Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Antigua Universidad s/n - Apdo. 28
20560 Oñati - Gipuzkoa (Spain)
opo@iisj.es / http://opo.iisj.net

L'adeguamento dell'ordinamento italiano al regolamento generale sulla protezione dei dati: qualche riflessione nella prospettiva del diritto internazionale privato e processuale

(The adaptation of the Italian legal system to the general data protection regulation: some reflections in the perspective of private and procedural international law)

OÑATI SOCIO-LEGAL SERIES FORTHCOMING: LEGAL CULTURE AND EMPIRICAL RESEARCH
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL/0000-0000-0000-1329
RECEIVED 18 SEPTEMBER 2022, ACCEPTED 23 SEPTEMBER 2022, FIRST-ONLINE PUBLISHED 28 SEPTEMBER 2022

LIVIO SCAFFIDI RUNCHELLA*

Riassunto

Il regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali intende garantire certezza del diritto e trasparenza per le persone fisiche e gli operatori economici. Il presente lavoro, muovendo dall'esame di alcune norme della legge italiana di adeguamento al regolamento, svolge alcune riflessioni sul tema nella prospettiva del diritto internazionale privato. L'indagine si inserisce in un quadro assai complesso poiché le nuove tecnologie mettono costantemente alla prova il processo legislativo, così come l'interpretazione e l'applicazione delle pertinenti disposizioni di legge. Inoltre, i dati personali nel mondo online non sono vincolati da confini geografici: la natura "ubiqua" di internet rende problematico localizzare le situazioni giuridiche che vengono di volta in volta in considerazione, rendendo difficile individuare il diritto applicabile nelle situazioni transfrontaliere.

Parole chiave

Regolamento (UE) n. 2016/679; Codice italiano in materia di dati personali; autorità di controllo e autorità giurisdizionali; consenso dei minori, risarcimento danni

Abstract

Regulation (EU) no. 2016/679 concerning the protection of individuals with regard to the processing of personal data, aims to ensure legal certainty and transparency for individuals and economic operators. This work, proceeding from the

* Assegnista di Ricerca di Diritto Internazionale, presso l'Università degli Studi di Messina. Email: lscaffidirunchella@unime.it

examination of some provisions of the Italian law for the adaptation to the regulation, undertakes some reflections on the subject in the perspective of private international law. The essay forms part of a very complex framework as new technologies constantly put the legislative process as well as the interpretation and application of the relevant legal provisions to the test. Furthermore, personal data in the online world are not bound by geographical boundaries: the "ubiquitous" nature of the internet makes it difficult to locate the legal situations that come under consideration from time to time, making it difficult to identify the applicable law in cross-border situations.

Key words

Regulation (EU) n. 2016/679; Italian Code regarding personal data; supervisory authority and jurisdictional authorities; consent of minors; compensation for damages

Table of contents

1. Osservazioni introduttive: il GDPR quale rimedio alla frammentazione giuridica

Com'è noto, il Regolamento (UE) 2016/679 (c.d. Regolamento Generale sulla Protezione dei Dati - GDPR),[1] divenuto applicabile dal 25 maggio del 2018, si colloca all'interno dell'ambiziosa strategia dell'Unione europea diretta a realizzare lo "spazio unico europeo di dati".[2] In un'economia sempre più basata sul trattamento di dati, la loro circolazione è considerata un fattore di innovazione e di crescita in grado di determinare rilevanti e concreti benefici per cittadini, imprese e pubbliche amministrazioni.[3] Secondo tale visione, il GDPR rappresenta un impulso allo sviluppo dell'economia dei dati perché, oltre a promuoverne la libera circolazione, rafforza il diritto delle persone fisiche alla tutela dei dati personali, aumentando la fiducia nella transizione digitale in corso.[4]

Il GDPR rappresenta, inoltre, una risposta alle trasformazioni radicali, intervenute nel mondo digitale sin dalla metà degli anni novanta, che hanno reso la precedente disciplina, cioè la Direttiva 95/46/CE (c.d. Direttiva Dati), non più adeguata. Tale strumento, risalente al 1995, era stato infatti adottato in un'epoca in cui soltanto un'esigua minoranza di cittadini europei utilizzava internet per le proprie attività quotidiane.

Fra le ragioni che hanno condotto all'adozione del GDPR va anche annoverata l'esigenza di rimpiazzare la direttiva con una fonte regolamentare. Sotto la vigenza della Direttiva dati, la prassi rivelava infatti l'esistenza di una certa frammentazione giuridica in materia, ascrivibile principalmente alla divergenza fra le varie leggi nazionali di recepimento dello strumento. Per tale ragione, il legislatore europeo non ha ritenuto

[1] 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, in GUUE del 4 maggio 2016, L 119, 1-88. In letteratura si suole fare riferimento al regolamento anche con l'acronimo GDPR (*General Data Protection Regulation*). Sugli obiettivi perseguiti dal GDPR, si veda, anche per ulteriori riferimenti bibliografici, Piñar Mañas (2018).

[2] Come indicato nella Comunicazione della Commissione europea del 6 maggio 2015 dal titolo *Strategia per il Mercato Unico Digitale in Europa* (COM/2015/0192 final), il mercato unico digitale si fonda su tre pilastri: migliorare l'accesso ai beni e servizi digitali in tutta Europa per le imprese e per i consumatori; creare un contesto favorevole e parità di condizioni affinché le reti digitali e i servizi innovativi possano svilupparsi; massimizzare il potenziale di crescita dell'economia digitale.

[3] Per rendersi conto della portata del fenomeno basti considerare i dati riportati nella Comunicazione della Commissione europea del 19 febbraio 2020, dal titolo *Una strategia europea per i dati* (COM/2020/66 final).

[4] Nel territorio dell'Unione europea gli strumenti in materia sono funzionali alla realizzazione del diritto fondamentale alla protezione dei dati, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE) e dai Trattati, in particolare, dall'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE). La prima delle due disposizioni specifica che il diritto alla protezione dei dati personali implica la possibilità del titolare del diritto di accedere ai propri dati personali, di ottenerne la rettifica e impone che questi siano trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo. Il fatto che la CDFUE distingua il diritto al rispetto per la vita privata e familiare, di cui all'art. 7, dal diritto alla protezione dei dati personali, esplicitamente sancito dall'art. 8 riflette l'accresciuta preoccupazione dell'Unione europea in materia. Dal canto suo, il Trattato di Lisbona del 2007 non solo ha sancito il carattere vincolante della CDFUE, ma ha anche introdotto, per il tramite dell'art. 16 del TFUE, una nuova base giuridica per la protezione dei dati personali che interessa tanto il settore privato quanto il settore pubblico. Per un'analisi di tali disposizioni vedasi, per tutti, Piroddi (2014a, 2014b). Per una ricostruzione dell'emersione di tale diritto nell'ordinamento dell'Unione europea e della sua trasfigurazione in diritto fondamentale si veda González Fuster (2014).

conveniente procedere a un aggiornamento, finanche radicale, della disciplina per mezzo di una nuova direttiva, preferendo invece ricorrere al regolamento, ovvero a uno strumento di portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile all'interno degli ordinamenti nazionali. Tale opzione evidenzia l'avvertito bisogno di garantire coerenza e di prevenire il prodursi di disparità a livello nazionale, anche sotto il profilo sanzionatorio.

Nonostante la chiara individuazione di dette esigenze, il GDPR lascia ampio spazio agli Stati membri, consentendo loro di ampliare, limitare o specificare la disciplina dell'Unione europea. Più precisamente, in primo luogo, il GDPR impone ai legislatori nazionali di intervenire per adottare misure esecutive. In secondo luogo, il GDPR consente agli Stati membri di limitare o ampliare l'ambito di applicazione di molte delle sue disposizioni e finanche di derogarvi. In terzo luogo, la disciplina contenuta nello strumento, anche quando non rinvia al diritto degli Stati membri, per molti profili non ha carattere esaustivo come, ad esempio, in tema di termini di prescrizione o di criteri per determinare il risarcimento del danno. Tutti questi spazi di intervento concessi ai legislatori nazionali sembrano voler realizzare un compromesso tra l'unificazione della disciplina in materia e il riconoscimento delle particolarità del diritto degli Stati membri.

Nel quadro dell'ordinamento italiano, il GDPR ha portato all'adozione del d.lgs. n. 101/2018[5] che ha modificato e rivisto il d.lgs. n. 196/2003 (c.d. Codice in materia di protezione dei dati personali). In particolare, la novella di armonizzazione — entrata in vigore il 19 settembre 2018 — conserva le parti del Codice non ritenute incompatibili con il GDPR e arricchisce il vecchio testo sul piano della conservazione e revisione dei provvedimenti generali del Garante per la protezione dei dati personali anteriori al regolamento, delle sanzioni penali e delle procedure sanzionatorie.

2. La posizione dell'interessato fra tutela amministrativa e tutela giurisdizionale

Il destinatario della tutela offerta dal GDPR è essenzialmente l'interessato (data subject) che viene definito dall'art. 4, n. 1), come "una persona fisica identificata o identificabile".[6] Tale soggetto, qualora si trovi sotto la giurisdizione di uno degli Stati membri dell'Unione europea, beneficia di una tutela che si realizza non soltanto tramite il riconoscimento di diritti sostanziali,[7] ma anche e soprattutto grazie alla previsione di strumenti d'azione finalizzati al controllo del rispetto della disciplina, nonché

[5] Decreto Legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[6] Gli altri attori principali del GDPR sono il titolare e il responsabile del trattamento. Il primo è definito dall'art. 4, n. 7), come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"; il secondo dal successivo punto come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

[7] All'interno del GDPR, oltre ai diritti che sono espressione dei principi fondamentali esistenti in materia, si annoverano diritti aggiuntivi e per certi versi più incisivi, quali il diritto di accesso, il diritto alla rettifica, il diritto alla cancellazione, il diritto alla portabilità dei dati personali, il diritto di opposizione. In proposito si rinvia a Pizzetti (2016).

all'esercizio e alla piena applicazione dei diritti sostanziali.[8] In particolare, nel caso di violazioni del GDPR, l'interessato ha a disposizione sia la via amministrativa sia la via giurisdizionale per ottenere tutela.[9]

Con riguardo alla prima tipologia di rimedi, l'art. 77 del GDPR attribuisce all'interessato il diritto di presentare reclamo per la violazione della disciplina sulla protezione dei dati, alternativamente, dinanzi all'autorità di controllo dello Stato membro in cui ha la propria residenza o il proprio lavoro, oppure dinanzi a quella del luogo ove si è verificata la presunta violazione.

Ai sensi dell'art. 2-*bis* del Codice sulla protezione dei dati personali, l'autorità di controllo, in Italia, è il Garante per la protezione dei dati personali.[10] Il successivo art. 143 disciplina il procedimento dinanzi a tale autorità, prevedendo che questo si conclude di regola con prescrizioni rivolte al titolare e al responsabile, oppure con un non luogo a provvedere. Rispetto al ricorso giudiziario, il reclamo all'autorità di controllo presenta vantaggi rilevanti sia con riferimento alla speditezza dell'*iter* procedimentale sia per quanto concerne i relativi costi.[11] Tale rimedio, tuttavia, non può essere esperito per ottenere il risarcimento del danno patito a causa del trattamento illegittimo, dovendo l'interessato necessariamente ricorrere, a questo fine, a un ricorso giurisdizionale, ai sensi dell'art. 79 del GDPR. L'impossibilità di fornire un rimedio risarcitorio non sminuisce comunque il ruolo delle autorità di controllo, poiché queste rimangono sempre un'importante fonte d'informazione e di supporto per coloro che lamentino la violazione del diritto alla protezione dei dati personali (Varney 2016).

Con riguardo ai rimedi esperibili dinnanzi all'autorità giurisdizionale, l'art. 79 del GDPR riconosce all'interessato il diritto di proporre un ricorso giurisdizionale effettivo, a norma dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), per

[8] L'importanza di disporre di adeguati rimedi in caso di violazione emerge indirettamente dalla giurisprudenza della Corte di Giustizia, in particolare nella sentenza resa nel caso *Facebook Ireland e Schrems* (Corte di Giustizia, Grande Sezione, sent. 16 luglio 2020, causa C-311/18, ECLI:EU:C:2020:559), avente ad oggetto il trasferimento di dati personali effettuato a fini commerciali da *Facebook Ireland*, cioè la sede europea del colosso statunitense, verso la sede centrale.

