di prestare il proprio consenso al trattamento dei dati personali, purché tale età non sia inferiore a 13 anni.

A titolo di esempio, sia il legislatore spagnolo che quello italiano hanno deciso di avvalersi della facoltà concessa dal Regolamento (UE) 2016/679 e hanno fissato l'età minima del consenso dei minori per il trattamento dei loro dati personali al di sotto dei 16 anni:

Nel caso dell'Italia, il legislatore ha scelto di abbassare l'età di 16 anni stabilita dal diritto dell'Unione e di fissarla a 14 anni (art. 2 quinquies del "Codice in materia di protezione dei dati personali", come modificato dal Decreto Legislativo 10 agosto 2018, n. 101), in contrasto con il parere dell'Autorità garante per l'Infanzia e l'Adolescenza, più propensa a rispettare il limite di età di 16 anni (anche se in dottrina si sono levate voci favorevoli alla riduzione a 13 anni [4]). Sembra che uno degli scopi principali di questo abbassamento dell'età sia stato quello di conciliare le disposizioni contenute nella normativa sulla protezione dei dati personali con altre disposizioni dell'ordinamento italiano [5], come la legge 4 maggio 1983, n. 184, sulla "Disciplina dell'adozione e dell'affidamento dei minori", che fissa a 14 anni l'età

[4] G. Boccia Artieri, *Privacy dei minori sui social, con il GDPR: così tuteliamo i loro interessi*, in *Agenda Digitale*, 2018. Consultabile al sito: https://www.agendadigitale.eu/sicurezza/privacy-dei-minori-sui-social-con-il-gdpr-cosi-tuteliamo-i-loro-interessi.

[5] L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Europa e Diritto Privato*, 2020, I, 5.

del consenso per l'adozione, o la legge 29 maggio 2017, n. 71, sulla "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", che stabilisce anche i 14 anni come età minima per richiedere la cancellazione di contenuti offensivi e lesivi della propria dignità (senza la necessità di informare i genitori). Ciò ha posto fine a un periodo di incertezza sulla questione del consenso al trattamento dei dati personali dei minori, in quanto, in assenza di un'espressa regolamentazione in materia, non vi era accordo sul fatto che il consenso potesse o meno essere dato dal minore stesso[6].

Nel caso della Spagna, l'art. 7.1 della Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (di seguito: LOPD) anche riduce il limite di età a 14 anni, stabilendo che "el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años" (il trattamento dei dati personali di un minorenne può basarsi sul suo consenso solo se ha più di 14 anni), pur derogando a questa regola in alcuni casi, e specificamente in "los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento" (quei casi in cui la legge richiede l'assistenza dei titolari della potestà genitoriale o della tutela per la conclusione dell'atto o del negozio giuridico nel contesto del quale si richiede il consenso al trattamento). La soluzione adottata dal legislatore spagnolo su questo punto sembra ragionevole, in quanto permette di conciliare le disposizioni sulla protezione dei dati con le norme generali sulla capacità dei minori: in particolare, con gli articoli 162 e 1263.1 del Codice Civile. Il primo esclude dalla rappresentanza dei genitori "los actos relativos a los derechos de la personalidad que el hijo, de acuerdo con su madurez, pueda ejercitar por sí mismo" (gli atti relativi ai diritti della personalità che il minore, secondo la sua maturità, può esercitare da solo), mentre il secondo stabilisce che "no pueden prestar consentimiento los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales" (il minore non emancipato non può prestare il consenso, salvo che per i contratti che la legge gli consente di stipulare da solo o con l'assistenza dei suoi rappresentanti e per quelli relativi a beni e servizi della vita quotidiana adeguati alla sua età secondo gli usi sociali). Sembra che ci troviamo proprio in uno dei casi in cui la legge consente ai minori di agire per conto proprio, a condizione che abbiano compiuto 14 anni e che non vi siano altre disposizioni di legge che fissino un limite diverso per lo specifico atto o negozio giuridico nell'ambito del quale viene richiesto il consenso al trattamento dei dati personali del minore. In ogni caso, il progetto di legge per la protezione dei minori negli ambienti digitali recentemente presentato dal governo spagnolo intende modificare il precetto

