Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero

The GDPR and the protection of the data subject between public and private enforcement in the case of cross-border processing

Livio Scaffidi Runchella
Assegnista di ricerca in Diritto Internazionale dell'Università degli Studi di Messina

Recibido: 06.09.2022 / Aceptado: 23.09.2022
DOI: 10.20318/cdt.2023.8083

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. Lo strumento lascia agli Stati membri dell'Unione europea ampi margini di autonomia processuale, particolarmente nel caso di trattamenti transfrontalieri. Per tale ragione emergono diversi problemi che riguardano la competenza giurisdizionale, il rapporto tra procedimenti paralleli siano essi di natura civile o amministrativa, il rapporto fra il rimedio amministrativo e l'azione di risarcimento del danno. 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.

Parole chiave: Trattamento dei dati personali, Regolamento (UE) n. 2016/679, Giurisdizione, Autorità di controllo e autorità giurisdizionali.

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. The legal instrument offers the Member States of the European Union wide margins of procedural autonomy, particularly in situations of cross-border processing. For this reason, various problems arise concerning jurisdictional competence, the relationship between concurrent proceedings whether they be of a civil or administrative nature, the relationship between the administrative remedy and the action for damages. 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.

Keywords: Processing of personal data, Regulation (EU) n. 2016/679, Jurisdiction, Supervisory authorities and judicial authorities.

I. Osservazioni introduttive: il GDPR fra protezione dell'interessato e circolazione dei dati personali.

1. I dati personali si trovano al centro della trasformazione, collegata allo sviluppo delle tecnologie digitali, che nel corso dell'ultimo decennio ha interessato l'economia, la società e, in ultima analisi, quasi tutti gli aspetti della vita quotidiana delle persone. L'incremento, senza precedenti, delle operazioni di raccolta, di archiviazione e di condivisione di dati personali con rilevanza transnazionale è probabilmente l'indice più evidente di tale cambiamento.

Nell'ambito dell'Unione europea, i dati sono considerati una risorsa essenziale per la crescita economica, la competitività, l'innovazione, la creazione di posti di lavoro e il progresso sociale in generale[1]. Nella sua comunicazione del 19 febbraio 2020, dal titolo "*Una strategia europea per i dati*", la Commissione ha manifestato l'intenzione di creare uno "spazio unico europeo di dati", all'interno del quale sia i dati personali sia quelli non personali possano circolare in maniera trans-settoriale, in modo da favorire la competitività globale e la sovranità dei dati dell'Unione europea. Quest'ultima ha pertanto l'urgenza di combinare una legislazione e una *governance* idonee allo scopo, investendo in norme, strumenti e infrastrutture, nonché in competenze per la gestione dei dati.

2. In tale scenario politico il Regolamento (UE) 2016/679 (conosciuto con l'acronimo GDPR – *General Data Protection Regulation*), divenuto applicabile dal 25 maggio 2018, cerca di coniugare il duplice obiettivo di rafforzare il diritto delle persone fisiche alla tutela dei dati personali e di promuovere la libera circolazione degli stessi[2].

Con riferimento al primo dei due obiettivi, il GDPR – in linea di continuità con la Direttiva 95/46/CE – introduce una serie di norme volte a consentire alla persona fisica di poter esercitare il controllo sui propri dati personali. In tal senso, il GDPR può essere annoverato fra gli strumenti che concretizzano il diritto fondamentale alla protezione dei dati, esplicitamente tutelato 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). L'art. 8 riconosce il diritto alla protezione dei dati personali come diritto fondamentale, emancipandolo dal diritto al rispetto per la vita privata e familiare che ha un autonomo fondamento nell'art. 7 CDFUE[3]. L'art. 16 TFUE introduce, invece, una nuova base giuridica per la protezione dei dati personali che interessa tanto il settore privato quanto il settore pubblico[4].

---

[1] Per rendersi conto della portata del fenomeno basti considerare che i dati previsionali per il 2025 riportano che, contestualmente all'aumento del volume globale dei dati (da 33 zettabyte nel 2018 a 175 zettabyte nel 2025), il valore della relativa economia dati nei 27 paesi dell'Unione raggiungerà l'ammontare di 829 miliardi di euro. Tale dato appare assai indicativo, soprattutto ove si consideri che nel 2018 il valore ammontava a 301 miliardi, pari al 2,4% del PIL complessivo degli Stati membri dell'Unione europea. In proposito si veda la Comunicazione della Commissione europea del 19 febbraio 2020, dal titolo "*Una strategia europea per i dati*" (COM/2020/66 final).

[2] Il GDPR può considerarsi parte integrante e rilevante di un quadro normativo che si compone anche della Direttiva (UE) 2016/680 in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini, della Direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, del prossimo regolamento sulla *ePrivacy*, che sostituirà la Direttiva 2002/58/CE, in materia di rispetto della vita privata e la protezione dei dati personali nelle comunicazioni elettroniche (proposta COM(2017) 10 final) e del Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[3] Secondo l'art. 8 della CDFUE «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[4] La Direttiva 95/46/CE aveva infatti come base giuridica l'art. 100 A del TCE (Trattato istitutivo della Comunità europea). Detta norma mirava al ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno, derivanti dalle disparità esistenti tra le normative nazionali. La direttiva, poiché anteriore sia alla Carta dei Diritti Fondamentali dell'Unione europea (CDFUE), sia al Trattato sul Funzionamento dell'Unione europea (TFUE), non poteva fare riferimento né all'uno né all'altro strumento. L'ancoraggio ai diritti fondamentali era piuttosto rappresentato dall'art. 8 della Convenzione europea dei diritti dell'uomo (Convenzione Edu) che riconosce il diritto al rispetto della vita privata e familiare. Il passaggio dalla Direttiva 95/46/CE al GDPR segna dunque un mutamento

3. Con riferimento al secondo dei due obiettivi, il GDPR è uno strumento funzionale alla competizione economica perché permette agli attori del mercato digitale, cioè ai cittadini, alle imprese e alle pubbliche amministrazioni, di non subire ostacoli di carattere giuridico o amministrativo e di poter contare su un insieme di regole condivise[5], alle quali anche i soggetti che operano fuori dall'Unione europea sono tendenzialmente obbligati ad attenersi[6].

I due obiettivi, per un verso, possono essere ritenuti convergenti, quantomeno nella misura in cui la garanzia di un alto livello di protezione dei dati personali determina un clima di fiducia che favorisce la libera circolazione dei dati e lo sviluppo dell'economia digitale[7]; per altro verso, possono tuttavia essere considerati conflittuali, perché le prescrizioni introdotte dal GDPR costituiscono un limite alla circolazione dei dati personali e, al contempo, la principale rete di protezione per il titolare del diritto alla loro tutela, consentendo di contenere l'asimmetria e la diseguaglianza sul piano informativo, tecnologico e normativo, che sussiste nel rapporto che si instaura con il titolare o il responsabile del trattamento. Peraltro, occorre considerare che il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali, sulla base del principio di proporzionalità[8].

4. L'introduzione del GDPR è riconducibile a diverse ragioni. Fra le principali è possibile annoverare la necessità di un aggiornamento della disciplina, quale risposta alle nuove sfide derivanti dalle profonde modifiche tecnologiche e informatiche che si sono verificate a partire dagli anni novanta con un ritmo incessante, nonché la volontà di creare un contesto omogeneo, all'interno del quale i dati

---

del fondamento giuridico, perché il nuovo strumento è stato adottato sulla base dell'art. 16 del TFUE che riconosce il diritto di ogni persona alla protezione dei dati personali che la riguardano, pur includendo anche un riferimento alla libera circolazione di tali dati. La formulazione della norma lascia intendere che la libera circolazione dei dati personali nell'Unione deve comunque rispettare il contenuto del diritto oggetto di tutela. Per un'analisi di tali disposizioni vedasi, per tutti, P. Piroddi, *Art. 16 TFUE*, in F. Pocar, M. C. Baruffi (a cura di), *Commentario breve ai trattati dell'Unione europea*, Padova, 2014, p. 189 ss., nonché Id., *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, *ibidem*, p. 1682 ss. Per una ricostruzione dell'emersione di tale diritto nell'ordinamento dell'Unione europea e della sua trasfigurazione in diritto fondamentale si veda G. Gonzalez Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Dordrecht, 2014, p. 185 ss.

[5] Tale aspetto risulta ancora più evidente ove si consideri che la libera circolazione dei dati costituisce l'obiettivo principale in relazione ai dati non personali. In proposito è possibile fare riferimento al recente Regolamento (UE) 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, entrato in vigore il 28 maggio 2019, che stabilisce un quadro per l'archiviazione e il trattamento dei dati in tutta l'Unione europea, vietando le restrizioni alla localizzazione dei dati se non giustificate e incoraggiando la realizzazione di codici di condotta per i servizi *cloud* per un mercato più flessibile e più accessibile sotto il profilo economico.

[6] Come noto, l'applicazione dei criteri dello stabilimento e del cosiddétto *targeting* previsti dall'art. 3 comporta che gli effetti del GDPR si estendono oltre il territorio dell'Unione europea, disciplinando anche l'attività di operatori che ivi non hanno alcun tipo di stabilimento o presenza. Tale risultato è rafforzato dalle disposizioni di cui al capo V, dal titolo "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali", che prevedono obblighi per gli operatori "extra UE" che trattano dati personali provenienti da soggetti che si trovano nell'Unione europea, anche nelle ipotesi in cui tali operatori non sarebbero, per proprio conto, assoggettati al regolamento. Su questo aspetto si rinvia, fra i tanti, a O. Tene, C. Wolf, *Overextended: jurisdiction and applicable law under the EU general data protection regulation*, in *Future of Privacy Forum White Paper*, 2013; D.J.B. Svantesson, *Extraterritoriality in data privacy law*, *Ex Tuto Publishing*, 2013, pp. 68-69; C. Kuner, *Extraterritoriality and regulation of international data transfers in EU data protection law*, in *International Data Privacy Law*, vol. 5, n. 4, 2015, p. 235-245; M.S.C. Taylor, *Permissions and Prohibitions in Data Protection Jurisdiction*, in *Brussels Privacy HUB Woking Paper n. 6*, 2016, p. 17.

[7] La Commissione nella Comunicazione «Una strategia europea per i dati» (COM(2020) 66 final), al punto 1, evidenzia che «I cittadini daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati». Su questo aspetto in dottrina vedasi N. Michail, C. Ponsart, *Le RGPD:* état *des lieux du règlement central du droit européen de la protection et de la libre circulation des données personnelles*, in *Cahiers de droit europeen*, 2021, 57.3, pp. 727-730. Gli autori evidenziano come la strategia di rinforzare la protezione delle persone fisiche in funzione dell'affermazione della libera circolazione e dello sviluppo del mercato interno è conosciuta in altri settori come quello della tutela dei consumatori e del diritto finanziario. La circolazione dei dati personali è, in tal senso, il presupposto per lo sviluppo delle altre libertà di circolazione previste dal TFUE e il diritto alla protezione dei dati un elemento che condiziona l'esercizio dell'insieme delle altre libertà e diritti fondamentali come, ad esempio, la libertà di espressione, di religione, di associazione e di circolazione.

[8] In tal senso, vedasi anche Corte di Giustizia, sent. del 24 settembre 2019, *Google (Portata territoriale della deindicizzazione)*, C-507/17, EU:C:2019:772, punto 60.

personali abbiano la possibilità di circolare liberamente e con elevate garanzie di tutela per le persone fisiche, considerato che la direttiva 95/46 non era riuscita a impedire la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione[9]. Tale ultima esigenza è probabilmente la principale ragione della decisione di adottare un nuovo strumento normativo in sostituzione della direttiva 95/46.[10] Il regolamento, a differenza della direttiva, si caratterizza, infatti, per avere disposizioni integralmente obbligatorie e direttamente vincolanti sia per le pubbliche autorità sia per gli individui localizzati nel territorio di tutti gli Stati membri, risultando quindi più stringente e maggiormente idoneo a garantire certezza, trasparenza e uniformità.

5. Per le persone fisiche la possibilità di disporre di un quadro giuridico omogeneo e semplificato rappresenta un rafforzamento della propria posizione. In particolare, l'obiettivo di assicurare un alto livello di protezione dei dati personali viene perseguito grazie al consolidamento e all'introduzione di diritti sostanziali, alla previsione di obblighi stringenti a carico del titolare o responsabile del trattamento, nonché alla predisposizione di un sistema di mezzi di ricorso che consente al titolare del diritto alla protezione (cosiddetto interessato) di agire nel caso in cui ritenga che tale diritto sia stato violato.

6. L'esigenza di uniformità e di semplificazione, tuttavia, non sempre risulta soddisfatta, specialmente nelle ipotesi di "trattamento transfrontaliero", cioè in riferimento a quei trattamenti che hanno luogo nell'ambito delle attività di diversi stabilimenti, situati in più di uno Stato membro, di un titolare (o responsabile) stabilito in più di uno Stato membro, oppure quei trattamenti che hanno luogo nell'ambito delle attività di un unico stabilimento del titolare (o responsabile) di questi, incidendo tuttavia in modo sostanziale su interessati che si trovano in più di uno Stato membro[11].

