



FRANCESCA RAGNO\*

### ***IL DIRITTO FONDAMENTALE ALLA TUTELA DEI DATI PERSONALI E LA DIMENSIONE TRANSAZIONALE DEL PRIVATE ENFORCEMENT DEL GDPR***

SOMMARIO: 1. La protezione dei dati personali nell'Unione europea: uno sguardo al GDPR da una prospettiva internazionalprivatistica. – 2. Il regime di *double enforcement* delineato nel Regolamento e le specificità degli strumenti di tutela di carattere privatistico. – 3. Il *private enforcement* nell'ambito di controversie di carattere transnazionale: la questione della giurisdizione. – 4. Il *private enforcement* nell'ambito di controversie di carattere transnazionale: la questione della legge applicabile. – 5. Considerazioni conclusive.

#### *1. La protezione dei dati personali nell'Unione europea: uno sguardo al GDPR da una prospettiva internazionalprivatistica*

In un'era caratterizzata da un'inarrestabile evoluzione tecnologica, dall'ascesa della comunicazione digitale, dall'ubiquità della Rete e dall'avvento dell'*Internet of things* e degli *smart objects*, la raccolta e la condivisione di dati personali ha assunto proporzioni tali da rendere necessario che l'Unione europea si dotasse di un apparato giuridico unitario funzionale ad un duplice obiettivo: la tutela del diritto fondamentale di ogni persona alla protezione dei propri dati personali<sup>1</sup>, da un lato,

---

\* Professore associato di Diritto internazionale, Università degli Studi di Verona.

Lo scritto rientra nell'attività di ricerca del team «Autonomia Negoziabile e Nuove Modalità di Regolazione dei Rapporti Contrattuali, delle Controversie Commerciali Transnazionali e delle Insolvenze Transfrontaliere», istituito nell'ambito del Progetto di Eccellenza del Dipartimento di Scienze Giuridiche dell'Università degli Studi di Verona «Diritto, Cambiamenti e Tecnologie».

<sup>1</sup> Nell'ordinamento dell'Unione europea il diritto alla tutela dei dati personali è cristallizzato nell'art. 16 TFEU e nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea; per un'analisi di tali norme v. P. PIRODDI, *Art. 16 TFEU*, 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*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve*, cit., p. 1682 ss. Per una ricostruzione dell'emersione di tale diritto nell'ordinamento dell'Unione e della sua trasfigurazione in diritto fondamentale v. G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Cham, 2014, p. 185. Come sottolineato dalla Corte di giustizia, il diritto fondamentale alla protezione dei dati personali non va inteso come “una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità” v., sentenza del 24 settembre 2019, causa C-507/17, *Google LLC c. Commission*

e la promozione della libera circolazione dei medesimi all'interno dell'Unione (e a specifiche condizioni anche verso Paesi terzi), dall'altro<sup>2</sup>.

Quest'ardua opera di bilanciamento ha trovato compimento con l'emanazione del regolamento (UE) 2016/679<sup>3</sup> (cd. GDPR), che è subentrato alla direttiva 95/46/CE<sup>4</sup> e alle eterogenee norme nazionali che l'hanno implementata, al fine di accrescere la certezza del diritto in un ambito strategico per lo sviluppo dell'economia digitale nel mercato unico<sup>5</sup>, muovendo dalla rilevanza costituzionale riconosciuta dall'ordinamento dell'Unione al «diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi»<sup>6</sup> e tenuto conto dell'indiscutibile funzione socio-economica di tale diritto<sup>7</sup>.

---

*nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, punto 60; sentenza del 9 novembre 2010, Cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, EU:C:2010:662, punto 48. Sul delicato equilibrio tra protezione dei dati personali e tutela di altri diritti fondamentali v. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Riv. dir. media*, 2018, p. 1 ss.

<sup>2</sup> Per approfondimenti sulle implicazioni discendenti dalla “doppia anima” della disciplina europea di protezione dei dati personali v. N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, Milano, 2019, p. 35 ss.

<sup>3</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, in *GUUE* L 119 del 4 maggio 2016, pp. 1-88.

<sup>4</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *GUCE* L 231 del 23 novembre 1995, pp. 31-50.

<sup>5</sup> Considerando n. 9: “(s)ebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE”. Come ampiamente rilevato dalla dottrina, tuttavia, l'uniformazione promossa è inficiata dall'ampio margine di manovra riconosciuto agli Stati membri da svariate norme del regolamento. Per approfondimenti sul tema v. J. WAGNER, A. BENECKE, *National legislation within the framework of the GDPR*, in *European Data Protection Law Review*, 2016, p. 353 ss. Sulle questioni internazionali/privatistiche sollevate dall'elevato numero di *opening clauses* (più di 50) rinvenibili in un regolamento che, sotto questo profilo, può certamente dirsi atipico v. 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, p. 310 ss.; M. MANTOVANI, *Horizontal Conflicts of Member States' GDPR Complementing Laws: the Quest for a Viable Conflict-of-Laws Solution*, in *Riv. dir. int. priv. proc.*, 2019, p. 535 ss.