[6] A favore di questa possibilità: V. CORREIRO, *Privacy del minore e potestà dei genitori*, in *Rassegna di Diritto civile*, 2004, IV, 1016; e S. PATTI, *Commento all'art. 23: Consenso,* 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 e F.D. BUSNELLI, Padova, 2007, 544.

citato e innalzare l'età per il rilascio del consenso digitale a 16 anni, per cui è possibile che questa norma cambi nel prossimo futuro.

Tuttavia, se il consenso al trattamento dei dati personali viene dato nel contesto della conclusione di un altro tipo di contratto, la validità di tale consenso richiederà non solo che il minore abbia raggiunto l'età di 14 anni, ma anche che abbia la capacità sufficiente secondo la legge per stipulare tale contratto[7]. Questo sembra essere ciò a cui l'art. 8.3 del Regolamento (UE) 2016/679 pare riferirsi quando afferma che "il paragrafo 1 non pregiudica 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". Pertanto, se il minore ha l'età per dare il consenso digitale ma non quella per stipulare il relativo contratto, quest'ultimo può essere annullato nonostante la liceità del trattamento[8].

Inoltre, il fatto che i minori che hanno compiuto 14 anni possano acconsentire al trattamento dei loro dati personali da parte degli operatori dei diversi servizi Internet non significa che le loro azioni su Internet siano al di fuori del controllo dei genitori. Questo potere di controllo è inerente all'esercizio della responsabilità genitoriale, che nel caso della legge italiana (art. 315-bis c.c.) e di quella spagnola (art. 154.2.1 c.c.) comprende il diritto/dovere di educare e istruire i figli.

Come già detto, nel caso di minori di 14 anni, il consenso deve essere prestato dai loro rappresentanti legali. Nel caso della legge italiana, ciò è espressamente previsto dall'art. 2 quinquies (1) del 'Codice in materia di protezione dei dati personali': "Il trattamento dei dati personali del minore di eta' inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, e' lecito a condizione che sia prestato da chi esercita la responsabilita' genitoriale" e, nel caso della legge spagnola, dall'art. 7.2 LOPD: "el tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela" (il trattamento dei dati dei minori di 14 anni, basato sul consenso, è lecito solo se viene dato il consenso del titolare dell'autorità parentale o della tutela, nella misura determinata dai titolari dell'autorità parentale o della tutela).

3.3 Consenso al trattamento di dati particolarmente protetti.

È opportuno fare un breve accenno ai dati personali specialmente protetti, che sono dati che non possono essere trattati in nessun caso, cioè nemmeno con il consenso dell'interessato. Tali dati comprendono quelli di cui all'articolo 9, paragrafo 1, del Regolamento (UE) 2016/679: "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

[7] S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Rimini, 2016, 107 e DEL NINNO, *Il rapporto genitori-figli minori nella prospettiva della normativa sul trattamento dei dati personali*, in *Rev. U. of Louisville*, 2016, I, 75.

[8] V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO e V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, 23.

biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

Tuttavia, l'esclusione del trattamento di tali dati da parte della legislazione europea non è assoluta, in quanto la suddetta disposizione prosegue affermando, al secondo punto, che il suddetto divieto di trattamento è esentato quando "l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche". Ma poi introduce una sorta di deroga all'eccezione, consentendo agli Stati membri di escludere la possibilità che i dati personali specialmente protetti possano essere trattati con il consenso dell'interessato: "salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1", quindi in pratica è una questione lasciata ai singoli Stati.