[9] Con riguardo all'attivazione dei rimedi, secondo l'art. 80, par. 1, l'interessato, sia nel caso di ricorso giurisdizionale sia nel caso di reclamo all'autorità di controllo, ha il diritto di agire per il tramite di un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, attivi nel settore della protezione dei dati personali. Tale opzione è stata recepita nell'ordinamento italiano dall'art. 10, comma 5, del Codice in materia di protezione dei dati personali. L'art. 80, par. 2, del GDPR, contempla, inoltre, la possibilità che ogni Stato membro si doti di organismi cui venga riconosciuta la possibilità di presentare di propria iniziativa, ovvero indipendentemente dal mandato conferito dall'interessato, un reclamo per conto delle asserite vittime.

[10] L'art. 58 del GDPR richiede che le autorità nazionali di controllo debbano disporre di una serie di poteri investigativi, correttivi, consultivi e di autorizzazione. Nell'ambito dei poteri correttivi, gli artt. 83 e 84 stabiliscono che per rafforzare il rispetto della disciplina del GDPR siano previste sanzioni pecuniarie, in aggiunta alle altre misure o in loro sostituzione. Lo strumento conferisce alle autorità di controllo una certa discrezionalità con riguardo alla valutazione delle singole ipotesi di violazione, alla scelta della sanzione adeguata e al suo ammontare, nell'ipotesi in cui questa abbia natura pecuniaria. Sul tema si veda Guardigli (2017).

[11] Dal punto di vista contenutistico, il reclamo deve includere l'indicazione, per quanto possibile dettagliata, dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate, delle misure richieste e degli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto. Il reclamo cui difettino uno o più requisiti, in ossequio al principio generale di libertà delle forme, può comunque essere analizzato dall'autorità di controllo a titolo di segnalazione. In proposito, si rinvia a Giordano (2019).

accertare l'eventuale violazione delle disposizioni sulla protezione dei dati dinanzi ai tribunali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento o, in alternativa, dinanzi ai tribunali dello Stato membro in cui l'interessato risiede abitualmente. In tale quadro, l'art. 82 del GDPR rappresenta la disposizione cardine della responsabilità civile in materia. Questa prevede che chiunque subisca un danno "materiale o immateriale" (più correttamente patrimoniale o non patrimoniale), causato da una violazione del GDPR o degli atti delegati o di esecuzione, adottati a livello nazionale, ha il diritto di rivolgersi all'autorità giurisdizionale per ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento dei dati personali. Tale diritto sorge nel momento in cui è stata realizzata una violazione di una delle disposizioni stabilite dal GDPR a seguito di una condotta, attiva od omissiva, del titolare (del contitolare o del responsabile) del trattamento. La possibilità di avvalersi del rimedio giurisdizionale non è confinata all'ipotesi di richiesta di risarcimento danni, ma comprende tutti i diritti sostanziali riconosciuti alle persone in materia di protezione dei dati: diritto all'accesso, alla rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità dei propri dati personali.

Sempre nel quadro della tutela giurisdizionale, l'art. 78 del GDPR accorda all'interessato il diritto di contestare sia le azioni sia l'inerzia dell'autorità di controllo. In particolare, si prevede la possibilità di rivolgersi ai giudici dello Stato membro in cui è stabilita l'autorità di controllo qualora questa non dia seguito a un reclamo, lo respinga in tutto o in parte, lo archivi o non agisca quando è necessario intervenire per proteggere i diritti dell'interessato.[12] La possibilità di esperire questo mezzo di tutela è attribuita non solo all'interessato, ma anche al titolare (o al responsabile) del trattamento, rappresentando una delle "*garanzie adeguate*" cui l'art. 58, par. 4, del GDPR subordina l'esercizio dei poteri conferiti alle autorità amministrative indipendenti.

Nell'ambito dell'ordinamento italiano, i provvedimenti vincolanti del Garante per la protezione dei dati personali suscettibili di impugnazione sono quelli prescrittivi (e le ordinanze-ingiunzione), adottati all'esito di procedimenti di contestazione di violazioni amministrative, nonché quelli di rigetto o di archiviazione di reclami. Secondo l'art. 10, comma 3, del d.lgs. 150/2011, i ricorsi avverso questi ultimi devono essere proposti, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento oppure entro sessanta giorni se il ricorrente risiede all'estero. La disposizione prevede espressamente che il giudice ordinario può annullare gli atti e i

[12] Il diritto a un ricorso giurisdizionale effettivo non pare riconosciuto pienamente nel caso in cui l'autorità di controllo non dia seguito al reclamo o non riferisca entro tre mesi sul suo stato o sull'esito. Nell'ipotesi di trattamento transfrontaliero l'interessato può, infatti, proporre il ricorso solo a condizione che l'autorità fosse competente in virtù dell'applicazione del meccanismo dello sportello unico (*one stop shot*) o ai sensi dell'art. 55 del GDPR. Secondo il meccanismo dello sportello unico l'autorità di controllo dello Stato in cui si trova la sede oppure la sede principale del titolare (o responsabile) del trattamento funge da autorità di controllo capofila (*Leading Supervision Authority*) per le attività di trattamento transfrontaliero e per le indagini. L'art. 55 concerne invece il trattamento effettuato da autorità pubbliche o organismi privati che agiscono per adempiere un obbligo legale al quale è soggetto il titolare del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. In tali casi, nonostante il legislatore abbia scelto un criterio flessibile in ordine alla competenza delle autorità di controllo, la scelta da parte dell'interessato risulta determinante in quanto può condizionare la successiva tutela giurisdizionale avverso la decisione amministrativa e presuppone in definitiva la capacità di individuare lo stabilimento principale.

provvedimenti del Garante oggetto di impugnazione. Tale controllo giurisdizionale incontra, tuttavia, un limite legato all'esigenza di avere un'interpretazione del diritto alla protezione dei dati personali uniforme in tutta l'Unione europea. Nell'ipotesi in cui venga esperito il ricorso contro una decisione dell'autorità di controllo precedentemente oggetto di un parere o di una decisione del Comitato europeo per la protezione dei dati (CEPD), resi nell'ambito del meccanismo di coerenza,[13] il Garante è tenuto a trasmettere tale parere o decisione all'autorità giurisdizionale adita e questa, nel caso in cui reputi la decisione invalida, non può annullarla o disapplicarla, ma è tenuta a deferire la questione alla Corte di giustizia, quale giudice naturale della validità degli atti delle istituzioni europee.

La tutela diretta innanzi all'autorità giudiziaria può essere invocata anche a prescindere dal precedente esperimento di rimedi di natura amministrativa (Giordano 2019). Nel caso in cui l'azione giudiziaria sia preceduta dal ricorso all'autorità di controllo, tuttavia, il GDPR non precisa come la giurisdizione civile si articoli rispetto al procedimento dinnanzi all'autorità di controllo né se, ed eventualmente in che misura, il giudice civile sia vincolato dalla decisione dell'autorità di controllo. A livello degli ordinamenti nazionali, la questione ha ricevuto risposte diverse: in taluni casi è previsto un meccanismo di alternatività; in altri casi è stata attribuita una possibilità di scelta, con l'obbligo o la facoltà di una delle due autorità di sospendere il proprio procedimento in attesa della decisione dell'altro organo; in altri casi ancora, si è previsto che le autorità amministrative e gli organi giurisdizionali possano procedere in parallelo, con il rischio quindi di giungere a decisioni contrastanti.[14] Parimenti, il GDPR, probabilmente a causa delle notevoli differenze sussistenti a livello nazionale, non disciplina la questione dell'efficacia delle decisioni dell'autorità di controllo nel separato giudizio che l'interessato abbia successivamente instaurato dinanzi all'autorità giurisdizionale per ottenere il risarcimento dei danni, né tantomeno la questione della "circolazione" delle prove acquisite nel procedimento amministrativo.

[13] Per garantire ulteriormente l'applicazione coerente della disciplina e per risolvere eventuali divergenze tra l'autorità capofila e le altre autorità, il GDPR prevede un Capo VII, dal titolo "Cooperazione e coerenza". Mentre la cooperazione è perseguita attraverso il meccanismo dello "sportello unico" (*one stop shot*), la coerenza è legata all'attività del Comitato europeo per la protezione dei dati (EDPB) e alla sua funzione consultiva e di organo di appello rispetto alle autorità di controllo nazionali. In particolare, il Comitato agisce in tre casi: se le autorità di controllo non sono d'accordo sulla decisione da assumere nel quadro della procedura di cooperazione; se le autorità di controllo non concordano su quale sia da considerarsi autorità capofila; se un'autorità di controllo non richiede un parere al EDPB quando questo è previsto o non dà seguito al parere adottato dal medesimo organo. Per una recente applicazione del principio dello "sportello unico" si veda Corte di Giustizia, Grande Sezione, sent. 15 giugno 2021, causa C-645/19, *Facebook Ireland e a.*, ECLI:EU:C:2021:483, oggetto del commento di Woods (2021).

[14] Sul punto risultano esemplificativi i casi a tutt'oggi pendenti dinanzi alla Corte di Giustizia, in particolare *BE contro Nemzeti Adatvédelmi és Információszabadság Hatóság* (Autorità nazionale incaricata della protezione dei dati e della libertà dell'informazione, Ungheria) (causa C-132/21), domanda di pronuncia pregiudiziale proposta dal Fővárosi Törvényszék (Corte di Budapest-Capitale, Ungheria) il 2 marzo 2021; *FT contro Land Hessen* (causa C-552/21), domanda di pronuncia pregiudiziale proposta dal Verwaltungsgericht Wiesbaden (Germania) il 7 settembre 2021; *UF contro Land Hessen* (causa C-26/22), domanda di pronuncia pregiudiziale proposta dal Verwaltungsgericht Wiesbaden (Germania) il 23 dicembre 2021; *AB contro Land Hessen e SCHUFA Holding AG* (causa C-64/22), domanda di pronuncia pregiudiziale proposta dal Verwaltungsgericht Wiesbaden (Germania) il 2 febbraio 2022.

Nell'ambito dell'ordinamento italiano, le possibili interferenze tra procedimento amministrativo e procedimento giurisdizionale sono disciplinate dall'art. 140-*bis* del Codice in materia di protezione dei dati personali, il quale indica chiaramente che non può essere proposto il reclamo al Garante se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria (comma 2); inoltre se, per il medesimo oggetto e tra le stesse parti, è stata già adito il Garante la domanda giudiziaria è parimenti improponibile, salva l'ipotesi di decorso del termine massimo per la decisione da parte del Garante sul reclamo proposto o di inammissibilità dello stesso (comma 3).[15]

Il principio dell'alternatività delle tutele presuppone che le domande si riferiscano alle stesse parti e abbiano identica *causa petendi* e identico *petitum*. In altri termini, deve trattarsi di domande che se pendenti contestualmente davanti a più giudici possano, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza. Tale coincidenza non può mai verificarsi con riferimento alla domanda risarcitoria perché l'autorità Garante, come detto, è competente all'adozione di provvedimenti di natura preventiva, inibitoria o conformativa, mentre per le domande risarcitorie è prevista la riserva esclusiva di giurisdizione ordinaria. L'autorità giudiziaria ordinaria può provvedere alla cognizione sulla domanda risarcitoria sia in sede di impugnazione del provvedimento del Garante (ai sensi dell'art. 152, comma 1, del Codice), sia autonomamente.[16] Tale ultimo scenario appare il meno probabile, perché è assai più verosimile che l'interessato, dopo aver presentato un reclamo dinnanzi al Garante e aver ottenuto l'adozione di una sanzione amministrativa nei confronti del titolare (o del responsabile) del trattamento, decida di rivolgersi al giudice civile per chiedere, sulla base della decisione assunta dall'autorità di controllo, il risarcimento dei danni patiti.