7. Questioni alquanto rilevanti attengono ai conflitti di leggi, poiché il GDPR non introduce disposizioni sulla legge applicabile e ciò nonostante che la sua disciplina lasci molto spazio agli Stati membri, consentendo loro, riguardo a particolari settori del trattamento dei dati, di ampliare limitare o specificare le norme contenute nel regolamento[12].

---

[9] La direttiva 95/46/CE risale infatti ad un epoca in cui l'utilizzo di internet era assolutamente marginale. Lo strumento inoltre, per sua natura, rimetteva ai singoli Stati l'emanazione della disciplina attuativa interna, lasciando loro ampi margini di adattamento e di deroga, soprattutto in settori particolari. Di conseguenza, per quanto la direttiva avesse come obiettivo sostanziale quello di creare una disciplina organica e armonica, si era creato un quadro normativo complesso e disomogeneo tra gli Stati membri, poiché questi avevano introdotto disposizioni talvolta profondamente diverse tra loro. Le divergenze tra gli Stati membri riguardavano i diritti sostanziali, i rimedi nel caso di violazione delle leggi di trasposizione della direttiva e i relativi poteri conferiti alle autorità di protezione dei dati e agli organi amministrativi e giurisdizionali. Tale situazione aveva determinato una frammentazione dei diritti e degli obblighi in materia e, conseguentemente, una condizione di incertezza giuridica non solo per le persone fisiche, ma anche per gli operatori economici e le autorità pubbliche. In proposito, anche per ulteriori riferimenti bibliografici, si veda A. Galetta, P. De Hert, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, in *Review of European Administrative Law*, Vol. 8, 1/2015, pp. 125-151, spec. p. 136.

[10] Il requisito della coerenza nel livello di protezione dei diritti conferiti dal GDPR è richiamato nei considerando 7, 9, 10, 13, 123, 129, 133 e 135. Su tale aspetto vedasi anche Corte di Giustizia, sent. 15 giugno 2021, *Facebook Ireland e a.*, C-645/19, EU:C:2021:483, punto 64; sent. 22 giugno 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, punto 83, e sent. 28 aprile 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, punto 52, nonché le conclusioni dell'avvocato generale Bobek nella causa *Facebook Ireland e a.* cit. (EU:C:2021:5), parr. 95-97.

[11] La definizione è contenuta nell'art. 4, par. 23, del GDPR. Al fine di valutare se risulti o meno realizzata la condizione di "incidere in maniera sostanziale", il Gruppo di Lavoro Articolo 29, che sotto il vigore della Direttiva 95/46 riuniva i rappresentanti di tutte le autorità di controllo dei vari Stati europei, nel documento del 13 dicembre 2016, aggiornato il 5 aprile 2017, dal titolo "Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento" (16/EN WP 244 rev.01) evidenzia come occorra una valutazione da compiersi caso per caso che tenga conto delle specifiche circostanze, del contesto in cui si svolge il trattamento e delle categorie di dati trattati e delle finalità di trattamento. Ad esempio, soddisfano detta condizione i trattamenti che producono concretamente, o è probabile che producano concretamente, una limitazione dei diritti o un'esclusione da benefici e opportunità, i trattamenti che espongano la persona a forme di disparità di trattamento, nonché i trattamenti che interessano un'ampia gamma di dati personali.

[12] Su questo profilo ci si limita a rinviare, anche per ulteriori riferimenti bibliografici, a J. Chen, *How the Best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*, in *International Data Privacy Law*, 2016, vol. 6, n. 4, pp. 313 ss. e M. Mantovani, *Horizontal Conflicts of Member States'GDPR-Complementing Laws: The Quest for a Viable Conflict-of-Laws Solution*, in *Rivista di Diritto Internazionale Privato e Processuale*, 2019, pp. 535-562.

8. Come si proverà a dimostrare nel prosieguo del presente lavoro, problemi giuridici emergono anche con riferimento ai profili di diritto processuale internazionale, che sebbene oggetto di una specifica disciplina, rimangono per taluni aspetti privi di coerenza, soprattutto in relazione al quadro di tutela riferibile al *public enforcement*, rendendo il sistema di tutela predisposto per gli interessati, nel suo insieme, piuttosto complesso e imprevedibile.

II. I rimedi riconosciuti all'interessato nel caso di violazione del diritto alla protezione dei dati personali.

9. L'applicazione efficace delle norme sulla protezione dei dati personali è affidata non solo a organi e organismi dell'Unione, ma anche alle autorità competenti degli Stati membri, in particolare alle autorità di controllo e ai giudici nazionali. Tali autorità sono al centro del sistema di mezzi di ricorso previsto dal regolamento che ha dunque una duplice natura: pubblicistica e privatistica.

10. Sotto il profilo del *public (administrative) enforcement*, come stabilito dall'art. 57, par. 1, lett. a), e chiarito dal considerando 129, il GDPR attribuisce alle autorità di controllo dei rispettivi Stati membri un compito di controllo, vigilanza e garanzia, rispetto all'effettiva e coerente applicazione delle proprie disposizioni, e prevede, a tal fine, che queste siano dotate di pervasivi poteri d'indagine, correttivi, sanzionatori, autorizzativi e consultivi. La disposizione citata dà attuazione all'art. 8, par. 3, della CDFUE che dispone che il rispetto delle regole in materia di protezione dei dati di carattere personale è soggetto al controllo di un'autorità indipendente.

11. Sotto il profilo del *private enforcement*, il regolamento ha predisposto strumenti e rimedi funzionali ad accordare all'individuo un maggiore controllo dei propri dati personali. I rimedi di diritto privato possono considerarsi il segnale di un'inversione di tendenza che va nella direzione dell'abbandono di un atteggiamento paternalistico nei confronti della protezione dei dati a favore di un approccio che valorizza l'autonomia dei singoli e le loro rivendicazioni. Il *private enforcement* rimane comunque essenzialmente uno strumento per rafforzare l'applicazione complessiva del GDPR: l'attribuzione del compito di tutelare il diritto alla protezione dei dati personali alle sole autorità amministrative indipendenti avrebbe, infatti, costituito un limite importante giacché queste, a causa dell'insufficienza dei fondi disponibili, non sempre sono in grado di dare corso a tutte le segnalazioni e a tutti i ricorsi ovvero sono costrette ad accordare priorità ai casi ritenuti più rilevanti[13]. Le decisioni emesse a seguito di azioni private hanno pure il vantaggio di avere maggiori possibilità di essere riconosciute ed eseguite in altri Stati membri, rispetto alle decisioni adottate dalle autorità di protezione dei dati. Le sentenze dei tribunali nazionali possono il più delle volte ricondursi nell'ambito di applicazione del regolamento (UE) n. 1215/2012 relativo alla competenza giurisdizionale, al riconoscimento e all'esecuzione delle decisioni in materia civile e commerciale (Regolamento Bruxelles 1-*bis*) e della Convenzione di Lugano del 2007, avente analogo oggetto, che disciplina i rapporti degli Stati membri dell'Unione europea con Norvegia, Islanda e Svizzera[14].

[13] La centralità degli strumenti di *private enforcement* è confermata dai dati che si riferiscono alle sanzioni comminate dall'autorità di controllo italiana nel 2022. Come evidenziato nell'articolo di F. Corti, *Reclami e segnalazioni privacy: quali conseguenze per l'organizzazione che viene segnalata?*, in www.laborproject.it, i dati indicano che solo il 20% circa dei provvedimenti a carattere sanzionatorio riguarda istruttorie partite da violazioni di dati personali o dalla diretta iniziativa dell'Autorità. La stragrande maggioranza delle ordinanze di ingiunzione pubblicate, invece, originano da reclami degli interessati, presentati ai sensi dell'art. 77 del GDPR. Con riferimento ai temi, numerosi reclami e segnalazioni hanno ad oggetto la pubblicazione di dati personali sui *social network* (commenti, fotografie, etc.), le comunicazioni di natura commerciale inoltrate via e-mail o sms (cosiddétto *telemarketing* selvaggio), i trattamenti di dati personali effettuati in ambito lavorativo, la pubblicazione sui siti web di pubbliche amministrazioni di atti e documenti che contengono dati personali di dipendenti, la diffusione sui siti web di istituti scolastici di dati personali riguardanti alunni e personale dipendente e, infine, la reperibilità in rete di informazioni relative a vicende giudiziarie.

[14] I due strumenti prevedono che ogni decisione, rientrante nell'ambito di applicazione dello strumento, venga eseguita in modo automatico in un diverso Stato membro, senza che sia necessario il ricorso ad alcun procedimento. La Corte di Giustizia

12. Nell'ipotesi di violazione della disciplina contenuta nel regolamento o negli strumenti nazionali di adeguamento, il sistema di ricorsi previsti dal GDPR riconosce dunque all'interessato la possibilità di seguire sia la via amministrativa sia la via giurisdizionale per ottenere tutela.

13. In particolare, l'interessato può presentare un reclamo dinanzi all'autorità di controllo, alternativamente nello Stato membro in cui risiede abitualmente, in quello in cui svolge la propria attività lavorativa o, infine, in quello nel quale si è verificata la presunta violazione (art. 77). Nel caso in cui l'autorità di controllo 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, questo ha il diritto di proporre un ricorso giurisdizionale effettivo per contestare il merito della decisione o l'inerzia dell'autorità di controllo (art. 78, parr. 1 e 2).[15]

14. La previsione di un diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo sembra suggerire che quest'ultima ha l'obbligo, non solo di svolgere un accertamento esaustivo dei fatti presentati dal reclamante, ma anche, nel caso di constatata violazione del regolamento, di agire nell'ambito dei suoi poteri di intervento, in particolare, irrogando una sanzione pecuniaria o emanando una ingiunzione. Secondo tale interpretazione l'autorità di controllo, in queste ipotesi, non godrebbe quindi di un margine di apprezzamento rispetto a un possibile intervento, potendo solamente scegliere quale tra i provvedimenti di cui all'art. 58, par. 2, del GDPR adottare. Secondo una diversa tesi, l'art. 57, par. 1, lett. f), del GDPR, letto alla luce dei considerando 129 e 141, secondo i quali ogni provvedimento adottato dall'autorità di controllo per garantire il rispetto del regolamento dovrebbe essere adeguato, necessario e proporzionato, imporrebbe all'autorità di controllo uno scrupoloso esame nel merito del reclamo, ma non prescriverebbe sempre e senza eccezioni l'intervento nel caso in cui venga accertata una violazione, dovendosi tener conto delle particolari circostanze sussistenti nel caso concreto. L'intervento dell'autorità sarebbe quindi dovuto solo nell'ipotesi in cui questo risulti necessario per la tutela dei diritti della persona interessata, mentre potrebbe essere escluso nel caso in cui una violazione, che si è verificata in passato, è improbabile che si ripeta perché, ad esempio, l'impresa titolare del trattamento ha successivamente adottato gli opportuni provvedimenti[16].

---

ha definito la portata della nozione di "materia civile e commerciale" facendo riferimento agli elementi che caratterizzano la natura dei rapporti giuridici tra le parti della controversia e all'oggetto della stessa. In linea di massima detta nozione comprende al suo interno le controversie tra privati ed esclude le controversie nelle quali una delle parti è un'autorità pubblica, a meno che questa agisca in qualità di privato, cioè al di fuori dell'esercizio di pubblici poteri (*acta iure imperii*). L'esatta portata della nozione di "esercizio della potestà d'imperio" è difficilmente definibile giacché la Corte al riguardo ha esaminato il fondamento e le modalità d'esercizio dell'azione intentata seguendo un approccio *case by case*. Sulla questione vedasi Corte di giustizia, sent. 16 dicembre 1980, causa C-814/79, *Paesi Bassi c. Rüffer*, ECLI:EU:C:1980:291, § 8; sent. 21 aprile 1993, causa C-172/91, *Sonntag c. Waidmann*, ECLI:EU:C:1993:144, § 20; sent. 14 novembre 2002, causa C-271/00, *Baten*, ECLI:EU:C:2002:656, § 30; sent. 15 maggio 2003, causa C-266/01, *Préservatrice foncière TIARD*, ECLI:EU:C:2003:282, § 22; sent. 15 febbraio 2007, causa C-292/05, *Lechouritou* e a., ECLI:EU:C:2007:102, § 31; in dottrina, con specifico riferimento al tema della tutela dei dati personali, si vedano M. Brkan, *Data Protection and European Private International Law*, in *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS*, 2015/40, p. 8 ss.; in dottrina si vedano P. A. de Miguel Asensio, *Aspectos internacionales del Reglamento general de protección de datos de la UE (I): cuestiones de competencia*, in www.pedrodemiguelasensio.blogspot.it, 11 maggio 2016, p. 3 ss.; P. Franzina, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. De Franceschi (ed.), *European Contract Law and the Digital Single Market*, Cambridge-Antwerp-Portland, 2016, p. 96 ss.; C. Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union*, in *Rivista di diritto internazionale privato e processuale*, 2016, pp. 653-675, spec. p. 668 ss.

[15] 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.