<sup>6</sup> Per questa accezione del diritto alla protezione dei dati personali cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2019, p. 11.

<sup>7</sup> Come osservato dalla dottrina “(i)l processo di commodification ha interessato pure i dati personali; tanto che l'esigenza principale a cui è indirizzata la disciplina del reg. UE 2016/679 è la circolazione dei dati ed essa è realizzata dettando regole di tutela della persona, volte cioè a fare in modo che quel fenomeno circolatorio, necessario e perciò inevitabile, non si spinga oltre il limite della dignità della persona” (R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, p. 2020, p. 765).

Come noto, il GDPR, autentica Magna Carta del diritto dell'Unione in materia di dati personali<sup>8</sup>, ha carattere inderogabile<sup>9</sup> ed è caratterizzato da un ambito di applicazione assai vasto. Sotto il profilo materiale, tale strumento disciplina il trattamento<sup>10</sup> (automatizzato o manuale) di informazioni riguardanti una persona fisica identificata o identificabile<sup>11</sup> (cd. “interessato”)<sup>12</sup> da parte di soggetti privati o di autorità o organismi pubblici. Posto che le informazioni oggetto di tutela non sono necessariamente riservate e non sempre attengono alla sfera privata e individuale delle persone, è evidente come il diritto alla protezione dei dati personali – nonostante gli evidenti punti di possibile convergenza<sup>13</sup> – vada concettualmente distinto dal diritto alla privacy<sup>14</sup>. La differenza ontologica tra tali diritti è del resto confermata dal loro diverso inquadramento nella Carta dei diritti fondamentali dell'Unione europea:

<sup>8</sup> Per questa definizione v. M. S. GAL, O. AVIV, *The Competitive Effects of the GDPR*, in *Journal of Competition Law & Economics*, 2020, p. 349.

<sup>9</sup> Il carattere inderogabile delle norme del GDPR comporta, sul piano internazionalprivatistico, che esse non siano eludibili attraverso la designazione della legge di uno Stato terzo (C. KOHLER, *Conflict of law issues in the 2016 Data protection regulation of the European Union*, in *Riv. dir. int. priv. proc.*, 2016, pp. 661-662) e non possano essere pregiudicate da sentenze/decisioni di un'autorità giurisdizionale o amministrativa di uno Stato terzo (art. 48 del GDPR).

<sup>10</sup> Sono tuttavia esclusi dal campo di applicazione del regolamento, *inter alia*, i trattamenti svolti per attività estranee dall'ambito di applicazione del diritto dell'Unione (art. 2, par. 2, lett. a) e i trattamenti effettuati da persone fisiche per l'esercizio di attività a carattere esclusivamente personale e domestico (art. 2, par. 2, lett. c)].

<sup>11</sup> Ai sensi dell'art. 4, par. 1, del regolamento si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

<sup>12</sup> Per il rilievo secondo cui l'ampiezza della categoria dei dati personali comporti che il rischio che il regime europeo in materia di dati personali assurga a una *law of everything* v. C. RINIK, *Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem*, in *International Review of Law, Computers & Technology*, 2019, pp. 1-2.

<sup>13</sup> Come è stato osservato, “privacy and data protection are characterized by a form of conceptual continuity where the former falls within the scope of mismanagement of personal information and the latter within the scope of wrongful failure to secure personal information”: ILA COMMITTEE ON THE PROTECTION OF PRIVACY IN PRIVATE INTERNATIONAL AND PROCEDURAL LAW (Chair: Burkhard Hess Co-Rapporteurs: Jan von Hein and Cristina Mariottini), *Interim Report and Commentary to the Draft Guidelines on Jurisdiction and Applicable Law*, reperibile alla pagina web: <<https://www.ila-hq.org/index.php/committees>>, p. 3. Nella giurisprudenza italiana si vedano Cass., 19 luglio 2016, n. 14694; Cass., 30 giugno 2001, n. 8889; Cass., 10 maggio 2001, no. 6507; Cass., 8 giugno 1998, n. 5658; in dottrina V. ZENO-ZENCOVICH, *Italian National Report: Data Protection in the Internet*, in D. MOURA VICENTE/S. VASCONCELOS CASIMIRO (a cura di), *Data Protection in the Internet*, Cham, 2020, p. 245.