La giurisprudenza nazionale, con riferimento alla disciplina previgente, ha chiarito che il provvedimento del garante ha natura di decisione amministrativa sul merito. Di conseguenza, il controllo giurisdizionale non si risolve in un mero sindacato di legittimità del provvedimento, ma implica un riesame integrale della decisione che riguarda l'intero rapporto, nell'ottica di garantire una tutela effettiva. In tale cognizione rientra anche la determinazione dell'entità dell'eventuale sanzione erogata e tale valutazione è insindacabile in sede di legittimità se congruamente motivata e immune

[15] La soluzione adottata dal legislatore italiano non pare intaccare il diritto a un ricorso giurisdizionale effettivo di cui all'art. 47 della CDFUE. In proposito la Corte di Giustizia nel caso Puškár (sent. 27 settembre 2017, causa C-73/16, ECLI:EU:C:2017:725), riferendosi alla disciplina previgente in materia di protezione dei dati personali, ha riconosciuto che il previo esperimento di un rimedio amministrativo è un mezzo per conseguire obiettivi di interesse generale legittimi in ragione del positivo effetto deflattivo del contenzioso e quindi della possibilità di definire le controversie in tempi più rapidi, incrementando l'efficienza del sistema giudiziario nel suo complesso. Di conseguenza la condizione del previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative è inammissibile soltanto nell'ipotesi in cui le modalità concrete di esercizio di detti rimedi pregiudichino eccessivamente il diritto ad un ricorso effettivo dinanzi al giudice, causino un ritardo sostanziale per la proposizione di un ricorso giurisdizionale, determinino la prescrizione dei diritti considerati o comportino costi eccessivi. Sull'argomento, più ampiamente, Trocker (2002), Arnull (2011).

[16] L'art. 152 del Codice in materia di protezione dei dati personali assoggetta le relative controversie al rito del lavoro. Sul tema si veda Bilotta (2019).

da errori logici o giuridici.[17] La natura di decisione amministrativa della decisione del Garante determina pure la sua inidoneità a passare in giudicato.[18]

Quanto all'utilizzabilità in sede di giudizio civile delle prove raccolte nel procedimento amministrativo davanti al Garante, pare doversi affermare la possibilità che queste possano essere ammesse, anche alla luce del fatto che il diritto processuale civile conosce le prove atipiche. Le risultanze dell'istruttoria del Garante, in considerazione del loro grado di approfondimento e della specializzazione dell'autorità che conduce l'attività, possono rappresentare un importante punto di riferimento nel processo di libero apprezzamento delle prove condotto dal giudice, anche se è da escludere che i provvedimenti del Garante siano da intendersi come fonti di accertamento vincolanti in relazione all'esistenza dell'infrazione.

Per quanto nell'ordinamento italiano le possibili interferenze tra procedimento amministrativo e procedimento giurisdizionale siano state disciplinate escludendo che l'azione dinanzi al Garante e l'azione dinanzi all'autorità giurisdizionale possano esercitarsi in parallelo, un certo margine di incertezza permane, anche e soprattutto in caso di trattamento transfrontaliero.

Con riferimento alle decisioni pronunciate da autorità giurisdizionali, considerato che il GDPR non contiene alcuna disposizione *ad hoc*, trova applicazione il regime generale di circolazione delle decisioni straniere valido in ambito europeo nella materia civile e commerciale, ossia il Regolamento (UE) n. 1215/2012, secondo il quale ogni decisione che rientra nell'ambito di applicazione dello strumento viene eseguita in modo automatico in un diverso Stato membro senza che sia necessario il ricorso ad alcun procedimento.[19]

Nel caso in cui l'azione risarcitoria venga esercitata dinnanzi al giudice italiano a seguito della violazione del GDPR accertata da un'autorità di controllo di un altro Stato membro, non è invece chiaro se il provvedimento di quest'ultima autorità possa essere accettato almeno come prova, rimessa all'apprezzamento del giudice. Risulta evidente che, nel caso in cui non venga dato alcun rilievo alla decisione adottata dall'autorità di controllo straniera, il titolare del trattamento convenuto nel giudizio di risarcimento del danno potrà mettere in dubbio la violazione anche se questa è affermata in un provvedimento che può essere finanche definitivo in ragione della mancata impugnazione o del rigetto della richiesta di annullamento. I giudici dinanzi ai quali viene intentata un'azione di risarcimento danni dovranno pertanto riesaminare i fatti e gli aspetti giuridici già oggetto di indagine e di valutazione da parte di un'autorità pubblica specializzata.

La mancata previsione nel GDPR di una norma che definisca gli effetti delle decisioni delle autorità di controllo rischia di compromettere la certezza del diritto, di produrre contraddizioni nell'applicazione del GDPR e di diminuire l'efficacia e l'efficienza procedurale delle azioni per il risarcimento del danno. Diversamente, tali preoccupazioni sono state tenute in considerazione in altri ambiti: la direttiva

[17] In tal senso, vedasi Corte di Cassazione, sez. I civile, ordinanza del 18 giugno 2018, n. 16061; sez. I civ., sentenza del 30 giugno 2016, n. 17143; sez. II civile, sentenza del 2 aprile 2015, n. 6778.
[18] Corte di Cassazione, sez. III civile, ordinanza del 25 maggio 2017, n. 13151.
[19] I provvedimenti possono anche essere non definitivi e possono derivare da procedimenti contenziosi o non contenziosi. Sulla nozione di materia civile e commerciale si veda *infra* par. 3, nota 27. Con riferimento alle disposizioni concernenti la sospensione delle azioni in caso di procedimenti paralleli dinnanzi a autorità giurisdizionali di diversi Stati membri si rinvia a Marongiu Buonaiuti (2017).

2014/104/UE, relativa a determinate norme che regolano le azioni per il risarcimento del danno ai sensi del diritto nazionale per violazioni delle disposizioni del diritto della concorrenza degli Stati membri e dell'Unione europea, prevede all'art. 9, par. 1, che gli Stati membri provvedono affinché una violazione del diritto della concorrenza constatata da una decisione definitiva di un'autorità nazionale garante della concorrenza sia ritenuta definitivamente accertata ai fini dell'azione per il risarcimento del danno.

3. La legge applicabile al consenso del minore

Tra gli aspetti più innovativi del GDPR vi è la previsione relativa alla capacità del minore sedicenne e ultra-sedicenne di prestare, ove richiesto, il consenso al trattamento dei propri dati personali nell'ambito dei servizi della società dell'informazione (art. 8, par. 1).[20] Detta disposizione persegue lo scopo di accordare ai minori una speciale protezione poiché "questi 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".[21] Il paragrafo successivo prevede, al medesimo fine, che il titolare del trattamento deve compiere ogni ragionevole sforzo per verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale, in funzione della tecnologia disponibile.

L'art. 8, par. 1, come anticipato, consente di derogare al prescritto limite: ciascuno Stato membro nell'adottare la relativa normativa nazionale può prevedere un'età inferiore, purché questa non vada al di sotto della soglia dei tredici anni. Tale scelta normativa sembra voler realizzare un compromesso tra l'esigenza di uniformare la tutela del diritto alla protezione dei dati personali dei minori nel territorio dell'Unione europea e il riconoscimento delle particolarità dei singoli Stati membri.[22]

Il legislatore italiano, con il d.lgs. n. 101/2018 ha deciso di servirsi dello spazio di manovra concessogli, stabilendo all'art. 2-*quinquies* del Codice in materia di protezione dei dati personali che "in attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale".[23] La disciplina nazionale di adeguamento dinanzi all'alternativa tra la prestazione del consenso da parte dell'esercente la responsabilità genitoriale in vece del minore e l'autorizzazione del primo alla prestazione del consenso da parte del minore

[20] L'art. 8 del GDPR trova applicazione solo quando ricorrono alcune condizioni specifiche. In primo luogo, è necessario che vi sia un'offerta di servizi della società dell'informazione rivolta direttamente al minore. In secondo luogo, occorre che l'offerta richieda il consenso esplicito dell'interessato per la sua accettazione e soprattutto per la legittimità del trattamento di dati personali. Per un approfondimento del tema si vedano Macenaite (2017) e, nella dottrina italiana, Spoto (2016).

[21] Sul punto si veda il considerando n. 38 del GDPR.

[22] Per una critica a tale opzione normativa si veda McCullagh (2016).

[23] Anche altri paesi hanno fatto ricorso a detta facoltà: il limite di età per il consenso del minore al trattamento dei propri dati personali risulta così fissato ai 15 anni in Grecia, Repubblica Ceca, Slovenia e Francia; ai 14 anni in Austria, Bulgaria, Cipro, Lituania; ai 13 anni di età in Belgio, Regno Unito, Spagna, Svezia, Danimarca, Estonia, Lituania, Lettonia, Finlandia, Polonia, Portogallo. Per un puntuale riferimento alle leggi di adeguamento al GDPR si rinvia a Mantovani (2019).

stesso si è schierata a favore della prima opzione. Il titolare della responsabilità genitoriale, pertanto, esercita il diritto quale legale rappresentante del minore, non limitandosi a integrare la minore capacità di agire di quest'ultimo.

La possibilità per i legislatori nazionali di intervenire per ampliare, limitare o derogare la disciplina contenuta nel GDPR rende necessario verificare se una ipotetica fattispecie risulti completamente disciplinata dallo stesso strumento oppure se vengano in considerazione le disposizioni nazionali di adeguamento al GDPR.[24] Nel primo caso trova applicazione la disciplina uniforme contenuta nel GDPR; nel secondo caso, laddove la fattispecie abbia una "dimensione" transnazionale, si pone la questione di determinare la legge applicabile, con il rischio che più leggi nazionali di adeguamento rivendichino parallelamente la propria applicazione a una determinata attività di trattamento (conflitti di leggi "positivi") o, al contrario, che nessuna legge nazionale di adeguamento si ritenga applicabile nel caso specifico (conflitti di leggi "negativi"). Tali situazioni rendono manifeste le difficoltà di coordinamento fra le leggi di adeguamento e il GDPR e l'incertezza giuridica che ne consegue (Mantovani 2019).[25]

Detta incertezza si riscontra anche quando i diversi ordinamenti che presentano punti di contatto con la fattispecie convergono sull'individuazione della medesima legge applicabile. Si consideri il caso in cui un servizio della società dell'informazione venga prestato gratuitamente da una società stabilità in Belgio a favore di clienti di cittadinanza italiana, residenti in Italia e che, nell'ambito di tale servizio, detta società raccolga e tratti i dati personali dei propri clienti, tra i quali un individuo di anni tredici. Nel caso in cui si venisse a scoprire che i dati raccolti sono impiegati anche a fini pubblicitari, per valutare la legittimità del trattamento e la fondatezza di un'eventuale richiesta di risarcimento dei danni occorrerebbe valutare se il consenso del minore al trattamento possa reputarsi legittimamente prestato e, in tal caso, sarebbe altresì necessario determinare la sua ampiezza, così da accertare se l'attività di *marketing* abbia o meno una base giuridica. Si tratta di una questione di liceità del trattamento che dipende dalla legge applicabile alla questione del consenso del minore, essendo questa da risolvere

[24] Tale considerazione vale chiaramente solo nell'ipotesi in cui la fattispecie possa collocarsi all'interno dell'ambito di applicazione territoriale e materiale del GDPR. In proposito, l'art. 3 del GDPR definisce il campo di applicazione territoriale del regolamento sulla base di due criteri principali: il criterio di stabilimento ("*establishment criterion*") e il criterio di collocazione fisica e geografica degli interessati ("*targeting criterion*"). Su tale aspetto si vedano, fra i tanti, Kuner (2021), Gömann (2017), De Hert e Czerniawski (2016).