Nel caso della Spagna, il legislatore ha scelto di escludere in ogni caso la possibilità che i dati specialmente protetti possano essere oggetto di trattamento, in quanto l'art. 9.2 LOPD prevede che "a los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico" (ai fini dell'articolo 9.2.a) del Regolamento (UE) 2016/679, al fine di evitare situazioni discriminatorie, il solo consenso dell'interessato non è sufficiente per revocare il divieto di trattamento dei dati la cui finalità principale è l'identificazione dell'ideologia, dell'appartenenza sindacale, della religione, dell'orientamento sessuale, delle convinzioni personali o dell'origine razziale o etnica). La legge italiana, invece, non contiene una disposizione di questo tipo, ma la Corte di Cassazione ha sottolineato che nel trattamento di dati particolarmente protetti si deve garantire che l'interessato non sia identificabile (cfr. Cass., SS.UU., 27 dicembre 2017, n. 30981 e Cass. civ., sez. I, 19 maggio 2014 n. 10947).

3.4 L'adempimento coercitivo come ostacolo al libero consenso.

Il consumatore viola il suo obbligo se non fornisce al professionista i suoi dati personali nei modi e nei tempi concordati nel contratto o se, dopo averli forniti al professionista, questi sono inesatti o incompleti.

Il problema è che la Direttiva (UE) 2019/770 non ha previsto espressamente l'eventualità che il consumatore non adempia al suo obbligo, né le possibili conseguenze di tale inadempienza, il che ci costringe a rivolgerci alle norme generali sui contratti per risolvere la questione. A questo proposito, trattandosi di un contratto di natura onerosa e sinallagmatica, se si tiene conto dell'art. 1453 c.c., la parte che ha adempiuto alla propria parte di contratto (in questo caso il professionista) "può a sua scelta chiedere l'adempimento o la risoluzione del contratto, salvo, in ogni caso, il risarcimento del danno" (stessa regola prevista dall'art. 1124.2 del Codice civile spagnolo: "el perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos" — la parte lesa

può scegliere tra l'adempimento o la risoluzione dell'obbligazione, con danni e interessi in entrambi i casi—).

Tuttavia, mi sembra quantomeno discutibile che l'art. 1453 c.c. e il potere che concede alla parte lesa per l'inadempimento della controparte possa essere applicabile a questo tipo di contratto. Infatti, se il professionista optasse per l'esecuzione coattiva del contratto nei termini concordati, il consumatore sarebbe obbligato a prestare il consenso al trattamento dei suoi dati personali, il che sarebbe in contrasto con l'art. 4.11 del Regolamento (UE) 2016/679, che, come abbiamo già visto, richiede che il consenso sia prestato liberamente. Tuttavia, data la natura prevalente del Regolamento (UE) 2016/679 rispetto alla Direttiva (UE) 2019/770, mi sembra di capire che il consumatore non potrebbe essere costretto ad adempiere coercitivamente al suo obbligo.

Di conseguenza, ritengo che ci sia un solo rimedio possibile a disposizione del professionista nel caso in cui il consumatore non rispetti l'obbligo di trasferire i suoi dati personali per il trattamento: la risoluzione del contratto.

4. La revoca del consenso come inadempimento contrattuale.

4.1 Il diritto dell'interessato di revocare liberamente il consenso.

Quando si tratta di un contratto concluso per lo scambio di contenuti personali o di servizi per il trasferimento di dati personali, il consumatore assume l'obbligo di consentire il trattamento dei suoi dati personali da parte del professionista (in quanto si tratta della prestazione che deve fornire nel contratto), e pertanto non sembra avere il diritto di revocare il proprio consenso al trattamento dei dati in questione in un momento successivo. Infatti, ammettere la possibilità per il consumatore di revocare il proprio consenso al trattamento dei dati personali in qualsiasi momento equivale a lasciare nelle sue mani la decisione sull'esecuzione del contratto.