<sup>14</sup> D. COOPER, C. KUNER, *Data Protection Law and International Dispute Resolution*, in *Recueil des cours*, Vol. 382, 2015, p. 60; C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impr.*, 2020, p. 864. Per approfondimenti sulla distinzione tra privacy e tutela dei dati personali (cd. *informational privacy*) v. C. FARALLI, *La privacy dalle origini ad oggi. Profilo storico-filosofico*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, cit., pp. 6-7; G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai «safe harbour principles» al «privacy shield»*, Roma, 2016, pp. 133-134; A. FORDE, *The Conceptual Relationship Between Privacy and Data Protection*, *Cambridge Law Review*, 2016, p. 135 ss.; J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, p. 222 ss.; S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014, p. 31 ss.; M. TZANOU, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, in *International Data Privacy Law*, 2013, p. 88 ss.; B. VAN DER SLOOT, *Privacy as Virtue: Moving Beyond the Individual in the Age of Big Data*, 2017, p. 11 ss.

mentre il diritto alla privacy è garantito dall'art. 7, il diritto alla tutela dei diritti personali è codificato nell'art. 8<sup>15</sup>.

Altrettanto ampio risulta l'ambito di applicazione territoriale della normativa europea<sup>16</sup>. Nell'individuare unilateralmente la propria sfera di operatività, il regolamento non si limita a valorizzare, sul modello di quanto previsto nell'art. 4 della previgente direttiva, l'ubicazione dello stabilimento del titolare (o del responsabile) del trattamento all'interno dell'Unione (art. 3, par. 1)<sup>17</sup>, ma estende la propria portata precettiva anche ai titolari (o ai responsabili) del trattamento di Paesi terzi rispetto alle attività di trattamento dei dati personali di interessati che si trovino nell'Unione<sup>18</sup>, subordinandola però ad una duplice condizione (art. 3, par. 2): le attività di trattamento devono essere funzionali ad offrire agli interessati beni o servizi

<sup>15</sup> Le due disposizioni prevedono, rispettivamente, che “Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni” (art. 7) e che “1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo 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 individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente” (art. 8). Come noto, siffatta distinzione non trova corrispondenza nella Convenzione europea sui diritti dell'uomo, che, all'art. 8, riconosce unicamente il diritto al rispetto della vita privata e familiare; la giurisprudenza della Corte europea dei diritti dell'uomo ha tuttavia supplito a tale lacuna normativa (ben comprensibile se si considera che la CEDU risale al 1950) ricorrendo ad un'interpretazione estensiva della nozione di vita privata: v., da ultimo, Corte europea dei diritti dell'uomo, sentenza del 28 settembre 2018, ricorso n. 60798/10 e 65599/10, *M.L. et W.W. c. Germania*, punto 86.

<sup>16</sup> A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, p. 126 ss.; M. GÖMANN, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*, in *Common Market Law Review*, 2017, p. 567 ss.

<sup>17</sup> Ai sensi dell'art. 3, par. 1, il regolamento si applica 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. Al riguardo la Corte di giustizia, in sede di interpretazione della direttiva 2016/679, ha chiarito che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una controllata destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro (sentenza del 13 maggio 2014, Causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, EU:C:2014:317, punto 60).

Per quanto concerne la nozione di stabilimento, va ricordato che la Corte di giustizia ha optato per un'interpretazione ampia tale da valorizzare “qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile”, a prescindere dalla forma giuridica adottata: v. sentenza del 1° ottobre 2015, Causa C-230/14, *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság*, EU:C:2015:639, punto 29.

<sup>18</sup> Si noti che ciò che è richiesto ai fini dell'applicazione del regolamento – ex art. 3 par. 2 – è la mera “presenza fisica” dell'interessato nell'Unione e non la sua “residenza”. Tale scelta è comprensibile se si considera il rango del diritto tutelato: “i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza” (Considerando n. 2). Per il rilievo secondo cui “la scelta di estendere la tutela prevista dalle disposizioni del regolamento anche alle ipotesi nelle quali tali soggetti siano solo presenti sul territorio europeo riecheggia (...) considerazioni relative all'ambito di applicazione degli strumenti in materia di tutela dei diritti fondamentali e al dovere dell'Unione di offrire una tutela efficace a tali diritti” v. G. ROSSILLO, *Diritti fondamentali, norme unilaterali e norme imperative alla luce del regolamento 2016/679 sul trattamento e la libera circolazione dei dati personali*, in *Liber amicorum Angelo Davì. La vita giuridica internazionale nell'età della globalizzazione*, vol. I, Napoli, 2019, p. 610.

(indipendentemente dal fatto che sia previsto un corrispettivo in denaro<sup>19</sup>) oppure a monitorare il loro comportamento (qualora il comportamento abbia luogo all'interno dell'Unione).

L'art. 3, par. 2, del GDPR, espandendo la sovranità digitale<sup>20</sup> dell'Unione europea fino a spingerla fino alle colonne d'Ercole del diritto internazionale<sup>21</sup>, rappresenta il precipitato normativo di un chiaro indirizzo extraterritoriale tracciato dalla giurisprudenza della Corte di giustizia<sup>22</sup> e caratterizzato da una specifica finalità politica: l'europeizzazione<sup>23</sup> della *governance* della Rete<sup>24</sup>. Tale norma appare particolarmente interessante sotto il profilo internazionalprivatistico non solo per la sua evidente valenza conflittuale<sup>25</sup>, ma anche perché sembra riecheggiare una logica comune alle norme del diritto dell'Unione europea che accordano ai consumatori il privilegio del foro e una disciplina di *favor* sotto il profilo della legge applicabile<sup>26</sup>.