[25] Per dimostrare come possano venire a determinarsi conflitti di leggi "positivi" e "negativi", l'autrice prospetta a titolo esemplificativo due diversi scenari. Il primo concerne un titolare del trattamento stabilito in Lussemburgo e soggetto, in quanto tale, alla locale legge di adeguamento con riguardo all'insieme delle attività di trattamento, indipendentemente dal fatto che tali operazioni siano eseguite o meno "nell'ambito delle attività" di tale stabilimento. Nel caso in cui lo stesso titolare del trattamento abbia un altro stabilimento all'interno del territorio del Belgio, nell'ambito delle cui attività detto trattamento di dati personali è effettivamente svolto, anche la legge belga di adeguamento al GDPR rivendicherebbe la propria applicazione, così come la legge francese nel caso in cui tali attività riguardino un interessato residente nel territorio francese e la legge portoghese se l'interessato, sebbene residente in Francia, sia un cittadino portoghese registrato presso il consolato. Il secondo scenario si riferisce a un interessato domiciliato in Germania che propone dinanzi alle autorità giurisdizionali francesi un'azione contro un titolare del trattamento stabilito in Francia. In tale caso il tribunale adito non può che accertare l'inapplicabilità della legge francese di adeguamento al GDPR che disciplina solo la posizione giuridica degli interessati residenti in Francia, e parimenti l'inapplicabilità della legge tedesca di adeguamento, poiché il trattamento non ha luogo sul territorio tedesco né nell'ambito delle attività di uno stabilimento tedesco.

preliminarmente rispetto alla valutazione della fondatezza della richiesta di risarcimento.[26]

Nel caso appena prospettato, una prima difficoltà nell'individuazione del diritto applicabile è legata alla qualificazione, operazione che risulta necessaria per ricondurre la fattispecie all'interno della corretta categoria giuridica. Risulta, in tal senso, fondamentale analizzare il rapporto tra il GDPR e i regolamenti in materia di diritto internazionale privato dell'Unione europea, in particolare, il Regolamento n. 593/2008, sulla legge applicabile alle obbligazioni contrattuali (c.d. Roma I) e il Regolamento n. 864/2007, sulla legge applicabile alle obbligazioni extracontrattuali (c.d. Roma II). Tali strumenti delimitano il proprio ambito di applicazione *ratione materiae* riferendosi, per un verso, alla "materia civile e commerciale" ed escludendo, per altro verso, le "questioni amministrative".[27]

Con riferimento alle esclusioni espresse, che circoscrivono ulteriormente l'ambito di applicazione degli strumenti menzionati, è possibile osservare come il Regolamento Roma I rimanga neutrale rispetto alla materia, mentre il Regolamento Roma II stabilisce chiaramente che esso non trova applicazione per le "obbligazioni extracontrattuali derivanti da violazioni della privacy e dei diritti relativi ai diritti della personalità, compresa la diffamazione", senza specificare se tale esclusione operi anche rispetto alle violazioni della protezione dei dati personali.

Il rapporto fra protezione dei dati e privacy non è di facile comprensione, al punto che in dottrina ci si domanda se i due diritti vadano considerati come separati o se invece la protezione dei dati possa farsi rientrare all'interno della nozione di "privacy in senso ampio" (Kokott e Sobotta 2013, Pizzetti 2016). A prescindere dal rilievo teorico della questione, sembra potersi affermare che, riguardo al Regolamento Roma II, considerazioni di ordine teleologico e sistematico impongono una preferenza per la seconda tesi. Del resto, se la privacy fosse esclusa dal campo di applicazione del

[26] Il consenso al trattamento, ai sensi dell'art. 6, par. 1, lett. a), del GDPR è una delle sei basi giuridiche che permette di giustificare la raccolta e il trattamento di dati personali per una o più specifiche finalità. Esso viene definito dall'art. 4 come "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".

[27] La Corte di Giustizia ha interpretato la nozione di "materia civile e commerciale" inizialmente con riferimento alla Convenzione di Bruxelles del 1968 concernente la competenza giurisdizionale e l'esecuzione delle decisioni in materia civile e commerciale, seguendo il principio della qualificazione autonoma, in base al quale il significato delle nozioni non va ricercato all'interno dei singoli ordinamenti degli Stati membri, bensì nell'ambito del medesimo strumento. Nel merito della questione i giudici di Lussemburgo hanno affermato che il fatto che una delle parti in causa è un ente di diritto pubblico non determina, come automatica conseguenza, l'esclusione della controversia dal campo di applicazione dello strumento. L'esatta portata della nozione di "esercizio della potestà d'imperio" resta comunque difficilmente definibile giacché la Corte ha esaminato il fondamento e le modalità d'esercizio dell'azione intentata seguendo un approccio *case by case*. In proposito vedasi Corte di giustizia, sent. 16 dicembre 1980, causa C-814/79, *Paesi Bassi c. Rüffer*, ECLI:EU:C:1980:291; sent. 21 aprile 1993, causa C-172/91, *Sonntag c. Waidmann*, ECLI:EU:C:1993:144; sent. 15 maggio 2003, causa C-266/01, *Préservatrice foncière TIARD*, ECLI:EU:C:2003:282; sent. 15 febbraio 2007, causa C-292/05, *Lechouritou* e a., ECLI:EU:C:2007:102; in dottrina sulla questione si vedano Brkan (2015), Kohler (2016). Nel caso di violazioni del GDPR, l'applicabilità dei Regolamenti Roma I e Roma II può risultare difficile da concettualizzare, poiché la materia rientra nell'"area grigia" tra il diritto pubblico e il diritto privato. Ciononostante, allorché l'azione venga promossa da un privato contro un altro privato, questa rientra, in linea di massima, nella "materia civile e commerciale", mentre nell'ipotesi in cui risulti coinvolta un'autorità pubblica occorre valutare, di volta in volta, se essa agisce o meno nell'ambito dei propri poteri.

regolamento e la protezione dei dati non lo fosse verrebbero a determinarsi enormi difficoltà nell'individuazione della legge applicabile per violazioni che incidono contestualmente su entrambi i diritti.

In caso di violazione delle disposizioni del GDPR o delle disposizioni nazionali di adeguamento allo strumento, il Regolamento Roma I viene in considerazione tutte le volte che la pretesa sottoposta all'attenzione del giudice origini da obblighi liberamente assunti dal titolare (o dal responsabile) del trattamento nei confronti dell'interessato. In proposito è possibile osservare come i contratti di fornitura di servizi online generalmente includano, nell'ambito delle loro condizioni generali, clausole relative alla protezione dei dati personali. Lo strumento non assume rilievo invece nel caso in cui non sussista fra le parti un rapporto contrattuale o nel caso in cui la violazione del diritto alla protezione dei dati non sia comunque riconducibile a obblighi liberamente assunti dal titolare (o del responsabile) del trattamento nei confronti dell'interessato.[28]

Nondimeno, anche nell'ipotesi in cui fra le parti intercorra un rapporto di natura contrattuale, la rilevanza del Regolamento Roma I è alquanto dubbia con specifico riferimento al "consenso del minore al trattamento". L'art. 1, par. 2, lett. a) dello strumento colloca infatti al di fuori del proprio campo di azione le "questioni di stato e capacità delle persone fisiche", le quali rimangono soggette alla legge individuata come applicabile in base alle norme interne di diritto internazionale privato. La disposizione, tuttavia, fa salvo l'art. 13, secondo cui se i contraenti si trovano in uno stesso paese, la persona capace in base alla legge del luogo dove il contratto è stato concluso non può opporre alla controparte l'incapacità derivante da una legge diversa, a meno che quest'ultima non sia a conoscenza di tale incapacità o l'abbia colpevolmente ignorata.

Il consenso del minore al trattamento dei dati personali non rientra, a nostro avviso, tra le questioni di capacità riconducibili entro l'ambito di applicazione dell'art. 13.[29] Detto consenso, in quanto condizione di liceità del trattamento, resta distinto e autonomo rispetto alla manifestazione di disponibilità all'utilizzo dei propri dati nell'ambito dell'operazione economica, sebbene i due aspetti possano coesistere in taluni casi.[30]

[28] Sulla distinzione fra obbligazioni contrattuali e obbligazioni extracontrattuali vedasi Corte di Giustizia, sent. 27 settembre 1988, causa C-189/87, *Kalfelis c. Schröder e a.*, ECLI:EU:C:1988:459; sent. 13 marzo 2014, causa C-548/12, *Brogsitter*, ECLI:EU:C:2014:148; sent. 28 gennaio 2015, causa C-375/13, *Kolassa*, ECLI:EU:C:2015:37. Più recentemente, i giudici di Lussemburgo (sent. del 7 marzo 2018, cause riunite C-274/16, C-447/16 e C-448/16, *flightright*, ECLI:EU:C:2018:160) hanno precisato che la nozione di contratto può essere invocata anche da un soggetto che non è parte perché "si devono considerare rientranti nella materia contrattuale tutte le obbligazioni che trovano la loro fonte nel contratto il cui inadempimento è invocato a sostegno dell'azione del ricorrente". Parte della dottrina sostiene l'applicabilità del Regolamento Roma I per le violazioni della disciplina contenuta nel GDPR (Kohler 2016 e Mantovani 2019). Altra parte, diversamente ritiene che le pretese risarcitorie debbano essere qualificate come extracontrattuali e che qualche dubbio in ordine alla riconduzione entro la nozione di obbligazione contrattuale residua solamente "nell'ipotesi in cui l'illiceità del trattamento fatta valere riposi sul mancato rispetto dei termini del consenso manifestato dall'interessato nell'ambito di un rapporto contrattuale". Anche in tal caso l'autrice sostiene, tuttavia, che "una qualificazione contrattuale dovrebbe essere esclusa alla luce della natura autorizzatoria e non negoziale del consenso" (Ragno 2020).

[29] Il presupposto dell'applicazione della norma, cioè il fatto che le parti si trovino nel medesimo paese, rende comunque l'art. 13 del Regolamento Roma I scarsamente rilevante nel quadro dei contratti conclusi tramite la rete internet.

[30] Sulla natura giuridica e sul ruolo del consenso nella complessiva operazione negoziale si vedano Sica (2001) e Caggiano (2021).

Nell'ambito dell'ordinamento italiano, in particolare, la natura di libertà fondamentale del diritto alla protezione dei dati personali comporta che questo debba collocarsi al di fuori delle regole della negozialità *tout court*. Secondo l'insegnamento tradizionale, infatti, gli atti nei quali si manifestano le libertà fondamentali della persona sono esclusi dalla regola dell'incapacità negoziale, salva solo l'interferenza del genitore o del tutore, giustificata dalla funzione di educazione e cura.

I due profili sembrano rimanere distinti e autonomi anche nell'ambito del GDPR: l'art. 8, par. 3, del GDPR, riferendosi alla disciplina concernente l'offerta diretta di servizi della società dell'informazione ai minori, specifica che questa "non pregiudica le previsioni di legge nazionali in materia di diritto dei contratti, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore"; l'art. 7 del GDPR stabilisce che l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Quindi, in teoria, si potrebbero immaginare situazioni in cui un individuo minore di età abbia acconsentito a un contratto di vendita o di servizi, ma non desiderando più che i propri dati siano trattati nell'ambito di esso, revochi il relativo consenso, senza che ciò influisca necessariamente sull'esecuzione del contratto esistente fra le parti. Specularmente, la violazione dell'oggetto principale del contratto non inciderebbe necessariamente sul successivo trattamento dei dati che avesse luogo in tale contesto.

Diversamente dagli altri legislatori nazionali, quello italiano non ha ritenuto di dover specificare l'ambito di applicazione spaziale della legge di adeguamento al GDPR, limitandosi ad abrogare l'art. 5 del Codice in materia di protezione dei dati personali che, sotto il vigore della Direttiva dati, svolgeva tale funzione.

In mancanza di un'apposita norma, dinanzi ai tribunali italiani nel caso di fattispecie che presentino elementi di estraneità, per la valutazione della capacità dei minori di anni sedici a prestare validamente il consenso al trattamento dei propri dati personali occorre riferirsi alle norme nazionali di conflitto, in particolare, all'art. 23 della legge n. 218/1995 di riforma del sistema di diritto internazionale privato. Tale disposizione riguarda la capacità di agire, intesa come idoneità del soggetto a compiere validamente atti giuridici. L'art. 23, comma 1, utilizza il criterio di collegamento della cittadinanza per la capacità di agire generale, ovvero per la capacità di compiere ogni atto che rientra nella sfera giuridica del soggetto agente. La norma è nondimeno accompagnata da una regola autonoma per le condizioni speciali di capacità di agire che possono essere richieste per i singoli atti (art. 23, comma 1, secondo frase). Questa stabilisce che tali condizioni speciali sono disciplinate dalla stessa legge regolatrice dell'atto. Il richiamo della *lex substantiae* e la contestuale deroga alla *lex patriae* sono giustificati dal fatto che la capacità di agire eccezionalmente anticipata del minore è correlata alla particolare natura dell'atto da compiere e per questo attiene alla materia di cui si tratta, piuttosto che allo statuto personale del soggetto.[31] Con riferimento al "consenso del minore al trattamento dei propri dati personali", il fatto che questo sia circoscritto all'offerta diretta di servizi della società dell'informazione, e non assuma invece rilievo di portata generale, porta a ritenere che trovi applicazione l'art. 23, comma 1, seconda frase, e dunque che la legge applicabile sia da individuarsi in quella regolatrice dell'atto.

[31] Parte della dottrina afferma che le ipotesi particolari di capacità di agire rientrano tra le capacità speciali (Clerici 1996 e Barel 2004); per una diversa posizione vedasi Ubertazzi (2006).