Il problema è che la normativa sulla protezione dei dati riconosce il diritto dell'interessato di revocare il consenso inizialmente prestato. A questo proposito, il Considerando 42 del Regolamento (UE) 2016/679 prevede che "il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio", e, in caso di dubbi, l'art. 7.3 del Regolamento (UE) 2016/679 prevede espressamente che "l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento" (il che ovviamente non pregiudica la liceità del trattamento basato sul consenso prima della sua revoca: cfr. art. 7.3 del Regolamento (UE) 2016/679). Di fatto, sembra che si tratti di un diritto assoluto e irrinunciabile[9]. E la natura assoluta del diritto di revocare il consenso al trattamento dei dati personali impedirebbe di sottoporlo a esclusioni o limitazioni, poiché qualsiasi

[9] L. AGUILERA RUIZ, *La revocación del consentimiento al tratamiento como incumplimiento esencial en el contrato de suministro de contenidos y servicios digitales a cambio de datos personales regulado en la Directiva (UE) 2019/770*, in M.T. ALONSO PÉREZ e E. HERNÁNDEZ SÁINZ, *Servicios digitales, condiciones generales y transparencia*, Navarra, 2020, 125.

ostacolo alla libera revoca del consenso sarebbe contrario alla legge sulla protezione dei dati personali.

In base a quanto sopra, e se si tiene conto della natura prevalente del Regolamento (UE) 2016/679 rispetto alla Direttiva (UE) 2019/770, si dovrebbe concludere che il fatto che il trasferimento dei dati personali del consumatore sia una delle clausole del contratto di fornitura di contenuti e servizi digitali non escluderebbe o limiterebbe il diritto del consumatore di revocare liberamente il consenso inizialmente prestato in qualsiasi momento. Infatti, il considerando 39 della Direttiva (UE) 2019/770 afferma espressamente che "il diritto alla cancellazione e il diritto del consumatore di revocare il consenso al trattamento dei dati personali dovrebbero applicarsi pienamente anche in relazione ai contratti disciplinati dalla presente direttiva. Il diritto del consumatore di risolvere il contratto conformemente alla presente direttiva non dovrebbe pregiudicare il diritto del consumatore di revocare, ai sensi del regolamento (UE) 2016/679, un eventuale consenso prestato per il trattamento dei dati personali del consumatore". Però, come ho sottolineato, dal punto di vista del diritto contrattuale, ciò significa lasciare a una delle parti (in questo caso il consumatore) la possibilità di decidere se eseguire o meno il contratto.

Si potrebbe forse pensare che, in realtà, il diritto dell'interessato di revocare il consenso dato per il trattamento dei suoi dati personali si tradurrebbe in ambito contrattuale in una sorta di diritto di recesso sine die a favore del consumatore. In tal modo, il consumatore potrebbe liberamente revocare il proprio consenso in qualsiasi momento e ciò non costituirebbe alcun tipo di violazione da parte sua nella dimensione contrattuale.

A mio avviso, non c'è dubbio che, se la revoca del consenso al trattamento dei dati personali avviene entro il periodo di 14 giorni previsto dall'articolo 9 della Direttiva (UE) 2011/83 sui diritti dei consumatori (di seguito: Direttiva (UE) 2011/83), tale revoca potrebbe essere tradotta in ambito contrattuale come esercizio del diritto di recesso del consumatore. Ciò a condizione, tuttavia, che siano soddisfatti i requisiti rigorosi per il diritto di recesso nei contratti per contenuti digitali o servizi forniti online, come stabilito dalla Direttiva.