[16] Tale questione è oggetto delle domande di pronuncia pregiudiziale promosse dal Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania) depositate il 14 dicembre 2021, causa C-768/21, *TR c. Land Hessen* e 11 gennaio 2022, cause riunite C-26/22 e C-64/22, *UF – AB c. Land Hessen*, a tutt'oggi pendenti dinnanzi alla Corte di Giustizia. Nelle conclusioni dell'avvocato generale Priit Pikamäe, presentate il 16 marzo 2023 nelle cause riunite *UF – AB c. Land Hessen*, §§ 39-40, si sostiene il carattere imperativo dell'obbligo dell'autorità di controllo di trattare i reclami. Secondo l'avvocato generale, dal momento che ogni violazione del GDPR potrebbe, in linea di principio, costituire una violazione dei diritti fondamentali, riconoscere all'autorità di controllo il potere discrezionale di trattare o meno i reclami risulterebbe incompatibile con il sistema previsto da detto regolamento e con gli obiettivi perseguiti dal legislatore europeo. Sull'argomento si vedano anche

15. In ogni caso, il potere riconosciuto alle autorità di controllo di adottare misure correttive esclude radicalmente che la procedura di reclamo possa essere assimilata a quella di una petizione. Il reclamo dinnanzi all'autorità di controllo è invece concepito come un meccanismo idoneo a salvaguardare in maniera efficace i diritti e gli interessi delle persone fisiche titolari dei dati personali. Alle decisioni dell'autorità di controllo viene riconosciuto un effetto giuridicamente vincolante e pertanto l'eventuale controllo giurisdizionale sulla decisione non può risolversi in un mero sindacato di legittimità del provvedimento, ma deve comportare un riesame integrale dello stesso. Il giudice nazionale, ai sensi dell'art. 78 del GDPR, può rivalutare la decisione, estendendo il proprio controllo a tutti gli aspetti pertinenti rientranti nel potere di valutazione esercitato dall'autorità di controllo che afferiscono non solo all'esame dell'oggetto del reclamo, ma anche al margine di discrezionalità riguardante la scelta degli atti di indagine e le misure correttive.[17]

16. Il GDPR prevede, inoltre, due tipi di rimedi giurisdizionali individuali che possono essere esercitati parallelamente o alternativamente rispetto al ricorso dinanzi all'autorità di controllo: il diritto a un ricorso effettivo sotto forma di richiesta di un'azione specifica da intraprendere (art. 79); il diritto al risarcimento, da parte del titolare o del responsabile del trattamento, dei danni subiti a seguito della violazione del regolamento (art. 82).

In particolare, ai sensi dell'art. 79, la persona interessata può promuovere un'azione nei confronti del titolare (o del responsabile) del trattamento dinanzi alle autorità giurisdizionali dello Stato membro in cui questo ha uno stabilimento oppure a quelle dello Stato membro in cui l'interessato risiede abitualmente, a meno che il titolare (o il responsabile) del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri[18]. Il par. 1 dell'art. 79 GDPR si riferisce genericamente alla violazione dei diritti previsti dal regolamento; pertanto devono ritenersi ricompresi tutti i diritti che lo strumento attribuisce alla persona fisica cui si riferiscono i dati personali oggetto di trattamento, fra i quali il diritto all'informazione (artt. 12, 13, 14, 19), il diritto di accesso (art 15), il diritto di rettifica (art 16), il diritto alla cancellazione (cosiddetto diritto all'oblio, di cui all'art. 17), il diritto alla limitazione del trattamento (art 18), il diritto alla portabilità dei dati (art. 20), il diritto di opporsi al trattamento dei dati relativi all'interessato, compresa la profilazione (art. 21), il diritto di non essere sottoposto a una decisione basata esclusivamente sul trattamento automatizzato (compresa la profilazione) (articolo 22), il diritto di essere informato in caso di violazione dei dati (art. 34). Il ricorso giurisdizionale di cui all'art. 79 deve potersi qualificare come effettivo, ai sensi dell'art. 47 della CDFUE, ovvero deve essere previsto a prescindere da ogni altro eventuale ricorso amministrativo o stragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo sulla base dell'art. 77. Il ricorso contro le decisioni giuridicamente vincolanti di un'autorità di controllo di cui all'art. 78 del GDPR non costituisce infatti, in sé, un ricorso giurisdizionale effettivo, dal momento che alcune rivendicazioni che possono derivare dalla violazione del regolamento non rientrano nelle competenze dell'autorità di controllo.

17. Con riguardo alla tipologia di azioni che possono essere esperite dinanzi all'autorità giurisdizionale, si ritiene che lo strumento attribuisca agli Stati membri la facoltà di articolare autonomamente i rimedi giurisdizionali, con l'eccezione dell'azione risarcitoria che viene sostanzialmente disciplinata dal regolamento e che non può essere esclusa dal diritto nazionale. Di conseguenza sono ammissibili le azioni dirette a ottenere un provvedimento di natura inibitoria, il quale invero assume particolare rilievo,

---

le conclusioni dell'avvocato generale Saugmandsgaard Ø del 19 dicembre 2019 rese nella causa *Facebook Ireland e Schrems* (C-311/18, EU:C:2019:1145), §§ 146-148.

[17] In tal senso, si vedano le conclusioni dell'avvocato generale Priit Pikamäe, cause riunite *UF – AB c. Land Hessen* cit., §§ 49-51.

[18] Tale ultimo limite risulta ispirato ai criteri propri del Regolamento Bruxelles I-*bis* che, all'art. 1, par. 1, delimita il suo campo di applicazione *ratione materiae*, specificando, per un verso, che questo riguarda la materia civile e commerciale, indipendentemente dalla natura dell'autorità giurisdizionale adita e, per altro verso, che rimane esclusa l'intera materia fiscale, doganale e amministrativa, nonché la responsabilità dello Stato per atti od omissioni nell'esercizio di pubblici poteri (*acta iure imperii*). Sulla questione vedasi altresì quanto rilevato nella nota 14.

dal momento che molti dei diritti attribuiti all'interessato comportano l'adempimento, ad opera della controparte, di specifici obblighi di *facere* o di *non facere*.[19]

Infine, ai sensi dell'art. 82, tutte le persone fisiche che hanno subito un danno derivante da una violazione del GDPR hanno il diritto di ottenere la riparazione del pregiudizio subito dal titolare (o responsabile) del trattamento dinanzi all'autorità giurisdizionale. L'impiego della formula "chiunque subisca un danno materiale o immateriale" sembra voler indicare che l'azione di risarcimento danni non è riservata ai soli interessati diretti[20].

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, a certe condizioni, ha il diritto di conferire mandato a un organismo, a un'organizzazione o a un'associazione senza scopo di lucro, attivi nel settore della protezione dei dati personali, affinché tali soggetti agiscano a suo nome. L'art. 80, par. 2, 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 dinanzi all'autorità di controllo, ai sensi dell'articolo 77, o anche di esercitare i diritti di cui agli articoli 78 e 79.[21]

La disposizione s'inserisce nella tendenza a favorire lo sviluppo di azioni rappresentative promosse da enti con l'obiettivo di tutelare interessi generali o collettivi e di rafforzare l'accesso alla giustizia delle persone lese[22]. Il fatto che il GDPR legittimi associazioni a tutela degli interessi individuali a instaurare, mediante un meccanismo di ricorso rappresentativo, azioni intese a far cessare trattamenti di dati contrari alle disposizioni del regolamento e a risarcire le vittime di violazioni, contribuisce incontestabilmente a rafforzare i diritti degli interessati e ad assicurare loro un elevato livello di protezione. La percezione che il titolare (o il responsabile) del trattamento sia troppo potente e la violazione troppo reiterata per essere considerata sanzionabile dissuade molte volte gli interessati dal rivolgersi alle autorità amministrative e, a maggior ragione, alle autorità giurisdizionali. Il coinvolgimento di organismi può rivelarsi utile anche per superare gli ostacoli di natura procedurale che limitano le azioni di risarcimento dei danni: l'elevata durata del procedimento civile; le consistenti spese a carico, dovute alla necessità di

[19] In senso critico su tale opzione legislativa A. Galetta, P. De Hert, *The Proceduralisation of Data Protection Remedies*. Sul punto si veda anche C. Kohler, *Conflict of law issues in the 2016 Data Protection Regulation of the European Union*, cit., p. 667.

[20] La disposizione, com'è noto, segna un passo in avanti nella tutela dell'interessato poiché l'art. 23 della direttiva 95/46/CE, che obbligava gli Stati membri a prevedere una richiesta di risarcimento danni nei confronti del titolare del trattamento, lasciava aperte alcune questioni cruciali, fra le quali la possibilità di richiedere e ottenere il risarcimento per danni di natura non patrimoniale e la possibilità di configurare la responsabilità in capo ai responsabili del trattamento. Per questa ragione la disposizione era stata recepita nel diritto nazionale degli Stati membri in modo molto incoerente, assumendo quindi una rilevanza pratica marginale.

[21] Si tratta di una disposizione che accorda agli Stati membri un certo margine di manovra, poiché questi possono prevedere differenti condizioni con riguardo alla legittimazione ad agire degli enti, delle organizzazioni o delle associazioni senza scopo di lucro. Nell'ambito dell'ordinamento italiano, l'art. 10, comma 5, del Codice in materia di protezione dei dati personali prevede che l'interessato possa dare mandato a un ente del terzo settore, soggetto alla disciplina del decreto legislativo n. 117/2017 e che sia specializzato nella tutela dei diritti alla protezione dei dati personali.

[22] Questa tendenza si è tradotta recentemente nell'adozione della direttiva (UE) 2020/1828, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (cosiddétta *Class action* europea), il cui termine di recepimento era fissato nel 25 dicembre 2022 e che ha trovato applicazione dallo scorso 25 giugno. Lo strumento, allo scopo di "contribuire al funzionamento del mercato interno e al conseguimento di un livello elevato di protezione dei consumatori", impone agli Stati membri di introdurre all'interno del proprio ordinamento l'istituto dell'azione rappresentativa a tutela degli interessi collettivi dei consumatori nel caso di violazioni di norme dell'Unione europea che disciplinano vari settori, fra i quali è annoverata anche la protezione dei dati. Tale azione è esperibile dagli enti legittimati, vale a dire associazioni di consumatori e di iscritte in un apposito elenco pubblico, nonché enti pubblici la cui legittimazione sia espressamente conferita dagli Stati membri e può essere promossa senza bisogno di mandato da parte dei consumatori. Se la violazione lede consumatori di diversi Stati membri, l'azione può essere proposta congiuntamente da più enti di diversi Stati. Sul tema v. anche Corte di Giustizia, sent. del 29 luglio 2019, *Fashion ID GmbH & Co.KG* contro Verbraucherzentrale NRW e V, causa C-40/17, EU:C:2019:629, §§ 43-63 e le conclusioni dell'avvocato generale del 2 dicembre 2020, *Meta Platforms Ireland*, causa C-319/20, EU:C:2021:979; in dottrina, A. Pato, *Collective Redress Mechanisms in the EU, in Jurisdictionand Cross-Border Collective Redress: A European Private International Law Perspective*, Bloomsbury Publishing, Londra, 2019, pp. 45-117; B. Gsell, *The New European Directive on Representative Actions for the Collective Interests of Consumers – A Huge, but Blurry Step Forward*, in *Common Market Law Review*, vol. 58, n. 5, 2021, pp. 1365-1400.

assumere un avvocato che abbia familiarità con una materia complessa; le difficoltà legate alla raccolta delle prove e all'onere della prova, in particolare per quanto riguarda le attività di trattamento realizzate su internet[23].

III. La delimitazione della giurisdizione nel caso di violazione del GDPR: l'introduzione dei fori speciali.

18. A differenza della direttiva 95/46/CE, il GDPR contiene, all'art. 79, par. 2, una specifica norma attributiva della competenza giurisdizionale per le azioni esperite nei confronti di un titolare (o responsabile) del trattamento, nel caso di violazione dei diritti dell'interessato. Tale disposizione appare assai rilevante poiché le controversie in materia si riferiscono di frequente a rapporti o situazioni di carattere transnazionale, dal momento che il trattamento dei dati personali è il più delle volte legato alla rete internet che si caratterizza per la sua apertura e globalità.

In particolare, l'art. 79, par. 2, attribuisce all'interessato la possibilità di convenire in giudizio il titolare (o il responsabile) del trattamento dinanzi al tribunale dello Stato in cui quest'ultimo ha uno stabilimento o, in alternativa, dinanzi ai giudici dello Stato membro della propria residenza abituale. Tali titoli di giurisdizione si riferiscono unicamente alle azioni che possono essere intentate dall'interessato nei confronti del titolare (o del responsabile) del trattamento e non viceversa. La mancanza di simmetria è da ricondursi all'obiettivo di proteggere il titolare del diritto alla protezione dei dati personali che ispira la disposizione in esame e, come anticipato, lo strumento nel suo complesso. Peraltro, le azioni promosse dal titolare (o dal responsabile) del trattamento nei confronti dell'interessato si fonderebbero, in linea di massima, su un rapporto contrattuale e non sulla violazione della disciplina a tutela dei dati personali. La competenza giurisdizionale speciale prevista dal regolamento è limitata *ratione materiae* alle rivendicazioni in materia di protezione dei dati che riguardano i diritti accordati dal GDPR[24].