Tale soluzione, per quanto appaia maggiormente aderente al tenore letterale delle norme rilevanti, risulta però foriera di risultati poco soddisfacenti perché rischia di alterare il livello di tutela che il legislatore italiano intende accordare in materia ai minori e, in alcuni casi, anche di sottrarre all'applicazione della legge italiana fattispecie che risultano più strettamente collegate con l'ordinamento italiano. Questa ultima eventualità si verifica tutte le volte in cui il fornitore dei servizi "imponga" all'interessato, in base all'art. 3 del Regolamento Roma I, una legge di un paese che non risulti strettamente collegato con la fattispecie contrattuale.

Nell'esempio prospettato in precedenza, allorché la legge belga venga individuata come *lex contractus*, perché scelta dalle parti o perché legge del paese nel quale si trova la residenza abituale della parte che deve effettuare la prestazione caratteristica, l'applicazione delle norme sostanziali della legge belga di adeguamento al GDPR porterebbe a considerare legittimo il trattamento, poiché in tale ordinamento la soglia minima per esprimere il consenso è fissata ai tredici anni di età, nonostante nella prospettiva dell'ordinamento italiano si giungerebbe a una diversa valutazione.

La possibilità che la disposizione sull'età minima del consenso, contenuta nella legge italiana di adeguamento al GDPR, trovi applicazione può affermarsi nella misura in cui questa sia riconducibile a quelle norme che, ai sensi dell'art. 6, par. 2, del Regolamento Roma I, non possono essere derogate contrattualmente nel paese in cui il consumatore ha la sua residenza abituale.[32] Il citato articolo è volto, com'è noto, alla tutela del consumatore, quale parte debole del contratto, in favore del quale vengono preservate le garanzie previste dalla legge della sua residenza abituale. Nella medesima ottica è formulata la disposizione che stabilisce che, in mancanza di scelta, la legge applicabile ai contratti con i consumatori è la legge del paese dove il consumatore ha la sua residenza abituale.

La tesi secondo cui le nozioni di interessato e di consumatore possono essere assimilate non è tuttavia pacifica. A suo sostegno può osservarsi come, al pari del consumatore, l'art. 4 del GDPR definisca l'interessato "persona fisica". Inoltre, il trattamento dei dati personali sottintende un rapporto asimmetrico, a prescindere dall'esistenza *inter partes* di un rapporto contrattuale. Tale squilibrio porta generalmente l'interessato ad accettare clausole predisposte unilateralmente dal fornitore di servizi online, al fine di evitare di dover rinunciare al servizio o di subirne l'interruzione.[33] Di contro, è possibile rilevare che la mera esistenza di un rapporto fra un interessato e la società non è sufficiente per qualificare la transazione come contratto di consumo (Brkan 2015, 2016, Chen 2016).

[32] Con riferimento all'applicazione delle disposizioni inderogabili dell'ordinamento della residenza abituale del consumatore-interessato la Corte di Giustizia (sent. 28 luglio 2016, *Verein für Konsumenteninformation* cit.) ha stabilito che le clausole sulla legge applicabile contenute nelle condizioni d'uso possono essere dichiarate abusive e quindi nulle, nei casi in cui non facciano riferimento al fattore di collegamento protettivo previsto dall'art. 6, par. 2, del Regolamento Roma I, poiché inducono erroneamente il consumatore a ritenere che solo il diritto indicato si applichi al rapporto contrattuale.

[33] Nel quadro dell'ordinamento italiano si veda, in tal senso, Corte di Cassazione, sez. I civile, sent. 2 luglio 2018, n. 17278.

Ulteriori problemi di inquadramento possono sorgere nell'ipotesi in cui la prestazione viene resa a titolo gratuito[34] e nell'ipotesi in cui l'interessato abbia concluso il contratto per motivi in parte professionali e in parte privati.[35]

La possibilità che la norma sull'età minima del consenso, contenuta nella legge italiana di adeguamento al GDPR, trovi applicazione si può affermare anche nell'ipotesi in cui questa sia qualificabile come norma di applicazione necessaria, perché in tal caso resterebbero escluse la legge scelta dalle parti o la legge designata sulla base di criteri oggettivi. In tal caso il riferimento normativo sarebbe rappresentato dall'art. 17 della legge n. 218/1995 nell'ipotesi in cui la fattispecie avesse natura non contrattuale e dall'art. 9 del Regolamento Roma I nell'ipotesi in cui la fattispecie avesse natura contrattuale. Tale ultima disposizione descrive le norme di applicazione necessaria come "disposizioni il cui rispetto è ritenuto cruciale da un paese per la salvaguardia dei suoi interessi pubblici (…) al punto da esigerne l'applicazione a tutte le situazioni che rientrino nel loro campo d'applicazione, qualunque sia la legge applicabile al contratto (…)".

Un argomento che porterebbe a escludere la possibilità di ricorrere alle norme di applicazione necessaria si ricava dal considerando 37 del Regolamento Roma I che afferma che solo in circostanze eccezionali i giudici degli Stati membri possono applicare deroghe basate su dette norme. Secondo il medesimo considerando, inoltre, le norme di applicazione necessaria dovrebbero essere distinte e intese in senso più restrittivo rispetto alle disposizioni alle quali non è permesso derogare convenzionalmente. Nella medesima direzione, è possibile osservare, infine, che il limite di età per esprimere il consenso risulta diretto principalmente alla tutela di interessi individuali e quindi sprovvisto di una dimensione che attiene all'organizzazione sociale ed economica dello Stato, concetti espressamente richiamati dall'art. 9.

Tali argomenti non paiono, a nostro avviso, decisivi. In primo luogo, è possibile osservare come in numerosi ordinamenti giuridici di Stati membri dell'Unione europea,

[34] In proposito appare di notevole interesse la sentenza della Corte di Giustizia resa nel caso *Schrems* (sent. 25 gennaio 2018, causa C-498/16, ECLI:EU:C:2018:37). La questione aveva a oggetto la competenza del giudice adito e, in particolare, la possibilità di invocare il foro del consumatore, nonostante il ricorrente avesse accettato, al momento dell'iscrizione al noto *social network*, una specifica clausola che designava come competenti i tribunali della California. Nel decidere la controversia, i giudici di Lussemburgo hanno considerato che nel caso di fornitura di servizi di *social-networking* o di altri servizi online il pagamento manca solo apparentemente, dal momento che esiste un costo nascosto, rappresentato proprio dalla possibilità di impiegare i dati dell'interessato in attività di marketing e di profilazione della clientela. I dati personali, raccolti apertamente attraverso la registrazione o surrettiziamente tramite *cookies*, devono quindi considerarsi la controprestazione del consumatore per il servizio ricevuto. Sul tema in dottrina si vedano, Langhanke e Schmidt-Kessel (2015), Helberger *et al.* (2017), De Franceschi (2019).

[35] La Corte di Giustizia ha affrontato in più occasioni la questione dei contratti conclusi a duplice scopo, accogliendo un'interpretazione rigorosa della nozione di "consumatore", secondo la quale una persona che conclude un contratto per beni destinati a scopi che sono in parte professionali e in parte privati non può fare affidamento sulle norme speciali a tutela del consumatore, a meno che lo scopo commerciale o professionale sia talmente limitato da risultare trascurabile nel contesto complessivo del rapporto contrattuale. In proposito, fra le tante, si veda Corte di Giustizia, sent. 15 luglio 2021, cause riunite C-152/20 e C-218/20, *SC Gruber Logistics*, ECLI:EU:C:2021:600. Tale impostazione è stata recentemente riconsiderata in senso più flessibile nel caso *Schrems* (sent. 25 gennaio 2018 cit.), poiché i giudici di Lussemburgo hanno affermato che lo *status* di consumatore può cambiare nel tempo, soprattutto all'interno di contratti di fornitura di servizi che per loro natura sono destinati a essere utilizzati a lungo.

la delimitazione spaziale delle normative di esecuzione del GDPR non sia stata lasciata al funzionamento delle norme di conflitto, bensì affidata il più delle volte a c.d. norme autolimitanti. La legge francese di adeguamento al GDPR, ad esempio, impiega quale proprio criterio di applicazione spaziale la residenza dell'interessato, indipendentemente dal fatto che il trattamento dei dati personali avvenga o meno in concreto in Francia. Similmente la legge croata prevede che il trattamento di alcune categorie di dati di individui domiciliati in Croazia è obbligatoriamente soggetto al diritto croato[36]. Tali opzioni legislative, nella misura in cui escludono il ruolo delle norme di conflitto di matrice bilaterale, si muovono in una logica unilateralistica o, in altri termini, nella sfera di eccezione del diritto internazionale privato tradizionale, analogamente alle norme di applicazione necessaria (Koutra 2019).

Inoltre, secondo parte della dottrina, lo scopo delle norme di applicazione necessaria non deve essere legato alla tutela di inter

essi di rilevanza cruciale per l'ordinamento di appartenenza; tale correlazione non solo non è necessaria, dal momento che anche le norme che perseguono scopi di tutela della parte contrattuale più debole possono risultare norme di applicazione necessaria[37], ma non è neanche sufficiente, poiché occorre comunque desumere la volontà dello Stato di prevedere un'applicazione esclusiva delle norme interne a dispetto di quelle richiamate dalle regole di conflitto (Davì 1981 e 1990, 630).

L'individuazione, da parte delle leggi nazionali, della soglia minima per il "consenso al trattamento dei dati personali dei minori di età", invero, risponde alla realizzazione del diritto fondamentale alla tutela dei dati personali, diritto che è riconosciuto in molte convenzioni internazionali in materia di diritti umani e dalla Carta dei diritti fondamentali dell'Unione europea. Il fatto che tale ultimo strumento qualifichi tale diritto come diritto autonomo e separato dal diritto al rispetto della vita privata non pare peraltro privo di rilevanza.

Invero, l'art. 8 del GDPR sembra indicare che il legislatore europeo abbia inteso affidare ai legislatori nazionali la ricerca del giusto equilibrio fra due opposti interessi: da un lato, la tutela dei minori considerati soggetti vulnerabili; dall'altro, il riconoscimento del margine di autonomia necessario a consentire ai minori lo svolgimento della propria personalità, anche alla luce del potenziale educativo connaturato ai servizi della società dell'informazione.[38] In tal senso, un limite eccessivamente basso per il consenso al trattamento dei dati personali dei minori rischia di pregiudicare il primo dei due interessi, un limite troppo elevato rischia invece di urtare il secondo. Le leggi nazionali

[36] Per un'analisi completa dei diversi approcci seguiti dagli Stati membri dell'Unione europea si veda Mantovani (2019).

[37] Corte di Giustizia, sent. 9 novembre 2000, causa C-381/98, *Ingmar GB*, ECLI:EU:C:2000:605. L'orientamento assunto dalla Corte nel caso *Ingmar*, confermato in molte decisioni successive, sembra indicare che l'affermazione dello stato sociale e del mercato interno abbiano portato a una trasformazione della nozione di norme di applicazione necessaria, nel senso di includere al suo interno la tutela delle parti contrattuali più deboli, quale espressione di un interesse di portata generale. Sul tema si vedano Kuipers (2012), van Bochove (2014) e, con specifico riferimento al GDPR, Rossolillo (2019).

[38] Un chiaro riferimento a tale interesse è rintracciabile nell'art. 6 della Convenzione di New York sui diritti del fanciullo del 1989 che impone a tutti gli Stati membri dell'Unione europea, in quanto parti del trattato, di promuovere la capacità dei minori di prendere decisioni e di fare scelte di vita libere, informate e positive. Su tali questioni, più ampiamente, Krivokapić e Adamović (2016), Livingstone *et al.* (2016).

di adeguamento potrebbero considerarsi quindi le uniche in grado di cogliere i "fattori ambientali locali", in particolare il livello di alfabetizzazione digitale e mediatica, di valorizzare al meglio la volontà degli adolescenti all'interno dell'ordinamento e di ridurre il più possibile i rischi presenti nel mondo digitale.