<sup>19</sup> Tale specificazione, non sorprendente se si pensa che nel mercato digitale i dati personali rappresentano molto frequentemente il corrispettivo a fronte del quale vengono forniti beni, servizi o contenuti (cfr., al riguardo, l'art. 3, par. 1 della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, *relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali*, in *GUUE* del 22 maggio 2019, L 136, p. 1 ss.), denota la natura multiforme del dato personale quale "oggetto di un diritto fondamentale" e, al contempo, "bene economico" (G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, cit., p. 7). Per approfondimenti sul tema dei dati personali quale corrispettivo contrattuale v. A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Milano, 2019, p. 1381 ss.; P. HACKER, *Daten als Gegenleistung Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, in *Zeitschrift für die gesamte Privatrechtswissenschaft*, 2019, p. 148 ss.; C. LANGHANKE, M. SCHMIDT-KESSEL, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 2015, p. 218 ss.; A. METZGER, *Data as counter-performance: What rights and duties do parties have?*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, p. 2 ss.; A. SATTLER, *Personenbezogene Daten als Leistungsgegenstand*, in *JuristenZeitung*, 2017, p. 1036 ss.

<sup>20</sup> Per questa espressione v. V. ZENO ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai «safe harbour principles» al «privacy shield»*, cit., p. 7.

<sup>21</sup> V. C. KOHLER, *Conflict of law issues in the 2016 Data protection regulation of the European Union*, cit., p. 660: "the scope of the Regulation reaches to the outer limits of what is permitted under international law. Indeed, the scope extends beyond the scenario in Google. As appears from Art. 3(2), of the Regulation, a company based in a third State, without any establishment in the Union will be subjected to the Regulation's data protection regime by merely directing its activities to the territory of the EU. However, the condition that the processing relates to data of a person who is "in the Union" would seem to justify the broadness of the territorial scope of the Regulation in the light of both the commercial objective of the data processing and the effects thereof in the EU. Indeed, given the ubiquity of the internet and other global media, the effects of any processing of data outside the Union will be felt immediately within the Union as if the processing had occurred here".

<sup>22</sup> Sentenza del 6 ottobre, 2015, Causa C-362/14, *Maximilian Schrems c. Data Protection Commissioner* (cd. Schrems I), EU:C:2015:650; sentenza del 13 maggio 2014, Causa C-131/12, *Google Spain SL*, cit.

<sup>23</sup> Sulla particolare accezione di tale termine per quanto concerne l'indagine in esame v. O. LYNKEY, *The Europeanisation of Data Protection Law*, in *Cambridge Yearbook of European Legal Studies*, 2017, p. 254.

<sup>24</sup> Cfr. G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, cit., p. 134.

<sup>25</sup> Sul tema v. G. ROSSOLILLO, *Diritti fondamentali, norme unilaterali e norme imperative alla luce del regolamento 2016/679 sul trattamento e la libera circolazione dei dati personali*, cit., p. 598; G.M. RUOTOLO, *La lotta alla frammentazione geografica del mercato unico digitale: tutela della concorrenza, uniformità, diritto internazionale privato*, in *Dir. comm. int.*, 2018, p. 519 ss.

<sup>26</sup> Come discusso altrove, le norme europee di diritto internazionale privato a protezione dei consumatori operano solo nell'ipotesi in cui il professionista indirizzi la propria attività nello Stato (membro) in cui essi risiedono (o sono domiciliati). Sul punto sia consentito rinviare a F. RAGNO, *Art. 6 Rome I Regulation*, in F. FERRARI (a cura di), *Concise Commentary on the Rome I Regulation*, Cambridge, 2020, p. 170 ss.

Quanto alla disciplina sostanziale posta dal regolamento, nel ventaglio di diritti “classici” e “dinamici”<sup>27</sup> riconosciuti agli interessati particolare centralità assumono il cd. diritto all’oblio<sup>28</sup> e il diritto alla portabilità dei dati<sup>29</sup>. Per quanto concerne gli obblighi posti ai titolari e ai responsabili del trattamento, sebbene non sia certo questa la sede per tratteggiare una disciplina delineata in molteplici articoli del regolamento, appare opportuno sottolineare come il GDPR sia incentrato su alcuni principi chiave (liceità, correttezza e trasparenza, limitazione della finalità, esattezza, limitazione della conservazione, integrità e riservatezza e responsabilizzazione)<sup>30</sup> che devono necessariamente essere osservati dagli “obbligati” in sede di raccolta e di trattamento dei dati personali (art. 5).