19. L'art. 79, par. 2, non specifica se i titoli speciali di giurisdizione si riferiscono alle sole azioni promosse a seguito della violazione dei diritti riconosciuti dal GDPR o se valgono anche nel caso di trattamento contrario alle disposizioni nazionali di adeguamento. Tale omissione può dare adito a qualche dubbio interpretativo, considerato che il regolamento contempla alcune "clausola di salvaguardia" che consentono ai legislatori nazionali di estendere l'ambito di applicazione materiale dello strumento, accordando tutela, ad esempio, ai trattamenti dei dati personali concernenti persone decedute[25]. La seconda interpretazione sembra da prediligere per diverse ragioni. Innanzitutto, è possibile sostenere che i diritti derivanti dalle leggi nazionali di attuazione derivano, anche se indirettamente, dal GDPR poiché

[23] In proposito si veda M. Requejo Isidro, *La aplicación privada del derecho para la proteción de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679*, in *La Ley Mercantil*, 2017, pp. 1-25.

[24] In ordine al profilo territoriale, il GDPR, al fine di determinare la propria applicabilità, richiede invece che sia soddisfatto almeno uno dei criteri di cui all'art. 3. Il primo criterio stabilisce che il regolamento trova applicazione «al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione» (cd. *establishment criterion*). Il secondo criterio prevede che il GDPR si applica a un titolare del trattamento o responsabile del trattamento che non ha uno stabilimento nell'Unione, laddove le attività di trattamento siano correlate all'offerta di beni o servizi agli interessati nell'Unione o al monitoraggio del loro comportamento, nella misura in cui il loro comportamento si svolge all'interno dell'Unione (cd. *targeting criterion*). Sui problemi sollevati dalla disposizione, in ragione della sua natura "esorbitante", si rinvia fra i tanti a C. Kuner, *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*, in *University of Cambridge Faculty of Law Research Paper*, 2021, 20, pp. 1-35, spec. 5-14; P. De Hert, M. Czerniawski, *Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context*, in *International Data Privacy Law*, 2016, vol. 6/3, p. 230 ss.; M.S.C. Taylor, *Permissions and Prohibitions in Data Protection Jurisdiction*, in *Brussels Privacy HUB Woking Paper n. 6*, 2016, pp. 1-25; nonché l'opera monografica di D.J.B. Svantesson, *Extraterritoriality in Data Privacy Law*, *Ex Tuto Publishing*, 2013, pp. 1-240.

[25] Il considerando 27, affermando che «gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute», consente a chi ha un interesse proprio oppure agisce a tutela del defunto, quale mandatario o per ragioni familiari meritevoli di protezione, di esercitare i diritti previsti dal regolamento anche nell'ambito di trattamenti dei dati personali di persone decedute.

è tale strumento che accorda agli Stati membri la facoltà di adottare, in circostanze specifiche, norme nazionali sulla protezione dei dati. Inoltre, con riguardo al diritto al risarcimento dei danni, il regolamento chiarisce che sono ricompresi i danni subiti a causa di un trattamento che viola le leggi nazionali di adeguamento. Infine, il considerando 146 del GDPR afferma che «un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento».[26]

20. Di fronte all'alternativa delineata dall'art. 79, par. 2, appare probabile che l'interessato, intenzionato a promuovere un'azione giurisdizionale contro il titolare o il responsabile del trattamento, opti per il giudice della propria residenza abituale, piuttosto che per il giudice dello Stato in cui si trova uno stabilimento del titolare (o del responsabile) del trattamento.[27] A proposito della ricostruzione del concetto di residenza abituale la Corte di giustizia è più volte intervenuta, affermando che detta nozione si ricostruisce in funzione della struttura e della finalità dell'atto che la contiene. Per stabilire il luogo di residenza abituale occorre quindi compiere un'analisi obiettiva e complessa delle circostanze di fatto preponderanti, in un intervallo di tempo determinato, nonché tenere conto dell'elemento soggettivo rappresentato dalla intenzione di stabilirsi in un determinato luogo e del fatto che il periodo di permanenza in un dato luogo deve essere significativo, ovvero non necessariamente continuativo, ma neanche occasionale. Con riferimento alla disciplina contenuta nel GDPR, pare doversi ritenere che nella maggioranza dei casi la residenza abituale della persona interessata coincida con il "centro degli interessi della vittima", quale titolo di giurisdizione elaborato dalla Corte di giustizia con riguardo alle violazioni dei diritti della personalità negli illeciti a distanza per il tramite dell'uso di internet. I due concetti non sono tuttavia sovrapponibili giacché una persona può avere il proprio centro d'interessi in uno Stato membro in cui non risiede abitualmente, nell'ipotesi in cui un vincolo particolarmente stretto con detto Stato risulti da altri elementi come, ad esempio, l'esercizio di un'attività professionale[28].

21. Il nuovo titolo di giurisdizione, fondato sulla residenza abituale dell'interessato, rafforza in modo rilevante i diritti procedurali del titolare del diritto alla protezione dei dati personali poiché pone rimedio alla situazione preesistente in cui l'interessato che lamentava di avere subito una violazione dei propri diritti poteva essere disincentivato ad agire in giudizio a causa del modesto valore economico dell'eventuale risarcimento danni reclamato, a fronte degli alti costi da sostenere per avviare il contenzioso in un paese diverso da quello di residenza abituale. L'attribuzione della competenza giurisdizionale al giudice più vicino all'interessato scongiura o quantomeno attenua il rischio di dover sopportare eccessive spese processuali, rendendo il rimedio risarcitorio accessibile e facilitato.

22. Se quanto appena osservato può ascriversi ai meriti del GDPR, occorre tuttavia aggiungere che il nuovo regime sulla competenza giurisdizionale appare difettare di chiarezza. In primo luogo, il GDPR non chiarisce il suo rapporto con le norme sulla competenza contenute nel regolamento Bruxel-

[26] Si veda tuttavia in senso contrario I. Revolidis, *Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?*, in *Masaryk University Journal of Law and Technology*, vol. 11, 1/2017, p. 25 ss.

[27] Al fine dell'individuazione del giudice competente, il luogo in cui si trova la residenza abituale dell'interessato va valutato, in mancanza di chiare indicazioni nel regolamento sul punto, facendo riferimento al momento della proposizione dell'azione e non al momento in cui è stato effettuato il trattamento dei dati personali che si assume illecito. Sulla questione di diversa opinione F. Ragno, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del gdpr*, in *Ordine internazionale e diritti umani*, 2020, pp. 818-838. L'autrice ritiene che il *forum actoris*, in conformità alla lettura che viene data al foro del consumatore, così come delineato dall'art. 18 del Regolamento Bruxelles I-*bis*, può legittimare l'attore a evocare il convenuto non solo dinanzi ai giudici dello Stato in cui risiede abitualmente al momento dell'instaurazione della lite, ma anche dinanzi ai giudici dello Stato in cui risiedeva abitualmente nel momento in cui è sorto il rapporto nell'ambito del quale il trattamento dei dati personali sia stato posto in essere.

[28] In proposito vedasi Corte di giustizia, sent. 2 aprile 2009, causa C-523/07, *A*, ECLI:EU:C:2009:225; sent. 22 dicembre 2010, causa C-497/10, *PPU - Mercredi*, ECLI:EU:C:2010:829 e sent. 25 ottobre 2011, cause riunite C-509/09 e C-161/10, *eDate Advertising e a.*, ECLI:EU:C:2011:685. In dottrina si rinvia, anche per gli opportuni riferimenti bibliografici, a A. Zanobetti, *La residenza abituale nel diritto internazionale privato: spunti di riflessione*, in AA.VV., *Liber amicorum Angelo Davì. La vita giuridica internazionale nell'età della globalizzazione*, vol. II, Napoli, 2019, p. 1361 ss.

les I-*bis*, nella convenzione di Lugano del 2007 (nei rapporti con gli Stati dell'Associazione europea di libero scambio: cosiddetti Stati EFTA) e con le norme nazionali in materia di competenza degli Stati membri[29]. Secondo la dottrina prevalente, i titoli di giurisdizione speciali previsti dal GDPR, in virtù di un criterio di specialità *ratione materiae*, sono destinati a prevalere sulle regole generali contenute nel regolamento Bruxelles I-*bis*, le quali potranno trovare applicazione solo se non risultino incompatibili con la disciplina speciale. Secondo tale dottrina detta interpretazione, per un verso, risulterebbe conforme all'obiettivo del GDPR di assicurare una maggiore certezza del diritto per gli operatori economici e gli interessati e, per altro verso, non pregiudicherebbe l'obiettivo di rafforzare i diritti dell'interessato, in quanto i titoli speciali di giurisdizione gli consentono comunque di agire dinanzi al giudice dello Stato membro della sua residenza abituale, foro che solitamente è quello considerato maggiormente in grado di garantire certezza ed effettività di tutela giurisdizionale[30].

23. È pur vero che una maggiore chiarezza su tale aspetto avrebbe giovato, dal momento che il regolamento Bruxelles I-*bis* e la convenzione di Lugano del 2007 possono comunque risultare rilevanti con riferimento alle ipotesi di chiamata in garanzia, di domande riconvenzionali proposte dal titolare (o dal responsabile) del trattamento, di cumulo soggettivo (art. 8, par. 1), di accettazione della giurisdizione (art. 26), di scelta del foro (art. 25). L'applicazione di tali istituti può, infatti, favorire l'effettiva tutela giurisdizionale dei diritti dell'interessato come avviene, ad esempio, nel caso in cui egli intenda agire al tempo stesso nei confronti di più titolari (o responsabili) del trattamento, stabiliti in Stati membri diversi, innanzi ai giudici dello Stato membro in cui uno di essi è stabilito[31].

24. Inoltre, il titolo di giurisdizione dello Stato membro in cui il titolare (o il responsabile) del trattamento ha "uno stabilimento" appare difficile da ricostruire, nell'ipotesi in cui nel territorio dell'Unione europea siano presenti più stabilimenti. L'interpretazione letterale della disposizione induce a ritenere che l'interessato abbia, in tale circostanza, la possibilità di avviare un procedimento in qualsiasi Stato membro in cui il titolare (o il responsabile) del trattamento abbia uno stabilimento, anche quando le presunte operazioni illecite sono del tutto estranee allo stabilimento individuato. Se tale opzione ermeneutica, per un verso, non contrasta con gli obiettivi dello strumento, dal momento che l'ampliamento dei fori disponibili per agire contro il titolare (o il responsabile) del trattamento rafforza i diritti dell'interessato, per altro verso, comporta il rischio di *forum shopping*, soprattutto in riferimento

[29] Sul punto l'unica indicazione è contenuta nel considerando 147 del GDPR che afferma che le disposizioni generali in materia di giurisdizione, quali quelle di cui al regolamento Bruxelles I-bis, non pregiudicano l'applicazione dei fori speciali contemplati dall'art. 79, par. 2, del GDPR. Tale precisazione si coniuga con la regola di coordinamento contenuta nell'art. 67 del regolamento Bruxelles I-bis che fa salva l'applicazione delle norme sulla competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materie specifiche contenute negli atti dell'Unione.

[30] Secondo altra parte della dottrina, la coesistenza fra titoli di giurisdizione speciali e titoli di giurisdizione generali (domicilio del convenuto, luogo in cui i servizi sono stati o avrebbero dovuto essere prestati in base al contratto, luogo in cui l'evento dannoso è avvenuto o può avvenire) e dunque l'ampliamento del ventaglio di fori alternativi a disposizione dell'interessato sarebbe in definitiva un'ulteriore espressione del regime di protezione accordato sul piano processuale a detto soggetto, sebbene a discapito del principio di prossimità e di prevedibilità del foro competente, ai quali si ispira invece il regolamento Bruxelles I-*bis*. Tale dottrina evidenzia altresì che la tesi della prevalenza dei fori speciali presenta lo svantaggio di non consentire l'accesso alla giurisdizione nell'ipotesi in cui un interessato, la cui residenza abituale vada localizzata in uno Stato terzo, lamenti una violazione dei diritti che gli vengono riconosciuti dal GDPR. Tale scenario è possibile in quanto il regolamento trova applicazione anche ai trattamenti posti in essere da titolari (o responsabili) che non hanno uno stabilimento all'interno del territorio dell'Unione europea, allorché questi offrano beni o servizi ad interessati presenti in uno degli Stati membri o ne monitorino il loro comportamento. In altri termini, i titoli di giurisdizione speciali non terrebero adeguatamente in considerazione l'ampiezza della nozione di interessato che è idonea a ricomprende al proprio interno anche le persone fisiche che non hanno la propria residenza abituale all'interno dei confini dell'Unione europea. Sul rapporto fra GDPR e il sistema Bruxelles I si confrontino P. Franzina, *Jurisdiction Regarding Claims* cit., p. 103; Kohler, *Conflict of Law Issues in the 2016 Data Protection Regulation* cit. p. 653 ss., spec. 668 ss.; P.A. De Miguel Asensio, *Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea. Revista española de Derecho internacional*, 2017, 69.1, pp. 99-102.