Tuttavia, se i suddetti requisiti non sono soddisfatti o se il periodo di 14 giorni previsto dalla normativa per l'esercizio del diritto di recesso è già trascorso, mi sembra più discutibile che il consumatore possa recedere unilateralmente dal contratto sotto la tutela di un presunto diritto di recesso sine die o ad nutum[10]. Questo diritto di recesso manca di copertura giuridica, in quanto non solo non esiste un riferimento specifico a questa possibilità nella legge, ma anche il carattere molto restrittivo con cui la Direttiva (UE) 2011/83 ha configurato il diritto di recesso sembra escludere qualsiasi tentativo di interpretazione estensiva dello stesso. Va ricordato che, se tale possibilità fosse ammessa, il consumatore sarebbe libero di recedere dal contratto una volta ottenuto il beneficio previsto dal contenuto digitale o dai servizi in questione (ad esempio, la visione di un film o la lettura di un e-book).

Pertanto, ritengo che questi casi in cui il consumatore revoca il consenso inizialmente dato per il trattamento dei suoi dati personali debbano essere

[10] R. SÁNCHEZ LERÍA, *El contrato de suministro de contenidos digitales a cambio de datos personales: a propósito de la propuesta de directiva 634/2015 de 9 de diciembre de 2015*, in *Revista Aranzadi de derecho patrimonial*, 2018, XLV, 22.

trattati come una violazione del contratto, in quanto impediscono al professionista di continuare il trattamento dei suoi dati personali. Occorre tenere presente che, una volta che il consumatore ha revocato il consenso, il professionista non potrà continuare a trattare i suoi dati personali, per cui le sue richieste non saranno soddisfatte. Questo perché il professionista normalmente ottiene un ritorno economico dai dati personali del consumatore non trattandoli sporadicamente, ma su base continuativa, mettendoli insieme ai dati di altri utenti e persino trasferendoli a terzi. In effetti, la proposta di Direttiva del Consiglio relativa al sistema comune d'imposta sui servizi digitali applicabile ai ricavi derivanti dalla fornitura di taluni servizi digitali fa esplicito riferimento al possibile trasferimento dei dati dei consumatori a terzi, affermando nella sua relazione che "(...) le imprese digitali possono ricavare dati relativi alle attività degli utenti sulle interfacce digitali, cosa che di norma serve a fornire pubblicità mirate a tali utenti, o possono trasmetterli a terzi a titolo oneroso (...)"; il che, a quanto mi risulta, richiederà sempre il consenso dell'interessato, poiché in caso contrario verrebbe violato l'obbligo di riservatezza cui è soggetto il responsabile del trattamento dei dati personali, ai sensi dell'articolo 5, paragrafo 1, lettera f), del Regolamento (UE) 2016/679.

4.2. Revoca del consenso al trattamento dei dati dei minori.

Abbiamo già visto sopra che l'interessato può revocare il consenso in qualsiasi momento e chiedere la cessazione del trattamento, possibilità che nel caso dei minori è rafforzata grazie alle disposizioni dell'art. 17. 1 f) del Regolamento (UE) 2016/679, che non solo conferisce ai minori la facoltà di revocare il consenso, ma anche il diritto di chiedere la cancellazione dei dati personali che li riguardano, senza che sia necessaria una violazione della normativa sulla protezione dei dati personali da parte del titolare del trattamento. Inoltre, il Considerando 65 del Regolamento (UE) 2016/679 contiene una disposizione che sembra anch'essa pensata per questo scenario: "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. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore".

4.3. Conseguenze della revoca del consenso nell'ambito contrattuale.

Per quanto riguarda i possibili effetti della revoca del consenso e della conseguente violazione del contratto, essi non sono stati espressamente previsti dalla normativa, in quanto la Direttiva (UE) 2019/770 si limita ad affermare, nel considerando 40, che "la presente direttiva non dovrebbe disciplinare le conseguenze per i contratti contemplati dalla presente direttiva nel caso in cui il consumatore revochi il consenso al trattamento dei dati personali del consumatore. Tali conseguenze dovrebbero rimanere riservata al diritto nazionale". Pertanto, il riferimento fatto dalla Direttiva (UE) 2019/770 ci ricondurrebbe alle norme generali previste dal Codice Civile in materia di

contratti e, in particolare, a quelle specificamente previste per i casi di violazione degli obblighi reciproci.