Nell’ottica del contenzioso transnazionale tra privati, di rilievo centrale appare la norma che annovera tra i presupposti di liceità del trattamento il consenso prestato dall’interessato rispetto “ad una o più specifiche finalità” (art. 6 par. 1, lett. a), ovvero la preordinazione del trattamento “all’esecuzione di un contratto di cui l’interessato è parte o all’esecuzione di misure precontrattuali adottate su richiesta dello stesso” (art. 6 par. 1, lett. b). Con riguardo al consenso, nozione autonoma da intendersi come “manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento” (art. 4, n. 11)<sup>31</sup>, particolarmente degna di nota appare la ripartizione dell’onere della prova ai sensi dell’art. 7, par. 1: tale norma richiede che sia il titolare del trattamento a dover essere in grado di dimostrare che l’interessato ha prestato il proprio consenso al trattamento dei propri dati personali<sup>32</sup>.

<sup>27</sup> Per questo distinguo v. F. PIZZETTI, *La protezione dei dati personali e la sfida dell’Intelligenza Artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 25 e 30.

<sup>28</sup> Sull’ambito di applicazione territoriale del diritto all’oblio v. l’importante sentenza della Corte di giustizia del 24 settembre 2019, Causa C-507/17, *Google LLC c. Commission nationale de l’informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772. In dottrina v. V. CUFFARO, *Cancellare i dati personali, dalla damnatio memoriae al diritto all’oblio*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, cit., p. 219 ss.

<sup>29</sup> In argomento v. S. TROIANO, *Il diritto alla portabilità dei dati*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, cit., p. 195 ss.

<sup>30</sup> Nel senso che tali principi denotino la volontà di creazione di un’autentica “carta dei diritti individuali” v. G. COMANDÉ, F. MALGIERI, *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo Regolamento europeo sulla Privacy*, Milano, 2018, p. 16. Sul principio di *accountability* quale perno su cui ruota il sistema del GDPR v. G. FINOCCHIARO, *Il principio di accountability*, in *Giur. it.*, 2019, p. 2778 ss.

<sup>31</sup> Come specificato dal considerando n. 32, “il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l’interessato manifesta l’intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un’apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell’informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l’interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l’inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell’interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso”.

<sup>32</sup> Per l’idea secondo cui tale disposizione si ponga in linea di continuità con il principio di responsabilizzazione, di cui all’art. 5, par. 2, v. S. BRINK, H. A. WOLFF (a cura di), *Art. 7 DS-GVO*, in *BeckOK Datenschutzrecht*<sup>33</sup>, Monaco di Baviera, 2020, para. 86.

## 2. Il regime di “double enforcement” delineato nel Regolamento e le specificità degli strumenti di tutela di carattere privatistico

Operata una succinta (ed evidentemente sommaria) ricostruzione delle linee direttrici in cui si articola la disciplina in esame, è possibile ora soffermarsi sul regime duale che il regolamento tratteggia<sup>33</sup> per quanto concerne il suo *enforcement*.

Sotto il profilo del *public (administrative) enforcement*, il regolamento attribuisce alle Autorità di controllo dei rispettivi Stati membri<sup>34</sup> un compito di controllo, vigilanza e garanzia rispetto all’effettiva e coerente applicazione delle proprie disposizioni<sup>35</sup> e a tal fine le dota di pervasivi poteri d’indagine, correttivi, sanzionatori<sup>36</sup>, autorizzativi e consultivi, prevedendo meccanismi di collaborazione (anche attraverso il supporto del Comitato europeo per la protezione dei dati) e di assistenza reciproca tra esse allorché il trattamento dei dati abbia carattere transfrontaliero<sup>37</sup>. L’azione delle autorità di controllo può essere sollecitata dagli interessati (o dai soggetti rappresentativi dei diritti degli interessati ex art. 80, par. 2), che lamentino una violazione del regolamento. Secondo quanto previsto dall’art. 77, infatti, la tutela di carattere amministrativo può essere invocata proponendo un reclamo all’autorità di controllo dello Stato membro in cui l’interessato risiede abitualmente o lavora oppure ove si è verificata la presunta violazione<sup>38</sup>. Le decisioni assunte al riguardo dall’autorità di controllo sono impugnabili attraverso un ricorso giurisdizionale<sup>39</sup>, che può essere esperito anche in

<sup>33</sup> Sottolinea la natura “mista” del sistema di protezione civilistico-pubblicistico approntato dal regolamento F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali*, G. FINOCCHIARO (a cura di), *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 132. In senso analogo v., altresì, J. BING, *Data Protection, Jurisdiction and the Choice of Law*, in *Privacy Law & Policy Reporter*, 1999, p. 92; B. HESS, *The Private-Public Divide in International Dispute Resolution*, in *Recueil des cours*, vol. 388, 2016, p. 170.