[31] Nondimeno i titoli di giurisdizione generali risultano applicabili per le eventuali azioni di accertamento negativo che il titolare (o il responsabile) del trattamento intendesse proporre nei confronti del titolare dei dati, come pure le eventuali azioni promosse dal titolare del trattamento nei confronti del responsabile del trattamento stesso o viceversa, considerato che i titoli di giurisdizione speciali contenuti nell'art. 79, par. 2, del RGDP sono previsti solo per le azioni proposte dall'interessato.

a quei profili in cui le discipline di adeguamento al GDPR dei diversi Stati membri divergano almeno parzialmente[32]. Tale soluzione non appare del tutto soddisfacente, particolarmente nel caso in cui il titolare (o responsabile) del trattamento non sia una grande piattaforma del web, ma una persona fisica o una piccola impresa perché nel caso in cui subiscano l'azione dell'interessato possono essere "trascinati" dinanzi a un tribunale straniero per difendersi da azioni che potenzialmente possono riguardare anche violazioni non gravi. Per tale ragione pare doversi condividere la posizione di quella parte della dottrina che ha considerato la possibilità di interpretare restrittivamente tale titolo di giurisdizione, limitando la scelta del foro a quello dello Stato membro in cui si trova lo stabilimento principale, in analogia a quanto previsto dall'art. 56 del regolamento che, nelle medesime ipotesi, ai fini del reclamo amministrativo, attribuisce la competenza all'autorità di controllo dello Stato membro in cui titolare del trattamento o il responsabile ha il suo "stabilimento principale"[33].

IV. I limiti dei meccanismi di cooperazione e assistenza delle autorità di controllo e del coordinamento delle azioni civili

25. Come detto in precedenza, il GDPR mette a disposizione degli interessati un sistema completo di mezzi di ricorso che consente loro, nel caso in cui ritengano di avere subito la violazione di un diritto ivi riconosciuto o altrimenti previsto dalla competente legge nazionale di attuazione, di proporre un reclamo dinanzi all'autorità di controllo, di impugnare, se del caso, la decisione adottata da tale autorità dinanzi ad un giudice o, infine, di proporre un ricorso giurisdizionale direttamente avverso il titolare (o il responsabile) del trattamento. Nel caso trattamenti transnazionali, il regolamento prevede una disciplina dedicata al coordinamento sia dei reclami proposti dinanzi alle autorità di controllo sia dei ricorsi presentati dinanzi a organi giurisdizionali, situati in diversi Stati membri, nell'intento di ridurre il rischio di esiti incoerenti nell'applicazione delle norme.

26. Con riguardo all'attività delle autorità di controllo, il capitolo VII del GDPR stabilisce meccanismi di cooperazione e assistenza reciproca tra le autorità di controllo dei diversi Stati membri. In particolare, l'art. 60 introduce il meccanismo dello "sportello unico" (*one-stop-shot*), secondo il quale,

[32] Il *forum shopping* risulterebbe ulteriormente accentuato in ragione dell'ampiezza della nozione di stabilimento. Invero il considerando 22 del GDPR, rifacendosi alla giurisprudenza della Corte di giustizia, afferma che questo «implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile (…)», specificando anche che «non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica». La nozione di stabilimento è quindi incentrata su un criterio flessibile e diverge dall'impostazione formalistica, secondo la quale un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata o sono presenti sue filiali o succursali. L'organizzazione dell'impresa deve caratterizzarsi per un sufficiente livello di stabilità e per la disponibilità di una struttura adeguata, in termini di risorse umane e tecniche. Altri elementi, quali il luogo in cui sono stati caricati i dati, lo Stato membro al quale sono rivolti i servizi, la nazionalità degli interessati o il luogo in cui risiedono i titolari dell'impresa, non sono decisivi al fine di determinare il luogo di stabilimento dell'impresa, sebbene possano costituire, in determinate circostanze, un indizio del carattere reale ed effettivo dell'attività svolta. Nei ragionamenti sviluppati dalla Corte di Giustizia nei casi *Google Spain* (Grande Sezione, sent. 13 maggio 2014, causa C-131/12, *Google Spain e Google*, ECLI:EU:C:2014:317), *Weltimmo* (sent. 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639) e *Amazon* (sent. 28 luglio 2016, causa C-191/15, *Verein für Konsumenteninformation*, ECLI:EU-:C:2016:612) emerge che, al fine di verificare l'esistenza di uno stabilimento, occorre considerare principalmente la presenza commerciale e il modello di affari praticato dal titolare del trattamento. Sulla questione, in dottrina, vedasi, tra i molti, M. Brkan, *Data Protection and Conflict-of-laws: A Challenging Relationship*, in *European Data Protection Law Review (EDPL)*, 2016, vol. 2/3, p. 327 ss.; K. Mc Cullagh, *Cross-Border Data Protection: Applicable Law and Territorial powers of National Data Protection Supervisors*, in *SCRIPTed: A Journal of Law, Technology and Society*, 2016, vol. 13/1, p. 95 ss.

[33] L'art. 4, n. 16), prevede che per "stabilimento principale" si intende «a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento».

nel caso in cui un trattamento, svolto nell'ambito delle attività di un unico stabilimento di un titolare (o responsabile) del trattamento, incida o abbia probabilità di incidere in modo sostanziale su interessati che si trovino in più di uno Stato membro, l'autorità situata nello Stato membro dell'unico stabilimento del titolare (o responsabile) del trattamento ha il compito di gestire e supervisionare il trattamento. Diversamente, nel caso in cui il trattamento abbia luogo nell'ambito delle attività di diversi stabilimenti di un titolare (o responsabile) del trattamento, situati in più di uno Stato membro, il compito di gestire e supervisionare il trattamento è affidato a quella del paese in cui si trovi lo "stabilimento principale" del titolare (o responsabile) del trattamento[34]. Nell'ipotesi in cui tali operazioni sui dati personali coinvolgano sia un titolare, sia un responsabile, l'autorità da individuarsi sarà quella competente per il titolare, mentre quella del responsabile sarà considerata soltanto come "autorità interessata", nozione che comprende al suo interno le autorità nel cui territorio si trovi uno stabilimento "secondario" del titolare (o del responsabile) del trattamento.

Appare evidente che la corretta individuazione dello stabilimento principale è interesse del titolare (o del responsabile), in quanto elimina ogni ambiguità sull'autorità di controllo che fungerà da interlocutore per le varie incombenze previste dal regolamento. Secondo il GDPR è, infatti, onere del titolare (o del responsabile) del trattamento individuare l'autorità capofila. Il meccanismo dello "sportello unico" non consente, quantomeno sotto tale profilo, il cosiddetto "*forum shopping*" poiché, nel caso in cui una società, per trarne vantaggio, affermi che il proprio stabilimento principale si trova in un determinato Stato membro, ma tale stabilimento non svolge alcun esercizio reale ed effettivo di attività gestionali o decisionali rispetto al trattamento di dati personali, spetta proprio alle autorità di controllo competenti individuare l'autorità di controllo "capofila", sulla base di criteri oggettivi e dell'analisi degli elementi probatori disponibili. A tal fine potrà risultare utile espletare attività di accertamento, con la collaborazione delle autorità di controllo coinvolte, considerato che la valutazione finale non può fondarsi esclusivamente sulle dichiarazioni rese dall'azienda o dal soggetto sotto esame[35].

27. La cooperazione può realizzarsi anche per il tramite delle cosiddette autorità interessate, cioè le autorità nel cui territorio si trovi uno stabilimento "secondario" del titolare (o del responsabile) del trattamento, quelle nel cui territorio si trovino interessati potenzialmente influenzati in modo sostanziale dal trattamento, nonché quelle nei confronti delle quali è stato proposto un reclamo, qualora diverse dall'autorità capofila. Un'autorità di controllo interessata ha peraltro competenza nella trattazione del caso, anche senza fungere da autorità capofila, nell'ipotesi in cui quest'ultima autorità decida di non occuparsene perché, ad esempio, ritiene che il trattamento produca effetti esclusivamente locali.

28. Il GDPR prevede anche un meccanismo di coerenza che opera sotto la supervisione del Comitato Europeo per la Protezione dei dati (CEPD), organo indipendente con funzione consultiva e di appello, rispetto alle autorità di controllo nazionali. Detto meccanismo viene attivato 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 capofila; se un'autorità di controllo non richiede un parere al CEPD quando questo è previsto o non dà seguito al parere adottato dal medesimo organo.

29. Il meccanismo dello sportello unico non copre tuttavia tutte le ipotesi di trattamento. Dalla lettura combinata degli artt. 55 e 56 del GDPR, relativi rispettivamente alla competenza delle autorità di controllo e alla competenza dell'autorità di controllo capofila, emerge che, nel caso in cui un titolare del trattamento, con sede localizzata in un paese terzo, effettui trattamenti transfrontalieri soggetti al GDPR, ma non disponga nel territorio dell'Unione europea né di un'amministrazione centrale né di

[34] Sulla nozione di "stabilimento principale" vedasi la precedente nota.

[35] Si veda al riguardo Gruppo di Lavoro Articolo 29, *Linee-guida per l'individuazione dell'autorità di controllo capofila* cit., p. 8. Per una recente applicazione del principio dello "sportello unico" vedasi Corte di Giustizia, sent. (Grande Sezione) del 15 giugno 2021, *Facebook Ireland Limited e a.* contro *Gegevensbeschermingsautoriteit*, causa C-645/19, ECLI:EU:C:2021:483, oggetto del commento di L. Woods, *Facebook Ireland and the One Stop Shop Under the GDPR*, in *European Law Review*, 2021, n. 5, pp. 685-691.

uno stabilimento con potere decisionale sulle operazioni che interessano i dati personali, il meccanismo dello sportello unico è escluso. Ciò comporta che diverse autorità di controllo possono essere chiamate a vigilare sul rispetto del GDPR in relazione ad asserite violazioni derivanti da un trattamento posto in essere da un determinato titolare (o responsabile) nei confronti di una pluralità di interessati che si trovino in diversi Stati membri.

30. La portata di tale rilievo risulta tuttavia ridimensionata in ragione del fatto che anche nelle ipotesi in cui non è prevista l'operatività del meccanismo dello sportello unico le autorità di controllo sono tenute a contribuire alla coerente applicazione del GDPR, cooperando tra loro e con la Commissione, senza che siano necessari accordi di mutua assistenza o di cooperazione tra gli Stati membri coinvolti.[36] Il caso che ha coinvolto la società statunitense *Clearview AI Inc.* è esemplificativo al riguardo, riferendosi a una ipotesi in cui il meccanismo dell'autorità capofila era escluso, in ragione della mancanza di uno stabilimento nel territorio dell'Unione europea. Detta società è stata oggetto dell'attenzione dell'autorità di controllo italiana perché ha sviluppato un *software* di riconoscimento facciale, in grado di sfruttare un *database* di dieci miliardi di immagini, molte di queste riferibili a interessati che si trovavano sotto la giurisdizione di Stati membri dell'Unione europea, fra cui l'Italia. Tale archivio era stato realizzato attraverso l'acquisizione di fotografie e video liberamente disponibili sulla rete Internet (sui *social network*, sui siti di imprese o pubbliche amministrazioni, sui blog), attraverso le informazioni estratte da queste fotografie (metadati di geolocalizzazione, il titolo dell'immagine o della pagina web etc.), nonché attraverso le rappresentazioni vettoriali che derivano dall'elaborazione dell'immagine con tecniche biometriche. Grazie all'acquisizione di tali informazioni, la *Clearview AI Inc.* aveva in sostanza creato un motore di ricerca per il riconoscimento facciale (cosiddetto *facial recognition search engine*) che le consentiva di offrire un servizio, destinato principalmente alle forze dell'ordine europee, per ricercare e individuare, a partire da una immagine, autori e vittime di reati, la cui identità era inizialmente sconosciuta. L'autorità di controllo italiana, con ordinanza ingiunzione del 10 febbraio 2022, ha dichiarato illecito il trattamento posto in essere dalla *Clearview AI*, comminandole una sanzione complessiva di venti milioni di euro, per la violazione di varie norme del GDPR. Nella motivazione del provvedimento emerge palesemente come l'autorità di controllo italiana abbia sviluppato il proprio ragionamento tenendo in considerazione le evidenze emerse nell'ambito dei procedimenti avviati dalle altre autorità di controllo europee, in particolare in ordine ai profili relativi all'applicabilità del GDPR, alla sussistenza della propria competenza, nonché alla commisurazione del grado di responsabilità. Quanto appena osservato sembrerebbe indicare dunque una certa attitudine delle autorità di controllo a cooperare fra loro, indipendentemente dal funzionamento del meccanismo dello sportello unico, anche se nel caso di specie appare alquanto rilevante il ruolo giocato delle parti private, ovvero due organizzazioni impegnate nella difesa della privacy e dei diritti fondamentali delle persone, poiché queste hanno avuto la premura di sottoporre all'attenzione dell'autorità di controllo italiana le precedenti decisioni adottate dalle autorità di controllo svedese e tedesca.