Quanto appena rilevato ci porta a ritenere che la norma italiana sul limite di età debba essere qualificata come norma di applicazione necessaria perché risulta la più idonea a disciplinare la validità del consenso espresso da minori abitualmente residenti in Italia. Diversamente, una soluzione fondata sulle norme bilaterali di conflitto rischierebbe di assoggettare il minore alla legge di uno Stato non strettamente collegato con la fattispecie e di privare il minore del più elevato standard di protezione accordato dal diritto della sua residenza abituale, impedendo così la realizzazione del risultato sostanziale che si prefigge l'art. 8 del GDPR. Nondimeno l'ambivalenza del limite rende estremamente difficile operare una qualsiasi comparazione tra la norma nazionale sul limite del consenso e l'omologa norma straniera individuata dalle norme di conflitto, al fine di valutare eventualmente l'esistenza di un analogo livello di protezione dell'interesse perseguito.[39]

L'obbligo di attribuire considerazione primaria all'interesse del minore deve quindi ritenersi prevalente rispetto all'esigenza di garantire certezza del diritto e trasparenza ai titolari (o responsabili) del trattamento, i quali nell'ipotesi in cui offrano servizi in Italia saranno onerati di verificare la residenza abituale degli interessati, non risultando sufficiente uniformarsi alla legge locale.

4. La determinazione e la valutazione del danno nelle domande risarcitorie per violazione del trattamento dei dati personali

Con riferimento alle domande risarcitorie per violazione del trattamento dei dati personali il GDPR stabilisce un quadro di norme di natura materiale uniforme che copre diversi profili: i criteri di imputazione e di esonero della responsabilità, il regime della responsabilità solidale e le condizioni di esercizio del diritto di rivalsa.

In particolare, ai sensi dell'art. 82, par. 1, chiunque abbia subito un danno materiale o immateriale cagionato da una violazione del regolamento ha diritto al risarcimento da parte del titolare o del responsabile del trattamento.

Nell'ottica di garantire all'interessato un risarcimento integrale dei danni subiti, il par. 4 della disposizione sopra citata introduce un regime di responsabilità solidale per tutti i soggetti coinvolti nelle medesime operazioni di trattamento e responsabili del pregiudizio prodotto. Resta comunque ferma la possibilità per il titolare o il responsabile del trattamento, che abbia pagato l'intero risarcimento del danno, di proporre un'azione di regresso contro gli altri titolari o responsabili per la porzione di risarcimento corrispondente alla loro parte di responsabilità per il danno causato (art. 82, par. 5).

[39] Su un piano più generale, Marongiu Buonaiuti (2017) afferma la riconducibilità delle disposizioni del GDPR alla nozione di norme di applicazione necessaria sulla base dell'art. 48 che esclude il riconoscimento di decisioni giudiziarie o adottate da autorità amministrative di Stati terzi che richiedano al titolare o al responsabile del trattamento di trasferire o rivelare dati personali, in assenza di un accordo internazionale in vigore tra lo Stato in questione e l'Unione europea o un suo Stato membro, salvo che il regolamento stesso disponga diversamente. Sulla questione si vedano anche Brkan (2015) e Kohler (2016).

Il regime giuridico sinteticamente delineato ha portato la dottrina a ritenere che la responsabilità in materia di protezione dei dati personali si configura come responsabilità semi-oggettiva per il titolare del trattamento, giacché la prova liberatoria è confinata entro limiti angusti e prescinde dalla colpa. In particolare, il titolare del trattamento per non incorrere in responsabilità deve dimostrare che l'evento dannoso non è a lui imputabile perché causato da una fonte estranea alla propria sfera di controllo oppure perché ha predisposto e messo in atto tutte le misure adeguate al fine di evitare che il danno si verificasse (artt. 24 e 32).[40] Diversamente il responsabile del trattamento può essere chiamato a rispondere per i danni causati dal trattamento dei dati personali unicamente in presenza di violazioni di obblighi specificamente posti dal regolamento in capo ai responsabili del trattamento ovvero in caso di violazione di istruzioni specificamente date dal titolare dei dati in ordine al trattamento dei dati stessi (Cordeiro 2019, Tosi 2019, Strugala 2020).

L'impostazione seguita dal GDPR pare collocarsi in linea di continuità con la Direttiva dati, dal momento che questa impiegava la stessa formula di esonero dalla responsabilità, indicando quali esempi concreti il caso di errore della persona interessata e il caso di forza maggiore. Il regime giuridico di imputazione della responsabilità trova la sua giustificazione nel fatto che l'attività di trattamento dei dati è generalmente di "portata massiva" e interferisce con i fondamentali diritti e libertà della persona. Le condotte realizzate nel corso delle operazioni di trattamento generalmente risultano essere piuttosto sofisticate, il che rende estremamente difficile, se non impossibile, per il danneggiato dimostrare la colpa del titolare (o responsabile) del trattamento e il danno non patrimoniale subito, con il rischio di vanificare le possibilità di tutela.

Il corpo di norme di diritto sostanziale sulla responsabilità civile per trattamento dei dati personali è tuttavia tutt'altro che completo, non includendo al proprio interno alcuni profili quali la prescrizione dell'azione risarcitoria, la sospensione della prescrizione e soprattutto i criteri per la valutazione del danno. In mancanza di armonizzazione, per determinare la legge applicabile a questi aspetti, risulta necessario riferirsi al diritto internazionale privato, in particolare alle norme di conflitto in materia di responsabilità contrattuale ed extracontrattuale in vigore nello Stato membro del foro.

Nel quadro dell'ordinamento italiano, nel vigore della Direttiva dati, l'art. 15 del Codice in materia di protezione dei dati personali, intitolato "danni cagionati per effetto del trattamento", prevedeva che chiunque cagionasse danni ad altri per effetto del trattamento di dati personali fosse tenuto al risarcimento ai sensi dell'art. 2050 del Codice civile. Si specificava inoltre che il danno non patrimoniale fosse risarcibile anche in caso di violazione delle disposizioni sulle "modalità del trattamento e requisiti dei dati". Detta disposizione è stata abrogata dall'art. 27 del d.lgs. n. 101/2018 per cui tale profilo

[40] L'art. 24, par. 1, del GDPR prevede che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente disciplina dell'Unione. Dette misure devono essere riesaminate e aggiornate qualora necessario. Il successivo art. 32 indica, collegandosi alla disposizione precedentemente menzionata, i criteri in base ai quali devono essere applicate le opportune misure tecniche e organizzative per garantire un livello di protezione adeguato al rischio. Tra questi figurano "lo stato dell'arte e i costi di attuazione, nonché la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche".

rimane unicamente disciplinato dall'art. 82 del GDPR che riconosce all'interessato il diritto all'integrale risarcimento del danno, comprensivo dei danni materiali e morali.

La questione della risarcibilità del danno per violazione dei dati personali ha in più occasioni interessato la giurisprudenza italiana che si è soffermata in particolare sulla configurabilità e sulla valutazione del danno non patrimoniale (Comandè 2007, Bargelli 2007, Ramaccioni 2009, Tosi 2019). In proposito, la Corte di Cassazione ha chiarito che la risarcibilità del danno non patrimoniale non può essere confinata alle sole ipotesi di pregiudizio derivante da violazione di disposizioni che costituiscano, ai sensi del Codice in materia di protezione dei dati personali, illeciti di rilievo penale. La Corte ha inoltre affermato il principio di diritto secondo cui il danno non patrimoniale, pur determinando una lesione del diritto fondamentale alla protezione dei dati personali, tutelato dall'art. 2 Cost., nonché dall'art. 8 della Convenzione Edu, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno", in quanto anche per tale diritto opera il bilanciamento con i principi di solidarietà e di tolleranza della lesione minima riconducibili all'art. 2 Cost. Di conseguenza, la mera violazione delle prescrizioni sulla modalità del trattamento e sui requisiti dei dati personali determina una lesione ingiustificata del diritto fondamentale alla protezione dei dati personali soltanto quando risulta offesa in modo sensibile, cioè oltre la soglia di tollerabilità, la sua portata effettiva, ferma restando la necessità di accordare una tutela piena della persona umana.[41] La giurisprudenza si è infine interrogata sulla possibilità che il danno non patrimoniale sia risarcibile, indipendentemente dal fatto che si siano in concreto realizzate ulteriori conseguenze nocive (intese come danno-conseguenza). Sul punto il giudice di legittimità ha affermato che il danno per violazione della disciplina a tutela dei dati personali, come ogni danno non patrimoniale, non può sussistere *in re ipsa* perciò, anche in presenza di un'acclarata illiceità nelle modalità di trattamento dei dati, al fine di dichiarare la risarcibilità del danno non patrimoniale, occorre verificare la reale consistenza del pregiudizio lamentato che quindi si configura come elemento autonomo rispetto alla lesione dell'interesse alla tutela dei dati personali. Tale soluzione, che persegue evidentemente lo scopo di porre un argine alle liti bagatellari, si colloca nel solco della tradizionale ricostruzione della responsabilità civile, incentrata sulla sua funzione riparatoria, a discapito della funzione preventiva e sanzionatoria (Ducato 2016).

Il fatto che gli Stati membri abbiano norme di diritto civile e orientamenti giurisprudenziali diversi sulla determinazione e valutazione del danno per illecito trattamento dei dati personali potrebbe favorire fenomeni di *forum shopping* o di *law shopping*.

La possibilità che gli interessati ricerchino il foro potenzialmente più conveniente per promuovere il giudizio di risarcimento dei danni per violazione della disciplina sulla tutela dei dati personali è in qualche modo "fisiologica", in ragione delle peculiarità dei sistemi processuali dei diversi Stati membri. La facoltà di scegliere tra i giudici dello Stato membro della propria residenza abituale e quelli dello stabilimento del titolare del trattamento, concessa al titolare del diritto alla tutela dei dati personali dall'art. 79 del

[41] Corte di Cassazione, sez. III civile, sentenza del 15 luglio 2014, n. 16133; sez. VI civile, ordinanza del 20 agosto del 2020, n.17383.

GDPR, porterà lo stesso a privilegiare il foro in cui il risarcimento dei danni è ammesso sulla base di meccanismi probatori meno rigorosi.

Egualmente il *forum shopping* è incentivato nel caso di domanda di risarcimento dei danni che sia riconducibile a un illecito non contrattuale, che pare essere l'ipotesi più frequente in materia. In tal caso, considerato che il Regolamento Roma II esclude dal suo ambito di applicazione le obbligazioni extracontrattuali derivanti da violazione della disciplina in materia di tutela dei dati personali, al fine di determinare la legge applicabile, è necessario fare riferimento alle norme del diritto internazionale privato nazionali del paese del giudice adito. È evidente che in mancanza di norme uniformi per l'individuazione del diritto applicabile, l'interessato sarà incline a rivolgersi al foro in cui le proprie pretese hanno maggiori possibilità di essere riconosciute e ciò in funzione non solo del contenuto della legge che verrà individuata come applicabile, ma anche delle leggi nazionali di adattamento al GDPR, visto che il loro ambito di applicazione è generalmente determinato sulla base di norme autolimitanti.

Nell'ipotesi in cui la domanda risarcitoria sia rivolta al giudice italiano, viene in considerazione l'art. 62 della legge n. 218/1995 dal titolo "responsabilità per fatto illecito". Tale disposizione, che com'è noto, risulta applicabile solo per le ipotesi che il Regolamento Roma II espressamente esclude dal suo ambito di applicazione, prevede al comma 1 che la responsabilità per fatto illecito è regolata, in linea generale, dalla legge dello Stato in cui si è verificato l'evento dannoso (*lex loci damni*). In alternativa, qualora il danneggiato lo richieda, dalla legge dello Stato in cui si è verificato il fatto che ha causato il danno (*lex loci commissi delicti*), ovvero la legge del luogo in cui si è svolta l'azione illecita. Secondo l'art. 62, comma 2, qualora il fatto illecito coinvolga soltanto cittadini di un medesimo Stato in esso residenti, si applica la legge di tale Stato e non è ammessa alcuna scelta. La legge applicabile regola l'intera fattispecie della responsabilità civile, fra cui la determinazione dell'area del danno risarcibile e i criteri di valutazione economica del pregiudizio. La scelta di tali criteri di collegamento è ispirata al c.d. "principio dell'ubiquità", più volte affermato dalla Corte di Giustizia riguardo al criterio speciale di giurisdizione previsto dall'art. 5, n. 3), della Convenzione di Bruxelles e dai rispettivi art. 5, n. 3), e art. 7, n. 2), dei due regolamenti che le sono succeduti. La disposizione, tuttavia, non pone i due criteri su un piano di equivalenza, poiché in mancanza di espressa richiesta del danneggiato viene applicata automaticamente la legge del luogo in cui si è verificato l'evento (Davì 1997, Tonolo 2001, Marongiu Buonaiuti 2013).