Si è però già visto, affrontando i possibili rimedi a disposizione del professionista in caso di inadempimento da parte del consumatore, che il potere attribuito dall'art. 1453 c.c. alla parte che adempie alla propria parte del contratto di scegliere tra esigere l'adempimento dell'obbligazione nei termini rigorosi in cui è stata pattuita o risolvere il contratto non può essere applicato a questo tipo di contratto. L'art. 4.11 del Regolamento (UE) 2016/679 impedisce al professionista di richiedere al consumatore di adempiere coercitivamente alla sua obbligazione, richiedendo che il consenso al trattamento dei dati personali sia prestato liberamente; inoltre, l'art. 7.3 del Regolamento (UE) 2016/679 riconosce il diritto dell'interessato di revocare il proprio consenso in qualsiasi momento. Pertanto, ancora una volta, l'unica possibilità per il professionista è quella di ricorrere alla risoluzione del contratto.

Come si può notare, fino a questo punto, le conseguenze previste dalla normativa per i casi in cui il consumatore revochi il consenso inizialmente prestato per il trattamento dei suoi dati sono le stesse previste per le altre violazioni. In tutti i casi citati, l'unico rimedio a disposizione del professionista in caso di violazione da parte del consumatore sarà la risoluzione del contratto, senza poter richiedere al consumatore il rispetto delle condizioni pattuite nel contratto, poiché ciò significherebbe imporgli di prestare il consenso al trattamento dei suoi dati personali, che non potrebbe più essere considerato come liberamente prestato, nei termini richiesti dalla normativa sulla protezione dei dati.

Esiste tuttavia una conseguenza specifica che sarà applicabile nella maggior parte delle violazioni dei consumatori, ma non in quelle dovute alla revoca del consenso al trattamento dei dati personali. Mi riferisco alla possibilità di stabilire un risarcimento a carico del consumatore per i danni causati al professionista in conseguenza della revoca del consenso e della conseguente violazione del contratto. A questo proposito, abbiamo già visto che il Considerando 42 del Regolamento (UE) 2016/679 stabilisce espressamente che "il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio".

5. A titolo di riflessione finale.

La configurazione dei dati personali dei consumatori come corrispettivo nei contratti per la fornitura di contenuti e servizi digitali solleva problemi in relazione al rilascio e alla revoca del consenso al trattamento dei loro dati personali. Problemi che derivano dalla necessità di coordinare le norme stabilite in due ambiti diversi: la protezione dei consumatori e quella dei dati personali.

Il fatto che il contratto sia classificato come oneroso significa che il consumatore è vincolato dal contratto e sorge l'obbligo di adempiere alla prestazione a cui si è impegnato. Tuttavia, ciò può entrare in conflitto con le

disposizioni della normativa in materia di protezione dei dati personali, che prevede che il consenso al trattamento dei dati debba essere prestato liberamente, il che impedirebbe al professionista di esigerlo in modo coatto. Va notato che il Regolamento (UE) 2016/679, che stabilisce le norme sulla concessione e la revoca del consenso al trattamento dei dati personali, prevale sulla Direttiva (UE) 2019/770. Pertanto, in caso di violazione da parte del consumatore, l'unica opzione a disposizione del professionista sarebbe la risoluzione del contratto.

Inoltre, la legislazione sulla protezione dei dati prevede che il consenso al trattamento dei dati personali debba essere liberamente revocabile. Il problema è che tale revoca costituirebbe di per se una violazione del contratto da parte del consumatore.

Ad ogni modo, nei casi in cui la violazione sia causata dalla revoca del consenso da parte del consumatore al trattamento dei propri dati personali, non potrà essere stabilito alcun tipo di risarcimento a carico del consumatore, in quanto la normativa sulla protezione dei dati rifiuta espressamente che il titolare dei dati possa sopportare qualsiasi tipo di danno in conseguenza della revoca del consenso.