<sup>34</sup> Ai sensi dell’art. 2 *bis* del Codice sulla protezione dei dati personali, l’Autorità di controllo, in Italia, è il Garante per la protezione dei dati personali.

<sup>35</sup> Cfr. art. 57 del regolamento.

<sup>36</sup> Per quanto concerne il regime di *public enforcement*, uno strumento centrale è rappresentato dalle sanzioni amministrative che possono essere irrogate dalle Autorità di controllo alle condizioni e nei termini stabiliti dall’art. 83. Per quanto il profilo delle sanzioni si noti che, nell’ordinamento italiano, il Codice in materia di protezione dei dati personali, così come novellato dal d.lgs. 10 agosto 2018, n. 101 (contenente disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento in esame), ha introdotto sanzioni penali per il caso di trattamento illecito di dati (art. 167) e per altre fattispecie delittuose tipizzate dal legislatore. Per approfondimenti al riguardo v. R. FLOR, “*Digital identity protection*”: Quo Vadis *Diritto penale?*, in P. BERTOLI, F. FERRARI, G. RIPAMONTI E G. TIBERI (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, Torino, 2019, p. 127 ss.

<sup>37</sup> Ai sensi dell’art. 4, par. 23, del regolamento ricorre tale ipotesi qualora il trattamento di dati personali abbia luogo “nell’ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell’Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro, oppure il trattamento incida o possa incidere in modo sostanziale su interessati in più di uno Stato membro”.

<sup>38</sup> Per una compiuta analisi sui meccanismi di tutela in via amministrativa previsti del regolamento anche alla luce della normativa codicistica italiana v. A. CANDINI, *Tutela amministrativa e giurisdizionale*, in G. FINOCCHIARO (a cura di), *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 742 ss.

<sup>39</sup> Ai sensi dell’art. 78, par. 3, tale ricorso va promosso dinanzi alle autorità giurisdizionali dello Stato membro in cui l’autorità di controllo è stabilita. Per quanto concerne l’Italia, l’art. 152 del Codice in materia di protezione dei dati personali assoggetta le controversie in esame al rito del lavoro, prevedendo che i ricorsi giurisdizionali vadano promossi, in via alternativa, dinanzi al tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell’interessato.

caso di inerzia da parte della stessa, di ritardi nella trattazione o nelle informazioni da fornire all'interessato (art. 78).

A corredo di tale sistema di tutela di stampo pubblicistico, il GDPR ha predisposto strumenti e rimedi di carattere privatistico funzionali a supplire alle possibili inadeguatezze del *public enforcement*<sup>40</sup>. All'interessato, segnatamente, l'art. 79, par. 1, del regolamento accorda, in attuazione dell'art. 47 della Carta<sup>41</sup>, la possibilità di promuovere un'azione nei confronti del titolare (o del responsabile) del trattamento dinanzi ad un'autorità giudiziaria "qualora ritenga" che i diritti riconosciutogli del regolamento siano stati violati a seguito di un trattamento. Posto che il rispetto di diritti da parte del titolare (o del responsabile) del trattamento comporta l'adempimento di specifici obblighi di *facere* o di *non facere*, se ne desume che l'azione in esame sarà di norma preordinata ad ottenere un provvedimento inibitorio<sup>42</sup>.

Ancora più significativa, ai fini della nostra analisi, è la tutela risarcitoria delineata nell'art. 82: tale norma, che ha immediatamente catalizzato l'attenzione di molti commentatori<sup>43</sup>, riconosce a "chiunque" abbia subito un danno "materiale o immateriale" causato da una violazione del regolamento "il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile dal trattamento".

Il regime di responsabilità solidale<sup>44</sup>, configurato dal GDPR in linea di sostanziale continuità con la disciplina previgente<sup>45</sup>, presenta tratti distintivi che meritano di essere ricordati.

In primo luogo, sotto il profilo soggettivo, la pretesa risarcitoria può essere invocata nei confronti del titolare (o del responsabile) del trattamento<sup>46</sup> non solo dall'interessato, ma anche da terzi che siano stati effettivamente pregiudicati da una violazione delle norme del

---

<sup>40</sup> Cfr. M. BRKAN, *Data protection and European private international law: observing a bull in a China shop*, in *International data privacy law*, 2015, p. 258.

<sup>41</sup> L'art. 47 della Carta, come noto, afferma il diritto di ogni individuo – i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati – ad un ricorso effettivo e ad un giudice indipendente e imparziale che esami la causa intentata equamente, pubblicamente ed entro un termine ragionevole.

<sup>42</sup> Sul punto v. C. KOHLER, *Conflict of law issues in the 2016 Data protection regulation of the European Union*, cit., p. 667.