31. A proposito del coordinamento tra azioni civili, l'art. 81 del GDPR, dal titolo «Sospensione delle azioni», prevede che nel caso di procedimenti paralleli, pendenti dinanzi a tribunali competenti in diversi Stati membri, le autorità interessate siano tenute a mettersi in contatto fra loro per avere conferma dell'esistenza di tale situazione. In tal caso, ogni giudice diverso da quello preventivamente adito può sospendere il procedimento, sempre che le azioni riguardino lo stesso oggetto relativamente al trattamento dello stesso titolare (o responsabile) del trattamento. Qualora il procedimento sia pendente in primo grado il giudice successivamente adito, su richiesta delle parti, può dichiararsi incompetente a condizione che il giudice preventivamente adito sia competente a conoscere della causa e che la sua

[36] Vedasi al riguardo il considerando 123 e l'art. 61 dal titolo "Assistenza reciproca" secondo il quale, peraltro, «1. Le autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini».

legge consenta la riunione dei procedimenti. La formulazione della norma è onnicomprensiva, nel senso che pare potersi applicare sia ai procedimenti giurisdizionali sorti a seguito dell'impugnazione della decisione di autorità di controllo, sia a una azione civile tra privati.

32. Per quanto le disposizioni citate possano mitigare il rischio che le autorità giurisdizionali giungano a valutazioni giuridiche diverse in ordine alla sussistenza di una violazione delle norme stabilite dal GDPR, significativi margini di incertezza permangono. In proposito la dottrina ha principalmente rilevato l'inadeguatezza del modo nel quale il GDPR ha curato il proprio rapporto con la disciplina contenuta in materia nel regolamento Bruxelles I-*bis*, evidenziando come tale quadro normativo si riveli, in ultima analisi, suscettibile di ostacolare il perseguimento dell'obiettivo di assicurare al titolare dei dati personali una tutela giurisdizionale effettiva dei diritti a lui riconosciuti[37]. In particolare, il GDPR, all'art. 81, appare accogliere un modello a metà strada fra gli istituti della litispendenza e della connessione come "conosciuti" nei principali strumenti di diritto internazionale privato dell'Unione europea, dal momento che fa riferimento alla sola identità dell'oggetto delle due domande, senza menzionare l'ulteriore presupposto oggettivo della litispendenza europea, rappresentato dall'identità di titolo. Un'ulteriore differenza emerge sotto il profilo soggettivo, in quanto la disposizione sopra citata richiede la sola identità del titolare ovvero del responsabile del trattamento, da identificarsi in linea di principio con la parte convenuta di ciascuna delle azioni concorrenti, non attribuendo quindi rilevanza all'identità del titolare dei dati personali al fine dell'applicazione del meccanismo di coordinamento tra procedimenti paralleli. Tale soluzione è prevista nonostante appaia in linea di massima più verosimile che un'esigenza di coordinamento possa sorgere tra procedimenti paralleli riguardanti violazioni delle disposizioni del regolamento in esame da parte di un determinato titolare o responsabile del trattamento nei confronti di una pluralità di titolari di dati personali, piuttosto che tra azioni proposte da un medesimo titolare dei dati nei riguardi di diversi titolari o responsabili del trattamento[38].

V. La difficile coesistenza fra rimedi amministrativi e rimedi giurisdizionali.

33. Il coordinamento fra azioni di *pubblic enforcement* e azioni di *private enforcement* risulta assai più complesso, soprattutto perché il legislatore europeo nel GDPR non ha inteso disciplinare il coordinamento dei diversi mezzi di ricorso di cui agli artt. 77, 78 e 79, abbracciando piuttosto il modello del "doppio binario" in cui il rimedio amministrativo e il rimedio giurisdizionale coesistono in posizione di reciproca autonomia, senza che l'uno sia sussidiario rispetto all'altro.[39] In altri termini, il regolamento non prevede alcuna competenza prioritaria o esclusiva né alcuna regola di prevalenza della valutazione effettuata dall'autorità amministrativa o dall'autorità giurisdizionale con riguardo all'esistenza di una violazione dei diritti riconosciuti all'interessato. In assenza di una disciplina dell'Unione in materia, ciascuno Stato membro, in forza del principio di autonomia processuale, ha stabilito le modalità delle procedure amministrative e quelle relative alla procedura giurisdizionale intese a garantire la tutela dei

[37] In tal senso F. Marongiu Buonaiuti, *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"*, in *Cuadernos de Derecho Transnacional*, 2017, p. 458 ss.

[38] Al riguardo vedasi F. Marongiu Buonaiuti, op. ult. cit., p. 457.

[39] Tale scelta normativa rischia di porsi in contrasto con diritti fondamentali riconosciuti dagli ordinamenti degli Stati membri dell'Unione europea. La Suprema Corte austriaca, nella sentenza del 23 maggio 2019 (OGH - 6 Ob91/19d), si è interrogata al riguardo, concludendo comunque che il regime del doppio binario previsto dal GDPR non determina alcuna violazione dell'art. 94, par. 1, della Costituzione austriaca ("B-VG") che in sostanza prevede l'obbligo di affidare l'oggetto dell'esecuzione o interamente al giudice o all'autorità amministrativa. Nella decisione i giudici austriaci hanno respinto, sulla base dell'art. 79 del GDPR e del primato del diritto dell'Unione europea, l'interpretazione della disciplina nazionale data dalla Corte Regionale di Vienna, secondo la quale solo il diritto al risarcimento, e non anche la richiesta di cancellazione dei dati personali da parte dell'attore, poteva essere fatto valere in tribunale. Nella decisione i giudici rilevano tuttavia che l'Austria è stato l'unico paese a votare contro l'adozione del GDPR proprio perché il parallelismo dei rimedi giuridici determina il rischio di decisioni giudiziarie contrastanti e di violazione del principio di cosa giudicata. Su tali aspetti, nella dottrina italiana, R. Giordano, *La tutela amministrativa e giurisdizionale dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1011 ss.

diritti spettanti agli interessati[40]. Gli ordinamenti nazionali hanno tuttavia previsto 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[41].

34. Risulta evidente che in tale ultimo scenario il rischio che l'autorità di controllo e il giudice o i giudici aditi possano giungere a valutazioni diverse, in ordine alla sussistenza di una violazione, è tutt'altro che remoto. Le possibili interferenze tra procedimento amministrativo e procedimento giurisdizionale sono state oggetto dell'intervento della Corte di Giustizia nel caso *Nemzeti Adatvédelmi és Információszabadság Hatósá* del 2021, originato dalla domanda di pronuncia pregiudiziale riguardo al coordinamento tra il reclamo presentato a un'autorità di controllo, ai sensi dell'art. 77, par. 1, del GDPR, da un lato, e i mezzi di ricorso previsti dagli artt. 78, par. 1, e 79, par. 1, del medesimo strumento, dall'altro lato[42]. Nella decisione i giudici di Lussemburgo hanno affermato che le disposizioni citate devono essere interpretate nel senso che i mezzi di ricorso da esse previsti possono essere esperiti parallelamente, senza che uno prevalga sull'altro ai sensi del regolamento, precisando tuttavia che l'esistenza di due decisioni contraddittorie metterebbe in discussione l'obiettivo di garantire un'applicazione coerente e omogenea delle norme in materia. Tale incoerenza determinerebbe una situazione di incertezza giuridica e di conseguenza un indebolimento della protezione delle persone fisiche con riguardo al trattamento dei dati personali che li riguardano. Sul punto, l'avvocato generale aveva rilevato che la sospensione del procedimento potrebbe rappresentare una soluzione in grado di garantire la certezza del diritto, senza compromettere – quantomeno nella sua sostanza – il diritto di agire dinanzi a un giudice che, per quanto di natura fondamentale, rimane comunque un diritto che non possiede valore assoluto, potendo subire restrizioni proporzionate che perseguano uno scopo legittimo[43].

35. Il parallelismo delle opzioni di tutela giuridica determina complessità anche nel caso di trattamenti transfrontalieri. Un primo motivo di complessità attiene al ricorso avverso una decisione dell'autorità di controllo. L'art. 77 del GDPR, come detto, attribuisce all'interessato il diritto di impugnare la decisione dinanzi alle autorità giurisdizionali dello Stato membro in cui risiede abitualmente o lavora oppure dello Stato membro del luogo ove si è verificata la presunta violazione. Ciò comporta che l'interessato ha la possibilità di introdurre un ricorso, in uno Stato membro, ad esempio l'Italia, anche nell'ipotesi in cui il titolare del trattamento abbia fissato il proprio stabilimento principale in un diverso Stato membro, ad esempio, l'Irlanda. Secondo quanto previsto dall'art. 60, par. 7, nel caso ipotizzato, se la decisione è sfavorevole al titolare (o responsabile) del trattamento, è l'autorità irlandese competente ad adottarla, avendo poi il compito di notificarla allo stabilimento principale o unico del titolare

[40] Egualmente, nella vigenza della direttiva 95/46/CE, veniva lasciato agli Stati membri il compito di determinare se imporre all'interessato di esaurire i rimedi amministrativi prima di poter rivolgersi all'autorità giurisdizionale. In proposito la Corte di Giustizia nel caso *Puškár* (sent. 27 settembre 2017, causa C-73/16, ECLI:EU:C:2017:725) ha affermato 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. La condizione del previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative è tuttavia inammissibile quando le modalità concrete di esercizio di detti rimedi pregiudichino eccessivamente il diritto a 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. Sul tema in dottrina si veda L. A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford, 2014, p. 187 ss.; A. Arnull, *The Principle of Effective Judicial Protection in EU law: An Unruly Horse?*, in *European Law Review*, 2011, 36.1, p. 51 ss.;

[41] Nell'ambito dell'ordinamento italiano, tale aspetto è disciplinato dall'art. 140-*bis* del cosiddétto 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 stato già adito il Garante, la domanda giudiziaria è parimenti improponibile, salva l'ipotesi di decorso del termine massimo per la decisione sul reclamo proposto o di inammissibilità dello stesso (comma 3).

[42] Corte di Giustizia, sent. 12 gennaio 2023, *Nemzeti Adatvédelmi* és *Információszabadság Hatóság*, causa C-132/21.

[43] Conclusioni dell'Avvocato Generale Jean Richard de La Tour, 8 settembre 2022, *Nemzeti Adatvédelmi* és *Információszabadság Hatóság*, causa C-132/21, § 70.

(o responsabile) del trattamento e di informare il garante per la protezione dei dati quale autorità di controllo interessata. Diversamente, ai sensi del successivo par. 8, se la decisione è sfavorevole alla persona interessata, spetta all'autorità di controllo italiana adottare la decisione che potrà poi essere impugnata dinanzi alle locali autorità giurisdizionali. Tale disciplina risulta di difficile applicazione sia nel caso in cui la decisione risulti sfavorevole in parte al titolare (o responsabile) del trattamento e in parte all'interessato, sia nel caso in cui l'autorità di controllo non dia seguito al reclamo o non riferisca sullo stato o sull'esito del ricorso nel termine di tre mesi. Nella prima eventualità risulta difficile determinare quale sia l'autorità giurisdizionale competente; nella seconda la possibilità dell'interessato di impugnare la decisione è condizionata dalla competenza dell'autorità di controllo, in virtù dell'applicazione del meccanismo dello sportello unico o ai sensi dell'art. 55 del GDPR, cioè se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. In sostanza, per quanto il legislatore europeo abbia optato per un criterio di competenza giurisdizionale flessibile, la scelta della autorità dinnanzi alla quale presentare il reclamo amministrativo risulta importante in quanto questa può condizionare la successiva tutela giurisdizionale effettiva avverso la decisione amministrativa e richiede dunque all'interessato la capacità di individuare lo stabilimento principale del titolare (o del responsabile) del trattamento.