Il ricorso all'*optio legis* a favore del danneggiato, per quanto circoscritta, determinerà verosimilmente fenomeni di *law shopping*, poiché l'interessato potrà chiedere, alternativamente, l'applicazione della *lex loci damni* o della *lex loci commissi delicti*, a seconda di quella che risulti più favorevole in ordine alla determinazione e valutazione del danno. Occorre pure considerare che, ai sensi del diritto internazionale privato italiano, per "fatto che ha causato il danno" deve intendersi l'attività propriamente esecutiva, per cui nel caso in cui atti esecutivi siano stati compiuti in Stati diversi, le relative leggi assumono tutte rilievo sicché la scelta del danneggiato potrà ricadere su ciascuna di esse. Il ventaglio delle leggi che possono essere oggetto della scelta del danneggiato sarebbe ancor più ampio nell'ipotesi in cui il danno si sia prodotto nel territorio di più Stati. L'inammissibilità del rinvio, sancita dall'art. 13, comma 2, della

legge n. 218/1995 valorizza peraltro l'opzione concessa al danneggiato perché questo sarà agevolato nel prevedere con esattezza la legge applicabile, non dovendo tenere conto delle norme di conflitto dell'ordinamento straniero designato dalle norme di conflitto del foro.

Il criterio del luogo in cui si verifica il danno appare di difficile concretizzazione perché porta alla moltiplicazione delle leggi applicabili, almeno in quei casi in cui il pregiudizio si produce contemporaneamente in tutti i luoghi in cui è consentito l'accesso alla rete.[42]

La possibilità per l'interessato di optare per l'applicazione della legge del luogo della condotta dannosa si scontra parimenti con la difficoltà di individuare tale legge in ragione del carattere virtuale delle mezzo nel cui contesto generalmente si verificano le violazioni del diritto alla tutela dei dati personali. In proposito, parte della dottrina sostiene che la *lex loci commissi delicti* andrebbe identificata con quella del luogo in cui i dati si trovavano fisicamente nel momento in cui si è verificato il danno. Tale soluzione, tuttavia, non è esente da difficoltà e incertezze, giacché il danneggiato, a causa delle caratteristiche della rete internet, non ha il più delle volte la possibilità di conoscere la collocazione dei dati personali o può reperire tale informazione soltanto a fronte di un costo elevato. Appare sul punto degna di nota la posizione assunta dalla Corte di Giustizia nel caso Wintersteiger del 2012, seppure in punto di competenza giurisdizionale. Il caso originava dalla violazione di un marchio nazionale registrato in uno Stato membro a causa della comparsa, sul sito internet di un motore di ricerca, di una pubblicità a seguito dell'utilizzo di una parola chiave identica a detto marchio.[43] In detta decisione i giudici di Lussemburgo hanno affermato che il fatto generatore del danno non va identificato nella comparsa della pubblicità, ma piuttosto nell'avviamento, da parte dell'inserzionista, del processo tecnico finalizzato alla comparsa dell'annuncio. Secondo la Corte, anche se l'avvio del processo tecnico da parte dell'inserzionista è

[42] Tale soluzione trova un qualche riscontro nella giurisprudenza della Corte di Giustizia relativa al caso *Shevill e a. c. Presse Alliance* con riguardo al profilo della competenza giurisdizionale (Corte di giustizia, sent. 7 marzo 1995, causa C-68/93, ECLI:EU:C:1995:61). In detta decisione i giudici avevano affermato che l'art. 5, n. 3), della Convenzione di Bruxelles del 1968 consentiva al soggetto leso di agire in giudizio nello Stato del luogo in cui era stato commesso il fatto causale del danno (il domicilio dell'editore responsabile della pubblicazione diffamatoria) o nello Stato in cui si era concretizzato il danno, circostanza dipendente dalla distribuzione territoriale del mezzo che conteneva il materiale diffamatorio. Il giudice del luogo in cui si era concretizzato il danno era competente solo a conoscere dei danni occorsi specificamente nello Stato membro di appartenenza, circostanza che doveva essere accertata in base al livello di distribuzione e vendita del mezzo in detto Stato. Questo principio di ripartizione delle competenze è stato definito dalla dottrina come "approccio a mosaico". La Corte si è ulteriormente occupata della questione nella causa *eDate Advertising e a.* (sent. 25 ottobre 2011 cit.) concernente un mezzo di comunicazione *on-line*. I giudici di Lussemburgo hanno in proposito affermato che tali situazioni si distinguono da quelle in cui i contenuti non sono in rete a causa, da un lato, della potenziale ubiquità dei contenuti in rete e, dall'altro, della difficoltà di individuare un metodo di misurazione dell'impatto territoriale della notizia lesiva. Ciò ha indotto la Corte a integrare la c.d. regola del "principio del mosaico", con un criterio aggiuntivo che individua quale titolo di giurisdizione il centro di interessi del soggetto leso. I giudici di tale luogo sono competenti a conoscere del merito di una domanda di risarcimento per la totalità del danno subito, perché l'impatto di contenuti in rete sui diritti della personalità di un soggetto può essere ivi meglio valutato. Sebbene il criterio del centro di interessi della vittima sia stato elaborato dalla Corte con esclusivo riguardo alle ipotesi di violazione dei diritti della personalità, per alcuni autori può essere applicato per analogia al campo della protezione dei dati personali, in ragione dell'analoga facilità di accesso al mezzo di comunicazione e della natura dei diritti coinvolti. In dottrina sul tema si vedano Bogdan (2011), Bollée e Haftel (2012), Muir Watt (2012) e Feraci (2012).

[43] Corte di giustizia, sent. 19 aprile 2012, causa C-523/10, *Wintersteiger*, ECLI:EU:C:2012:220.

effettuato su di un server appartenente al gestore del motore di ricerca utilizzato dall'inserzionista, il luogo in cui è stabilito detto server non può essere considerato quello del fatto generatore del danno, in ragione, da un lato, della sua localizzazione incerta e, dall'altro, dell'obiettivo di prevedibilità cui devono tendere le regole sulla competenza.

Diversamente la soluzione che identifica la *lex loci commissi delicti* con il luogo di stabilimento del soggetto che ha trattato i dati presenta una sufficiente prevedibilità in quanto detto luogo è suscettibile di essere determinato sulla base di dati certi, anche se implica il rischio che il titolare (o il responsabile) del trattamento possa alterare il fattore di connessione, spostando la propria attività in uno Stato poco sensibile alla tutela dei dati personali, rendendo di fatto poco utile l'*optio legis* accordata al danneggiato (Feraci 2012, e Marino 2012).

5. Considerazioni conclusive

Il Regolamento Generale sulla Protezione dei dati (Regolamento (UE) 2016/679 - GDPR), rappresenta un importante tassello della strategia dell'Unione europea per il mercato unico digitale. La sua adozione è legata anche all'esigenza di semplificazione del quadro giuridico in materia. Tale necessità si riscontra sia in relazione al public (administrative) enforcement, incentrato sui poteri di azione dell'autorità di controllo, sia in relazione al private enforcement, incentrato sul diritto di ottenere il risarcimento del danno riconosciuto a "chiunque" abbia subito un danno "materiale o immateriale" causato da una violazione del regolamento. L'obiettivo, tuttavia, è stato solo parzialmente raggiunto poiché permangono diversi aspetti della disciplina che appaiano incerti e problematici.

Nell'ambito del public (administrative) enforcement, il regolamento non specifica come l'azione dell'autorità di controllo – sia essa sollecitata o meno dall'interessato – possa conciliarsi con il rimedio civilistico. Parimenti lo strumento non si preoccupa di definire gli effetti delle decisioni delle autorità di controllo straniere ai fini dell'azione di risarcimento danni. Considerato che a livello degli ordinamenti nazionali dette questioni hanno ricevuto risposte assai diverse, i rischi di contraddizioni nell'applicazione del regolamento e ingiustificate complicazioni procedurali nelle azioni di risarcimento del danno appaiono alquanto accentuati, soprattutto nell'ipotesi di trattamento transfrontaliero.

Nell'ambito del private enforcement, l'esigenza di semplificazione è stata la ragione principale che ha portato il legislatore a scegliere di sostituire la Direttiva 95/46/CE con il diverso strumento giuridico del regolamento: le disposizioni dettagliate, uniformi e direttamente applicabili avrebbero dovuto esaurire le questioni legate ai conflitti di leggi. Il regolamento, tuttavia, lascia agli Stati membri un ampio spazio di intervento per ampliare, limitare o finanche derogare alla disciplina contenuta nel GDPR. Tale facoltà copre aspetti importanti del diritto alla tutela dei dati personali, fra le quali l'individuazione della soglia di età del minore per esprimere validamente il consenso al trattamento dei propri dati personali.

Tale assetto normativo comporta che le questioni legate all'individuazione del diritto applicabile non solo continuano a porsi, ma possono essere in alcuni casi particolarmente rilevanti. Nel caso in cui una fattispecie risulti disciplinata dalle disposizioni nazionali

di adeguamento al regolamento, la questione di determinare la legge applicabile appare alquanto complessa, dato che i legislatori degli Stati membri hanno fatto ricorso a soluzione assai diverse per delimitare l'ambito di applicazione spaziale delle leggi nazionali. Sussiste, inoltre, il rischio concreto che più leggi nazionali di adeguamento rivendichino parallelamente la propria applicazione a una determinata attività di trattamento (conflitti di leggi "positivi") o, al contrario, che nessuna legge nazionale di adeguamento rivendichi la propria applicabilità nel caso specifico (conflitti di leggi "negativi").

L'esame della disposizione relativa all'età del consenso del minore per il trattamento dei propri dati personali evidenzia che esigenze di chiarezza imporrebbero al legislatore dell'Unione di indicare se nello spazio di intervento riservato agli Stati membri alcune disposizioni possano delinearsi come norme di applicazione necessaria e collocarsi dunque nella "sfera di eccezione" del diritto internazionale privato tradizionale, basato su norme di confitto di matrice bilaterale. In mancanza di chiarezza sul punto appare quindi probabile che le imprese che trattano dati personali decidano di rispettare l'età massima prevista dal regolamento, ovvero i sedici anni, per essere certe di non violare alcuna normativa nazionale, pregiudicando così l'autonomia riconosciuta ai minori dalla loro legge di residenza.

Un ulteriore aspetto della ricerca di semplificazione è riconducibile alla presenza di norme di natura materiale uniforme che coprono diversi profili delle domande risarcitorie per violazione del trattamento dei dati personali. Questo corpo di norme è tuttavia incompleto, non includendo al proprio interno altri aspetti, fra i quali i criteri per la valutazione del danno. In mancanza di armonizzazione, per determinare la legge applicabile a detta questione, risulta necessario riferirsi al diritto internazionale privato, in particolare alle norme di conflitto in materia di responsabilità contrattuale ed extracontrattuale in vigore nello Stato membro del foro, con il rischio di incentivare fenomeni di forum shopping o di law shopping.

La poca attenzione prestata dal legislatore dell'Unione europea all'interazione tra il GDPR e le nuove leggi statali di adeguamento determina in definitiva un quadro giuridico tutt'altro che semplice e prevedibile, indebolendo, a causa della mancanza di omogeneità, il livello generale di protezione delle persone fisiche. La mancanza di certezza giuridica e operativa rischia quindi di condurre a uno sviluppo dell'economia digitale nel mercato interno non equilibrato, in cui i diritti sanciti non potranno essere sistematicamente garantiti.

La pratica legale e la giurisprudenza avranno nei prossimi anni il compito di individuare e risolvere le possibili carenze del GDPR, dando indicazioni al legislatore per le successive riforme che si renderanno necessarie.

Riferimenti

Arnull, A., 2011. The Principle of Effective Judicial Protection in EU law: An Unruly Horse? *European Law Review* [online], 36(1), 51–70. Disponibile alla pagina: https://www.researchgate.net/profile/Anthony-Arnull/publication/290568823_The_Principle_of_Effective_Judicial_Protection_in_EU_law_An_Unruly_Horse/links/5755ae5108ae155a87b9c8cb/The-Principle-of-

Effective-Judicial-Protection-in-EU-law-An-Unruly-Horse.pdf [Accesso il 26 settembre 2022].

Barel, B., 2004. Commento all'art. 23, 44 ss. *In:* G. Cian ed A. Trabucchi, eds., *Commentario breve al Codice Civile, Diritto internazionale privato e Diritto societario prima della riforma*, VII ed. Padova: Cedam.