<sup>43</sup> F. BILOTTA, *La responsabilità civile nel trattamento dei dati personali*, in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, p. 445 ss.; M. RATTI, *La responsabilità da illecito trattamento dei dati personali*, in G. FINOCCHIARO (a cura di), *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 773. ss.; G.M. RICCIO, *Art. 82 - Diritto al risarcimento e responsabilità*, in *GDPR e normativa privacy - Commentario*, a cura di G.M. RICCIO, G. SCORZA, E. BELISARIO, Milano, 2018, p. 596.

<sup>44</sup> L'art. 82, par. 4, del GDPR suggella la regola della solidarietà passiva nell'ipotesi in cui una molteplicità di titolari del trattamento o responsabili del trattamento oppure ancora il titolare del trattamento e il responsabile del trattamento congiuntamente siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento.

<sup>45</sup> Cfr. M. TESCARO, *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'Internet Provider nel diritto italiano tra Direttiva 2000/31/CE, Regolamento UE 2016/679 e Direttiva UE 2019/790*, in *jus civile*, 2020, 1, p. 86. Per un raffronto tra l'art. 23 della direttiva 95/46, trasposto nell'ordinamento italiano mediante l'art. 15 del Codice privacy (ora abrogato), e l'art. 82 del GDPR v. S. SERRAVALLE, *Il danno da trattamento dei dati personali nel GDPR*, Napoli, 2020, p. 10 ss.

<sup>46</sup> Al riguardo va però differenziata la posizione del titolare e del responsabile del trattamento: mentre il primo "risponde per il danno cagionato dal suo trattamento che violi il presente regolamento", il secondo "risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento".

regolamento<sup>47</sup>. Quest'interpretazione, ancorché non univocamente condivisa in dottrina<sup>48</sup>, sembra suffragata non solo dal dato letterale della norma, ma anche dalle finalità perseguite dal regolamento. Sotto il primo profilo, è significativo che l'art. 82 si distingue da una pluralità di altre disposizioni del regolamento omettendo ogni richiamo alla figura dell'interessato (*ubi lex voluit dixit, ubi noluit tacuit*)<sup>49</sup>. Sotto il secondo profilo, la crucialità della protezione dei dati per il corretto funzionamento del mercato digitale, ad avviso di chi scrive, non può che implicare il riconoscimento delle posizioni giuridiche di chi in tale mercato opera, ad esempio quale concorrente. A suffragio di quanto sopra esposto, basti ricordare l'indirizzo emerso nella giurisprudenza tedesca e italiana<sup>50</sup> secondo cui la violazione delle norme sulla privacy e sui dati personali da parte di un'impresa sono suscettibili di integrare la fattispecie di illecito per concorrenza sleale di cui, rispettivamente, all'art. 3 della legge tedesca sulla concorrenza sleale<sup>51</sup> (*Gesetz gegen den unlauteren Wettbewerb*) e all'art. 2598, n. 3 del codice civile italiano<sup>52</sup>. La controversa<sup>53</sup> possibilità di qualificare le norme del GDPR quali “regole di condotta del mercato” ai fini dell'applicazione di una specifica normativa nazionale è stata di recente posta all'attenzione della Corte di giustizia a seguito di un rinvio pregiudiziale promosso dalla Suprema Corte tedesca<sup>54</sup>: posta la rilevanza del quesito posto, non rimane altro che attendere

<sup>47</sup> In questo senso v., anche, M. RATTI, *La responsabilità da illecito trattamento dei dati personali*, cit., p. 775; G.M. RICCIO, *Art. 82 - Diritto al risarcimento e responsabilità*, cit., p. 600.

<sup>48</sup> *Contra*, ad esempio, v. E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, p. 98 e ss.

<sup>49</sup> Peraltro nemmeno il considerando (n. 146) riferibile alla norma in esame può essere richiamato a supporto di un'interpretazione restrittiva della categoria dei danneggiati. Al contrario, il fatto che in tale considerando la titolarità del diritto al risarcimento sia riconosciuta alla “persona” e non alla “persona fisica” (termine onnipresente nel regolamento) parrebbe ulteriormente supportare la bontà della lettura prospettata.

<sup>50</sup> V., ad esempio, per la prima, le sentenze dell'Oberlandesgericht Stuttgart del 27 febbraio 2020, 2 U 257/19, in *Monatsschrift für Deutsches Recht*, 2020, p. 684, dell'Oberlandesgericht Naumburg del 7 novembre 2019, 9 U 6/19, reperibile al sito <<https://openjur.de/u/2262636.html>>, dell'Oberlandesgericht Hamburg del 25 ottobre 2018, 3 U 66/17, in *Gewerblicher Rechtsschutz und Urheberrecht*, 2019, p. 86 e, per la seconda, Trib. Roma, Sez. spec. per la proprietà industriale e intellettuale, ordinanza del 3 luglio 2007, reperibile sul sito: <[http://www.astrid-online.it/static/upload/protected/TRIB/TRIB-CIVILE-ROMA-Ord-03\\_07\\_07pdf.pdf](http://www.astrid-online.it/static/upload/protected/TRIB/TRIB-CIVILE-ROMA-Ord-03_07_07pdf.pdf)>.