36. Un secondo elemento di complessità attiene all'efficacia di provvedimenti di ingiunzione, eventualmente ammessi dal diritto nazionale applicabile, aventi ad oggetto diritti riconosciuti all'interessato dal GDPR (ad esempio, il diritto alla cancellazione o alla rettifica) nel territorio di un altro Stato membro. Si consideri, ad esempio, il caso di un ordine di cancellazione di dati personali, proveniente da un'autorità giurisdizionale competente sulla base del titolo della residenza abituale dell'interessato nello Stato membro del foro. È possibile chiedersi se tale autorità sia o meno competente ad adottare detto provvedimento nel caso in cui il titolare del trattamento abbia il suo stabilimento principale in un altro Stato membro, dove assume e attua decisioni sulle finalità e sulle modalità del trattamento dei dati. In proposito pare doversi ritenere che, considerato che il GDPR non contiene alcuna disposizione riguardo alla circolazione delle decisioni pronunciate da autorità giurisdizionali, trovi applicazione il Regolamento Bruxelles I-*bis* che detta la disciplina comune del riconoscimento e dell'esecuzione delle decisioni in materia civile e commerciale emesse dalle autorità giudiziarie degli Stati membri. Tale strumento, com'è noto, esprime l'idea di un unico spazio giudiziario europeo, caratterizzato dalla reciproca fiducia fra gli organi giudiziari e dalla libera circolazione delle decisioni, prevedendo che le sentenze che rientrano nel proprio ambito di applicazione vengano riconosciute ed eseguite senza che sia necessario il ricorso ad alcun procedimento, salva la possibilità di far valere motivi ostativi di cui all'art. 45, secondo la procedura delineata dagli artt. 46-51. Il Regolamento Bruxelles I-*bis* ricorre a un concetto ampio di decisione, ricomprendendovi anche i provvedimenti provvisori e cautelari emessi da un'autorità giurisdizionale competente a conoscere del merito ai sensi e all'esito di una procedura che si svolge nel contradditorio delle parti o, se adottati *inaudita altera parte*, comunque notificati alla parte interessata prima dell'esecuzione. Inoltre, l'art. 54, par. 1, del Regolamento Bruxelles I-*bis* prevede che nel caso in cui una decisione contenga un provvedimento ignoto al diritto dello Stato membro richiesto, tale provvedimento, compreso ogni eventuale diritto in esso indicato, dovrebbe essere adattato, nella misura del possibile, a un provvedimento che in base al diritto di tale Stato membro abbia efficacia equivalente e persegua obiettivi analoghi[44]. La circolazione di provvedimenti di ingiunzione che riconoscano

[44] La disposizione è da annoverarsi fra le novità del Regolamento Bruxelles I-*bis*. La Corte di Giustizia con riguardo al regime previsto dal Regolamento CE 44/2001, sostituito a partire dal 10 gennaio 2015 dal Regolamento Bruxelles I-*bis*, aveva operato una sorta di distinzione fra riconoscimento ed esecuzione delle decisioni. Per quanto riguarda l'esecuzione delle sentenze, la quale comporta l'adozione di provvedimenti coercitivi al fine di garantire l'attuazione di un diritto sancito da una decisione, la Corte ha fatto espressamente riferimento sia alla legge dello Stato d'origine sia a quella dello Stato richiesto per adattare gli effetti della decisione straniera agli effetti che produrrebbe una decisione nazionale. Di contro, per quanto riguarda il riconoscimento delle decisioni, la Corte si è generalmente riferita alla sola legge dello Stato membro in cui la sentenza è stata pronunciata. Secondo tale soluzione, qualificata dalla dottrina come norma dell'«estensione degli effetti», occorre fare riferimento alla legge dello Stato membro d'origine al fine di determinare gli effetti della sentenza invocata in un secondo Stato membro, tra i quali, segnatamente, i punti decisi da tale sentenza, i diritti ivi sanciti e le loro conseguenze materiali sulla situazione giuridica delle parti. In dottrina sul tema vedasi H. Gaudemet-Tallon, e M.-É. Ancel, *Compétence et exécution des*

diritti all'interessato non appare in linea con quanto previsto in ordine alla ripartizione delle competenze tra le autorità di vigilanza degli Stati. Il considerando 122 chiarisce al riguardo che ciascuna autorità di controllo è competente per l'espletamento dei compiti assegnatele e per l'esercizio dei poteri ad essa conferiti, ai sensi del GDPR. La sola eccezione a questa regola è rappresentata dal meccanismo dello sportello unico che, come detto, si attiva nel caso in cui il titolare (o responsabile) del trattamento operi in più Stati dell'Unione europea oppure il trattamento dei dati, pur effettuato da un titolare con sede in un solo Stato, incida in modo sostanziale su interessati residenti in più di uno Stato membro dell'Unione. Per ragioni di chiarezza sarebbe stata quindi utile una disposizione sul riconoscimento dei provvedimenti di ingiunzione e sulla portata dei relativi effetti, nonché la previsione di meccanismi volti a favorire la verifica dell'effettiva attuazione.[45]

37. Un terzo elemento di complessità attiene alla possibilità per le autorità di controllo di avviare un giudizio civile, nel caso in cui queste non rivestano la posizione di autorità capofila per il trattamento transfrontaliero di cui trattasi. Detta questione è stata affronta dalla Corte di Giustizia nella sentenza *Facebook Ireland e a.* del 2021, originata dal rinvio pregiudiziale sollevato dalla Corte di Appello di Bruxelles dopo che l'autorità di controllo belga, in forza della normativa nazionale aveva agito in sede giudiziale per fare accertare presunte violazioni del regolamento e ottenere una ingiunzione diretta a far cessare il trattamento di dati personali degli internauti nel territorio belga, effettuato dal *social network* Facebook, per mezzo di *cookie*, *social plugin* e *pixel* e alla distruzione dei dati personali così ottenuti[46]. I giudici di Lussemburgo hanno riconosciuto il ruolo preminente dell'autorità di controllo capofila per quanto riguarda il trattamento transfrontaliero, evidenziando che la coesistenza di diverse azioni non collegate, e potenzialmente contraddittorie, da parte delle autorità di controllo interessate può compromettere la coerenza e l'efficacia del sistema dell'Unione europea di tutela dei dati personali, con ricadute negative sul perseguimento dell'obiettivo di garantire un livello elevato di protezione dei diritti dei singoli. Consentire alle autorità di controllo di adire liberamente i loro giudici nazionali, in circostanze in cui alle stesse è precluso di avvalersi dei loro poteri amministrativi, in ragione dell'operatività dei meccanismi di cooperazione e coerenza previsti dal regolamento, aprirebbe la strada a una facile elusione di tali meccanismi e sconfesserebbe l'esigenza di una leale ed efficace cooperazione fra le autorità di controllo capofila e le autorità di controllo interessate. Il potere delle autorità interessate di agire dinanzi all'autorità giurisdizionale è infatti limitato, potendo esercitarsi nei soli casi e secondo le procedure previste dal GDPR, ad esempio, in relazione alle misure provvisorie che l'autorità può adottare nel proprio territorio a seguito della mancata risposta o del rifiuto di dare seguito alla domanda di fornire «informazioni utili e prestare assistenza reciproca» (art. 61, parr. 5 e 8). La Corte di Giustizia ha inoltre chiarito che spetta all'autorità giudiziaria investita di un'azione dall'autorità di controllo determinare se le norme sulla ripartizione delle competenze, nonché le procedure e i meccanismi pertinenti previsti dal GDPR, siano stati correttamente applicati nell'ambito del procedimento principale[47].

---

jugements en Europe, LGDJ, 6ª edizione, 2018, pp. 550 ss.; M. Requejo Isidro, *Brussels I Bis: A Commentary on Regulation (EU) n. 1215/2012*, Elgar Commentaries in Private International Law Series, 2022, p. 551 ss.

[45] Ulteriori dubbi sorgano nel caso in cui l'ingiunzione debba essere eseguita al di fuori del territorio dell'Unione europea. Tale questione, che attiene alla portata territoriale del GDPR e alla giurisdizione prescrittiva, è stata in parte affrontata dalla Corte di Giustizia, con riferimento al regime preesistente, nella sentenza *AG Szpunar* (Grande sezione, sent. 24 settembre 2019, causa C-507/17, ECLI:EU:C:2019:772) nella quale i giudici di Lussemburgo hanno affermato che il gestore di un motore di ricerca, quando accoglie una domanda di deindicizzazione, è tenuto ad effettuare tale operazione non in tutte le versioni del suo motore di ricerca, ma nelle versioni di tale motore corrispondenti a tutti gli Stati membri. Ulteriori indicazioni possono trarsi dalla decisione resa nel caso *Glawischnig-Piesczek* (sent. del 3 ottobre 2019, causa C-18/18, ECLI:EU:C:2019:821), avente ad oggetto la responsabilità dei prestatori di servizi di *hosting*. In dottrina si veda D. J. B. Svantesson, *Private International Law and the Internet*, III ed., Netherlands: Kluwer Law International, 2016, p. 474.

[46] Corte di Giustizia, sent. 15 giugno 2021, *Facebook Ireland e a.*, causa C-645/19, ECLI:EU:C:2021:483.

[47] Nella decisione *Facebook Ireland e. a.,* la Corte non ha risposto alla questione posta dal giudice del rinvio riguardo alla possibilità che delle procedure siano portate avanti in parallelo. Sul punto i giudici di Lussemburgo hanno rilevato che non era stato in alcun modo accertato che tale situazione si sarebbe verificata nella fattispecie sottoposta ad essi e pertanto, conformemente alla propria consolidata giurisprudenza in materia, hanno dichiarato inammissibile la questione pregiudiziale. Se la posizione della Corte non è criticabile tenuto conto della sua giurisprudenza ben consolidata, è innegabile che la questione posta dal giudice del rinvio è degna di interesse e che la situazione evocata potrebbe verificarsi nella pratica.

Tali considerazioni appaiono rilevanti, a maggiore ragione, nell'ipotesi in cui violazioni della disciplina dell'Unione in materia di protezione dei dati personali vengano accertate da un'autorità diversa dalle autorità di controllo, ad esempio un'autorità garante della concorrenza, che nell'ambito dei suoi poteri esamini, in via incidentale, la conformità delle prassi di una impresa alla disciplina contenuta nel GDPR. Per quanto la materia della tutela dei dati personali possa presentare in molti casi punti di contatto con altre materie, un'autorità di controllo diversa da quella istituita in base al regolamento non può ritenersi competente né a constatare, in via principale, eventuali violazione del GDPR, né ad applicare le sanzioni previste. Lo sconfinamento nelle competenze delle autorità di controllo, infatti, comprometterebbe la piena armonizzazione del diritto in materia di protezione dei dati, il cui elemento centrale è un meccanismo di attuazione armonizzato fondato sul principio dello «sportello unico», sancito dagli artt. 51-67 del GDPR.[48]

VI. *(segue)* la questione dell'efficacia delle decisioni dell'autorità di controllo nel successivo giudizio civile sul risarcimento dei danni

38. Il GDPR, probabilmente a causa delle notevoli differenze sussistenti a livello nazionale, non disciplina neanche la questione dell'efficacia delle decisioni adottate dall'autorità di controllo nell'eventuale separato giudizio che l'interessato intenda instaurare dinanzi all'autorità giurisdizionale per ottenere il risarcimento dei danni. Non risulta perciò chiaro se, ed eventualmente in quale misura, il giudice civile sia vincolato dalla decisione dell'autorità di controllo.

Verosimilmente negli Stati membri i cui sistemi processuali ammettono le cosiddette "prove atipiche", la decisione dell'autorità di controllo che accerti la violazione del regolamento assumerà una qualche rilevanza all'interno del giudizio per il risarcimento dei danni[49]. In altri ordinamenti potrebbero avere invece una diversa posizione, consentendo al titolare del trattamento convenuto nel giudizio di risarcimento danni di mettere in dubbio la violazione, anche nell'ipotesi in cui questa sia affermata in un provvedimento definitivo, in ragione della mancata impugnazione o del rigetto della richiesta di annulla-

[48] In proposito si vedano le conclusioni dell'avvocato generale della Corte di Giustizia del 20 settembre 2022, *Meta Platforms e a. (Conditions générales d'utilisation d'un réseau social)*, causa C-252/21, ECLI:EU:C:2022:704. La causa ad oggi pendente origina dalla questione pregiudiziale sollevata dal Tribunale superiore del Land di Düsseldorf, vertente, fra l'altro, sulla competenza di un'autorità nazionale garante della concorrenza, quale il Bundeskartellamt, ad esaminare, in via principale o incidentale, i comportamenti di un'impresa alla luce di talune disposizioni del regolamento (UE)2016/679.

[49] Nell'ordinamento italiano, anche prima dell'entrata in vigore del GDPR, i provvedimenti del Garante per la tutela dei dati personali hanno rappresentano un importante punto di riferimento nel processo di libero apprezzamento delle prove condotto dal giudice, anche se non sono state considerate come fonti di accertamento vincolanti, riguardo all'esistenza dell'infrazione. In proposito si veda F. Cafaggi (a cura di), *Casebook italiano in materia di diritti di protezione dei dati personali*, Ottobre 2018, Re-Jus Project, disponibile alla pagina www.rejus.eu/sites/default/files/content/materials/italian_casebook_data_protection.pdf, p. 38. Il problema dei rapporti fra l'*enforcement* amministrativo e quello giudiziale è stato maggiormente approfondito con riguardo al settore del diritto della concorrenza. Già prima dell'entrata in vigore del decreto legislativo del 19 gennaio 2017, n. 3, adottato in conformità della delega contenuta nella legge del 9 luglio 2015, n. 114, in attuazione della Direttiva 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, la Cassazione riteneva che il provvedimento accertativo di un illecito anticoncorrenziale adottato dall'Autorità Garante della Concorrenza e del Mercato fosse dotato di «una elevata attitudine a provare» la condotta lesiva della concorrenza. La giurisprudenza, a partire dal primo decennio del secondo millennio, ha coniato il concetto di «prova privilegiata» per designare le situazioni appena descritte. Inizialmente l'accertamento dell'Autorità Garante è stato reputato una fonte di presunzioni *iuris tantum*, rimessa al prudente apprezzamento del giudice e contestabile dall'interessato con qualsiasi controprova ammessa dall'ordinamento. Nel giro di pochi anni la giurisprudenza di legittimità è poi arrivata a estendere le maglie della prova privilegiata, fino al punto di affermare l'impossibilità che circostanze di fatto già accertate nel provvedimento amministrativo fossero rimesse in discussione all'interno del successivo giudizio civile, impedendo così all'impresa convenuta di sostenere l'insussistenza della violazione in base allo stesso materiale probatorio od alle stesse argomentazioni già disattese in sede di procedimento amministrativo. *Ex plurimis*, Cassazione, sent. 13 febbraio 2009, n. 3640, sent., 14 marzo 2011, n. 5942, sent. 10 maggio 2011, n. 10211, sent. 20 giugno 2011, n. 13486, sent. 23 aprile 2014, n. 9116. In dottrina, sul percorso compiuto dalla giurisprudenza italiana di legittimità, si veda F. Pasquarelli, *Da prova privilegiata a prova vincolante: il valore probatorio del provvedimento dell'AGCM a seguito della direttiva 2014/104/UE*, in *Diritto industriale*, II, 2016, n. 3, pp. 252 ss.; M. Golia, *La circolazione dell'accertamento dall'atto amministrativo al processo civile: intorno alla categoria di «prova privilegiata»*, in *Rivista trimestrale di diritto e procedura civile,* n. 2, 2021, pp. 379 ss.

mento. In detti Stati membri il giudice dinanzi al quale viene intentata un'azione di risarcimento danni sarà quindi chiamato a riesaminare i fatti e gli aspetti giuridici già oggetto di indagine e di valutazione, potendo all'esito di tale esame discostarsi dalle conclusioni contenute nella decisione finale adottata dall'autorità di controllo nazionale o straniera sulla medesima violazione del GDPR.