Bargelli, E., 2007. Art. 15: Danni cagionati per effetto del trattamento: II: comma 2°. *In:* C.M. Bianca e F.D., Busnelli, *La protezione dei dati personali, Commentario al D.lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*. Padova: Cedam, 410–426.

Bilotta, F., 2019. La responsabilità civile nel trattamento dei dati personali, 445-470. *In:* R. Panetta, ed., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*. Milano: Giuffrè.

Bogdan, M., 2011. Defamation on the Internet, Forum Delicti and the E-Commerce Directive: Some Comments on the ECJ Judgment in the eDate Case. *Yearbook of Private International Law*, 13, 483–491.

Bollée, S., e Haftel, B., 2012. Les nouveaux (dés)équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez. *Recueil Dalloz*, 1285-1293.

Brkan, M., 2015. Data Protection and European Private International Law. *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS* [online], 2015/40, 1–37. Disponibile alla pagina: https://cadmus.eui.eu/bitstream/handle/1814/36335/RSCAS_2015_40.pdf?sequence=1&isAllowed=y [Accesso il 26 settembre 2022].

Brkan, M., 2016. Data Protection and Conflict-of-laws: A Challenging Relationship. *European Data Protection Law Review (EDPL)*, 2(3), 324–341.

Caggiano, I.A., 2021. Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale. *Annali-Università degli Studi Suor Orsola Benincasa* [online], 11(1), 7–50. Disponibile alla pagina: https://universitypress.unisob.na.it/ojs/index.php/annali/article/view/1202 [Accesso il 26 settembre 2022].

Chen, J., 2016. How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation. *International Data Privacy Law*, 6(4), 310–323.

Clerici, R., 1996. Commento all'art. 47, 1298 ss. *In:* S. Bariatti, ed., *Commentario alla Legge 31 maggio 1995 n. 218, Riforma del sistema italiano di Diritto Internazionale Privato*, in *Le nuove leggi civili commentate*.

Comandè, G., 2007. Art. 15: Danni cagionati per effetto del trattamento: I: comma 1°. *In:* C.M. Bianca e F. D., Busnelli, *La protezione dei dati personali, Commentario al D.lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*. Padova: Cedam, 362–409.

Cordeiro, A.B., 2019. Civil Liability for Processing of Personal Data in the GDPR. *European Data Protection Law Review*, 5(4), 492–499.

Davì, A., 1981. *L'adozione nel diritto internazionale privato italiano*. Milano: Giuffrè.

Davì, A., 1990. Le questioni generali del diritto internazionale privato nel progetto di riforma. *Rivista di diritto internazionale*, 73, 556–638.

Davì, A., 1997. *La responsabilità extracontrattuale nel nuovo diritto internazionale privato italiano*. Torino: UTET.

De Franceschi, A., 2019. Il "pagamento" mediante dati personali. *In:* V. Cuffaro, R. D'Orazio e V. Ricciuto, eds., *I dati personali nel diritto europeo*. Torino: Giappichelli, 1381–1413.

De Hert, P., e Czerniawski, M., 2016. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law* [online], 6(3), 230–243. Disponibile alla pagina: https://www.researchgate.net/profile/Michal-Czerniawski/publication/305340840_Expanding_the_European_data_protection_scope_beyond_territory_Article_3_of_the_General_Data_Protection_Regulation_in_its_wider_context/links/60ed8d910859317dbddb8d5e/Expanding-the-European-data-protection-scope-beyond-territory-Article-3-of-the-General-Data-Protection-Regulation-in-its-wider-context.pdf [Accesso il 26 settembre 2022].

Ducato, R., 2016. La lesione della privacy di fronte alla "soglia di risarcibilità": la nuova Maginot del danno non patrimoniale? *International Review of Law, Computers and Technology*, 4, 1–10.

Feraci, O., 2012. Diffamazione internazionale a mezzo di Internet: quale foro competente? Alcune considerazioni sulla sentenza eDate. *Rivista di diritto internazionale*, 95(2), 461–469.

Giordano, R., 2019. La tutela amministrativa e giurisdizionale dei dati personali. *In:* V. Cuffaro, R. D'Orazio e V. Ricciuto, eds., *I dati personali nel diritto europeo*. Torino: Giappichelli, 1001–1016.

Gömann, M., 2017. The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement. *Common Market Law Review*, 54(2), 567–590.

González Fuster, G., 2014. *The emergence of personal data protection as a fundamental right of the EU.* Cham: Springer International.

Guardigli, E., 2017. Il garante per la protezione dei dati e la cooperazione fra autorità garanti. Le Autorità di controllo. *In:* G. Finocchiaro, ed., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Bologna: Zanichelli, 489–515.

Helberger, N., Zuiderveen Borgesius, F., e Reyna, A., 2017. The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law. *Common Market Law Review*, 54(5), 1427–1465.

Kohler, C., 2016. Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union. *Rivista di diritto internazionale privato e processuale*, 52(3), 653–675.

Kokott, J., e Sobotta, C., 2013. The Distinction between Privacy and Data Protection in the jurisprudence of the CJEU and the ECHR. *International Data Privacy Law* [online], 3(4), 222–228. Disponibile alla pagina: https://ejtn.eu/PageFiles/19789/J.Kokott%20and%20C.%20Sobotta%20The%20distinction%20between%20privacy%20and%20data%20protection%20in%20the%20jurisprudence%20of%20the%20CJEU%20and%20the%20ECtHR.pdf [Accesso il 26 settembre 2022].

Koutra, A.A., 2019. Les situations de conflits de lois entre Etats membres dans le cadre du RGPD: une analyse à la lumière de l'exemple du consentement du mineur au traitement de ses données à caractère personnel. *Faculté de droit et de criminologie, Université catholique de Louvain* [online], 1–75. Disponibile alla pagina: https://dial.uclouvain.be/memoire/ucl/en/object/thesis%3A20098 [Accesso il 26 settembre 2022].

Krivokapić, D., ed Adamović, J., 2016. Impact of General Data Protection Regulation on Children's Rights in Digital Environment. *Belgrade Law Review* [online], 64(3), 205–220. Disponibile alla pagina: https://scindeks-clanci.ceon.rs/data/pdf/0003-2565/2016/0003-25651603205k.pdf [Accesso il 26 settembre 2022].

Kuipers, J.J., 2012. *EU law and private international law: the interrelationship in contractual obligations*. Leiden/Boston: Brill/Nijhof.

Kuner, C., 2021. *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection* [online]. University of Cambridge Faculty of Law Research Paper, 20, 1–35. Disponibile alla pagina: https://ssrn.com/abstract=3827850 [Accesso il 26 settembre 2022].

Langhanke, C., e Schmidt-Kessel, M., 2015. Consumer data as consideration. *Journal of European Consumer and Market Law,* 4(6), 218–223.

Livingstone, S., Carr, J., Byrne J., 2016. *One in Three: Internet Governance and Children's Rights* [online]. Innocenti Discussion Paper n. 2016-01. Firenze: UNICEF Office of Research, 1–36. Disponibile alla pagina: https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf [Accesso il 26 settembre 2022].

Macenaite, M., 2017. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779.

Mantovani, M., 2019. Horizontal conflicts of member states' GDPR-complementing laws: the quest for a viable conflict-of-laws solution. *Rivista di Diritto Internazionale Privato e Processuale*, 55(3), 535–562.

Marino, S., 2012. La violazione dei diritti della personalità nella cooperazione giudiziaria civile europea. *Rivista di diritto internazionale privato e processuale*, 48(2), 363–380.

Marongiu Buonaiuti, F., 2013. *Le obbligazioni non contrattuali nel diritto internazionale privato*. Milano: Giuffrè.

Marongiu Buonaiuti, F., 2017. La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con

la disciplina contenuta nel regolamento "Bruxelles I-bis". *Cuadernos de Derecho Transnacional* [online], 9(2), 448–464. Disponibile alla pagina: https://doi.org/10.20318/cdt.2017.3881 [Accesso il 26 settembre 2022].

McCullagh, K., 2016. The general data protection regulation: a partial success for children on social network sites? *In:* T. Bräutigam e S. Miettinen, eds., *Data protection, privacy and european regulation in the digital age* [online], 110–139. Helsinki: Forum Iuris. Disponibile alla pagina: https://ssrn.com/abstract=2985724 [Accesso il 26 settembre 2022].

Muir Watt, H., 2012. Cour de justice de l'Union européenne. (C-509/09 et C-161/10 aff.jtes). - 25 octobre 2011. *Revue critique de droit international privé*, 389–411.

Piñar Mañas, J.L., 2018. L'oggetto del Regolamento Generale sulla protezione dei dati: tra diritto alla privacy e libera circolazione dei dati personali. *In:* A. Mantelero e D. Poletti, eds., *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* [online]. Pisa University Press, 53–67. Disponibile alla pagina: https://www.dimt.it/wp-content/uploads/2019/05/images_pdf_regolarelatecnologia.pdf [Accesso il 26 settembre 2022].

Piroddi, P., 2014a. Art. 16 TFUE, 189 ss. *In:* F. Pocar e M.C. Baruffi, eds., *Commentario breve ai trattati dell'Unione europea*. Padova: Cedam.

Piroddi, P., 2014b. Art. 8 Carta dei diritti fondamentali dell'Unione europea, 1682 ss. *In:* F. Pocar e M.C. Baruffi, eds., *Commentario breve ai trattati dell'Unione europea*. Padova: Cedam.

Pizzetti, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo regolamento europeo* (vol. 1). Torino: Giappichelli.

Ragno, F., 2020. Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR. *Ordine internazionale e diritti umani* [online], 4, 818–838. Disponibile alla pagina: https://www.rivistaoidu.net/wp-content/uploads/2021/12/4_RAGNO.pdf [Accesso il 26 settembre 2022].

Ramaccioni, G., 2009. La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali, 243 ss. *In:* F. Ruscello, ed., *Studi in Onore di Davide Messinetti* (vol. 2). Napoli: Edizioni Scientifiche Italiane.

Rossolillo, G., 2019. Diritti fondamentali, norme unilaterali e norme imperative alla luce del regolamento 2016/679 sul trattamento e la libera circolazione dei dati personali. *In:* G. Contaldi *et al*., eds., *Liber amicorum Angelo Davì. La vita giuridica internazionale nell'età della globalizzazione* (vol. 1). Napoli: Editoriale Scientifica, 597–617.

Sica, S., 2001. Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica. *Rivista di diritto civile*, 6, 621–641.

Spoto, G., 2016. Disciplina del consenso e tutela del minore. *In:* S. Sica, V. D'Antonio e G.M. Riccio, eds., *La nuova disciplina europea della privacy*. Padova: Cedam, 111–130.

Strugala, R., 2020. Art. 82 GDPR: Strict Liability or Liability Based on Fault? *European Journal of Privacy Law & Technologies* [online], special issue, 71–79. Disponibile alla

pagina: https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1133/373 [Accesso il 26 settembre 2022].

Tonolo, S., 2001. *Art. 54*, 305 ss. *In:* G. Conetti, S. Tonolo e F. Vismara, eds., *Commento alla riforma del diritto internazionale privato italiano*. Torino: Giappichelli.

Tosi, E., 2019. *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*. Milano: Giuffrè.

Trocker, N., 2002. L'articolo 47 della Carta dei diritti fondamentali dell'Unione europea e l'evoluzione dell'ordinamento comunitario in materia di tutela giurisdizionale dei diritti. *In:* G. Vettori, ed., *Carta europea e diritti dei privati.* Padova: Cedam, 381–417.

Ubertazzi, B., 2006. *La capacità delle persone fisiche nel diritto internazionale privato*. Padova: Cedam.

van Bochove, L.M., 2014. Overriding Mandatory Rules as a Vehicle for Weaker Party Protection in European Private International Law. *Erasmus Law Review* [online], 3, 147–156. Disponibile alla pagina: https://doi.org/10.5553/ELR.000030 [Accesso il 26 settembre 2022].

Varney, M., 2016. Effective Redress of Grievance in Data Protection: An Illusion? *Maastricht Journal of European and Comparative Law* [online], 23(3), 550–567. Disponibile alla pagina: https://core.ac.uk/download/pdf/151161407.pdf [Accesso il 26 settembre 2022].

Woods, L., 2021. Facebook Ireland and the one stop shop under the GDPR. *European Law Review*, 5, 685–691.