Il fatto che in relazione al *public enforcement* il regolamento preveda un sistema particolarmente complesso di ripartizione della competenza fra le diverse autorità di controllo, con lo scopo di evitare decisioni finali contrastanti, appare in contraddizione con la mancanza di una disposizione che accordi rilevanza alle decisioni definitive dell'autorità di controllo all'interno del giudizio per il risarcimento del danno. Allo stato attuale, pertanto, i tribunali che decidono sulle richieste di risarcimento danni possono discostarsi dalle conclusioni di una decisione finale presa dalla competente autorità di controllo, nazionale o straniera, sulla stessa presunta violazione della legge sulla protezione dei dati. Inoltre, il GDPR è sprovvisto di una norma che imponga la sospensione dei termini di prescrizione per i reclami presentati da privati per il tempo in cui l'autorità di controllo indaga sulla stessa violazione; di conseguenza tale questione è affidata ai diversi diritti nazionali.

L'importanza della ricerca di una qualche forma di sincronia fra il *public* e il *private enforcement* peraltro emerge in altri ambiti del diritto dell'Unione europea. Ad esempio, la direttiva 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 che gli Stati membri debbano provvedere affinché una violazione del diritto della concorrenza constatata da una decisione definitiva di un'autorità nazionale garante della concorrenza sia ritenuta definitivamente accertata o, in alternativa, valga «almeno a titolo di prova *prima facie*, del fatto che è avvenuta una violazione del diritto della concorrenza», ai fini dell'azione per il risarcimento del danno proposta, rispettivamente, dinanzi ai giudici nazionali o ai giudici di altro Stato membro.

Nel settore del diritto della concorrenza l'approccio seguito dal legislatore europeo è riconducibile alla specialità dell'attività di controllo e repressione svolta dalle autorità di controllo, nonché all'estensione delle regole che tradizionalmente sono previste per garantire il contraddittorio e i diritti di difesa per il destinatario della sanzione. In altri termini, all'autorità di controllo anti-trust risultano affidati compiti che presentano un carattere secondario sostanzialmente assimilabile a quello svolto dagli organi giurisdizionali.

L'obiettivo dell'unicità dell'accertamento, diretto a evitare contrasti tra quanto accertato, in relazione alle medesime circostanze fattuali, prima in sede amministrativa e poi in sede giurisdizionale, è funzionale a garantire un elevato livello di tutela degli individui. L'interesse perseguito non ha una dimensione solamente privatistica, perché il *private enforcement* ha una funzione anche e dichiaratamente pubblicistica, al punto che la Corte di Giustizia definisce le azioni di risarcimento danni per violazione delle regole di concorrenza dell'Unione come "parte integrante del sistema di applicazione di tali regole, che mira a contrastare i comportamenti anticoncorrenziali delle imprese e a dissuaderle dall'adottare tali comportamenti"[50]. Per fare ciò, l'accertamento della responsabilità e l'individuazione del soggetto responsabile devono coincidere in sede di *public* e *private enforcement*. Nella visione del legislatore dell'Unione europea, il carattere vincolante dell'accertamento condotto dall'autorità indipendente in materia di concorrenza risulta quindi un espediente tecnico-giuridico per incrementare l'effettività del diritto della concorrenza.

Analogamente a quanto avviene nel settore del diritto della concorrenza, anche le azioni di risarcimento del danno causato da violazioni del GDPR richiedono generalmente una complessa analisi fattuale, poiché gli elementi di prova necessari per comprovare la fondatezza della domanda risarcitoria sono spesso detenuti esclusivamente dal titolare (o responsabile) del trattamento o comunque non sono sufficientemente noti o accessibili all'interessato. In tali circostanze, rigide disposizioni giuridiche che prevedano che gli attori debbano precisare dettagliatamente tutti i fatti relativi al proprio caso all'inizio di un'azione e presentare elementi di prova esattamente specificati possono impedire in maniera indebita l'esercizio efficace del diritto al risarcimento riconosciuto espressamente dall'art. 82 del GDPR. Inoltre, allo stesso modo del contenzioso in materia di diritto della concorrenza, anche quello in materia di

[50] Corte di Giustizia, sent. 14 marzo 2019, in causa C-724/17, *Skanska Industrial Solutions e a.* (ECLI:EU:C:2019:204), punti 45 ss.

tutela dei dati personali si caratterizza per l'esistenza di un'asimmetria informativa fra le parti, pertanto l'attribuzione al titolare dei dati personali di vantaggi sul piano probatorio rappresenterebbe un elemento di riequilibrio delle diverse posizioni[51].

L'adozione di una norma che affermi il principio dell'unicità dell'accertamento, limitando le facoltà probatorie del titolare (o responsabile) del trattamento le cui operazioni sono state valutate dall'autorità di controllo come in violazione del GDPR, non sarebbe incompatibile con il principio della tutela giurisdizionale effettiva, garantito dall'art. 6 della Convenzione Edu e dall'art. 47 della CDFUE, poiché la sostanziale limitazione dei poteri processuali della parte convenuta nel processo di risarcimento del danno, cui sarebbe impedito di dare prova contraria della avvenuta violazione che sia accertata in via definitiva, risulterebbe controbilanciata dalla piena garanzia giurisdizionale accordata all'autore della violazione nei confronti dei provvedimenti sanzionatori dell'autorità, che potrebbero essere impugnati dinanzi al giudice ordinario ai sensi dell'art. 78 del GDPR.[52] Sarebbe quindi in tale sede che il titolare (o il responsabile) del trattamento, asserito trasgressore della disciplina a tutela dei dati personali, dovrebbe e potrebbe con pienezza di mezzi contestare il fondamento giuridico fattuale della propria pretesa responsabilità.[53] Del resto al giudice competente sull'impugnazione dovrebbe essere riconosciuto dagli ordinamenti nazionali un potere di controllo pregnante sui provvedimenti di accertamento o irrogativi di sanzioni delle autorità indipendenti, attraverso l'affermazione di un sindacato pienamente sostitutivo, non limitato alla sola legittimità dell'atto e capace di estendersi anche ai profili di discrezionalità tecnica. Peraltro nelle azioni risarcitorie cosiddette *stand alone* (ossia non precedute da una decisione dell'Autorità), il giudice civile, ai fini risarcitori, è chiamato a verificare direttamente ed in prima persona i presupposti dell'illecito, senza che occorra alcuna intermediazione dell'autorità di controllo.

L'introduzione di un effetto vincolante modellato sull'esempio del diritto europeo della concorrenza, *de lege ferenda*, appare una scelta conveniente per rafforzare le sinergie tra *pubblic* e *private enforcement* e di conseguenza giungere ad un miglioramento nell'applicazione della disciplina contenuta nel regolamento. Invero le autorità di controllo offrono le più ampie garanzie di competenza tecnica e il *pubblic enforcement* rimane la lama più affilata a disposizione del titolare dei dati personali, come si evince dagli artt. 58, 83 e 84 del GDPR. Ragioni di equilibrio di sistema portano a ritenere che l'esecuzione privata dovrebbe limitarsi a integrare gli sforzi delle autorità di controllo, rivelando ulteriori violazioni del regolamento sulla protezione dei dati che potrebbero altrimenti rimanere non perseguite a causa della mancanza di risorse o delle diverse priorità che le autorità di controllo si prefissano.

VII. Conclusioni

39. 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 alle esigenze di semplificazione e di unificazione del quadro giuridico in materia. Tale necessità si riscontra sia in relazione al *public (administrative) enforcement*, fondato sui

[51] Sul punto per un'approfondita analisi vedasi W. Wurmnest, M. Gömann, *Comparing Private Enforcement of EU Competition and Data Protection Law*, in *Journal of European Tort Law*, 2022, vol. 13.2, pp. 154-182.

[52] Peraltro, secondo la giurisprudenza della Corte Edu, il *fair trial* non ha ad oggetto unicamente il processo, ma anche il procedimento, amministrativo, considerato che per «tribunale» deve intendersi qualunque autorità che, pur attraverso un procedimento non formalmente come nell'ordinamento interno, adotti atti modificativi della realtà giuridica, incidenti significativamente nella sfera soggettiva di un soggetto privato, anche se tale funzione viene esercitata al di fuori di una organizzazione giurisdizionale. Secondo i giudici di Strasburgo la decisione amministrativa incidente su diritti e obblighi di carattere civile, per quanto adottata senza il rispetto di tutti i requisiti prescritti dal principio del *fail trail*, può nondimeno essere considerata adottata conformemente alla Convenzione, laddove le garanzie procedurali ivi previste siano comunque riscontrabili nella sede di controllo della decisione stessa. Si vedano in proposito Corte Edu, sent. 26 agosto 1997, *De Haan c. Paesi Bassi*, ric. n. 22839/93, §§ 52-55; sent. 27 ottobre 2009, *Crompton c. Regno Unito*, ric. n. 42509/05, § 79 e, in un contesto disciplinare, sent. 25 settembre 2018 (Grande Camera), *Denisov c. Ucraina*, ric. n. 76639/11, §§ 65, 67 e 72.

[53] In senso critico con riguardo alla materia della concorrenza, S. Bariatti - L. Perfetti, *Prime osservazioni sulle previsioni del "Libro bianco in materia di azioni per il risarcimento del danno per violazione delle norme antitrust della Commissione e del Codice del consumo quanto alle relazioni tra procedimenti antitrust e giurisdizione*, in *Rivista italiana di Diritto Pubblico comunitario*, 2008, 4, pp. 1151-1176.

poteri di azione dell'autorità di controllo, sia in relazione al *private enforcement*, incentrato sul diritto di ottenere il risarcimento del danno che viene riconosciuto a "chiunque" abbia subito un danno "materiale o immateriale" in conseguenza della violazione del regolamento. Il rafforzamento del *private enforcement*, operato dal GDPR, mira a innalzare i livelli di tutela delle persone fisiche e a garantire un'applicazione più completa, poiché le autorità pubbliche non possono occuparsi di tutti i casi a causa delle limitate risorse disponibili.

40. L'obiettivo di chiarezza perseguito dal GDPR è stato solo parzialmente raggiunto poiché permangono diversi aspetti della disciplina che risultano incerti e problematici. Innanzitutto, le disposizioni che riguardano la competenza giurisdizionale e il rapporto tra procedimenti civili paralleli non appaiono efficacemente coordinate con la disciplina internazionalprivatistica comune in materia civile e commerciale, attualmente contenuta nel regolamento n. 1215/2012 (cosiddetto "Bruxelles I-*bis*").

41. Parimenti la disciplina concernente il rapporto tra i ricorsi previsti dal GDPR, in caso siano adite simultaneamente autorità di controllo di più Stati membri riguardo a un trattamento di dati personali effettuato dallo stesso titolare del trattamento, risulta in molti casi di difficile applicazione, oltre a poter determinare l'inoperatività del criterio di competenza giurisdizionale della residenza abituale dell'interessato, introdotto dal legislatore per rafforzare i diritti procedurali delle persone fisiche titolari del diritto alla tutela dei dati personali.

Infine, il profilo di criticità più significativo, a parere di chi scrive, attiene al rapporto fra il rimedio amministrativo – sia esso sollecitato o meno dall'interessato – e il rimedio civilistico. L'autonomia processuale che gli Stati membri mantengono sul punto, particolarmente nelle situazioni di rilievo transnazionale, può far sì che la tutela concessa in forza di una decisione emessa a seguito di un ricorso proposto dinanzi all'autorità di controllo, che accerta una violazione delle disposizioni del regolamento, possa risultare incoerente con una seconda decisione giurisdizionale, derivante da un ricorso proposto dinanzi all'autorità giurisdizionale.

La possibile esistenza di due decisioni contraddittorie mette in discussione l'obiettivo di garantire un'applicazione coerente e omogenea delle norme in materia di tutela delle libertà e dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione europea. Tale eventualità al contempo comporta un indebolimento della protezione delle persone fisiche con riguardo al trattamento dei dati personali che li riguardano, nella misura in cui l'incoerenza che può derivarne è idonea a determinare una situazione di incertezza giuridica.