<sup>51</sup> Ai sensi di tale norma compie atti di concorrenza sleale “chiunque violi una disposizione di legge destinata, tra l'altro, a regolamentare il comportamento sul mercato nell'interesse dei suoi operatori, quando la violazione sia di natura tale da ledere in modo sensibile gli interessi dei consumatori, degli altri operatori del mercato o dei concorrenti”.

<sup>52</sup> Secondo tale disposizione compie atti di concorrenza sleale chiunque si valga “direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda”.

<sup>53</sup> Per un'opinione avversa a quella mantenuta nel testo v., nella giurisprudenza tedesca, sentenza del Landesgericht Magdeburg del 18 gennaio 2019, 36 O 48/18, in *Monatsschrift für Deutsches Recht*, 2019, p. 402; sentenza del Landesgericht Bochum del 7 agosto 2018, O 85/18, in *Betriebsberater*, 2018, p. 2580; sentenza del Landesgericht Wiesbaden del 5 novembre 2018, 5 O 214/18, in *Kommunikation & Recht*, 2019, p. 281. Per una posizione oltremodo restrittiva al riguardo v. sentenza dell'Oberster Gerichtshof del 26 novembre 2019, 4 Ob 84/19k, disponibile sul sito <<https://www.ris.bka.gv.at>>, secondo cui la tutela dei personali equivarrebbe ad un diritto di esclusiva, la cui lesione potrebbe essere fatta valere unicamente dall'interessato. Al di là del fatto che l'assimilazione del diritto alla tutela dei dati personali ad un diritto di esclusiva mal si concilia con il dato per cui ai sensi dell'art. 6 sono perfettamente leciti trattamenti non fondati sul consenso degli interessati, appare davvero incomprensibile come la Corte non colga la stridente contraddizione delle proprie affermazioni rispetto ai poteri di iniziativa e di impulso *ex officio* riconosciuti alle autorità di controllo.

<sup>54</sup> V. ordinanza del Bundesgerichtshof, 26 maggio 2020, Ref. I ZR 186/17, disponibile al sito <<https://openjur.de/u/2241869.html>>: la Corte suprema tedesca, muovendo da un caso relativo ad supposto illecito trattamento da parte di Facebook dei dati personali degli utenti che fruivano della “App Center”

la posizione dei giudici del *Kirchberg* sul punto per poterne auspicabilmente ricavare indicazioni rispetto (anche) al profilo in esame.

Per quanto concerne il danno e la sua risarcibilità, va sottolineato che, come indicato nel considerando n. 146, il concetto di danno (patrimoniale e non patrimoniale)<sup>55</sup> dovrebbe essere interpretato estensivamente e tenendo conto degli approdi giurisprudenziali della Corte di giustizia<sup>56</sup>. In ogni caso è posto in capo al danneggiato l'onere di provare sia il danno lamentato sia il nesso eziologico sussistente tra esso e l'asserita violazione delle norme del Regolamento<sup>57</sup> (tenuto conto degli atti delegati e agli atti di esecuzione adottati in conformità al regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni dello stesso); visto che i legittimati attivi all'azione risarcitoria non sono i soli interessati, la tesi per cui, ai sensi dell'art. 82, la violazione delle norme del GDPR produrrebbe un danno in *re ipsa* non pare persuasiva<sup>58</sup>.

Di contro, per quanto consta il criterio di imputazione della responsabilità, sul danneggiato non incombe l'onere di provare la colpa del danneggiante. Al contrario, è il titolare (o il responsabile) del trattamento a dover dimostrare che l'evento dannoso non gli è in alcun modo imputabile. Alla luce del principio di responsabilizzazione e dai "marcati profili di oggettivazione del rischio da trattamento dei dati personali"<sup>59</sup> che permeano il GDPR, si reputa che il danneggiante possa liberarsi da responsabilità solo dimostrando di avere adottato le misure tecniche e organizzative adeguate a prevenire il danno<sup>60</sup>, se del caso esibendo certificazioni protocolli che attestino il rispetto di elevati standard di sicurezza<sup>61</sup>.

---

disponibile sulla piattaforma Facebook, ha chiesto alla Corte di giustizia di chiarire se "le regole di cui al capo VIII del regolamento ostino alla possibilità che disposizioni nazionali che – oltre ai poteri di intervento delle autorità di vigilanza preposte al controllo e all'applicazione del regolamento e ai mezzi di ricorso a disposizione degli interessati – legittimino concorrenti, da un lato, e associazioni, istituzioni e camere di diritto nazionale, dall'altro, ad agire contro i soggetti che abbiano violato il regolamento (UE) 2016/679 (indipendentemente dalla violazione di diritti specifici dei singoli interessati e senza il mandato del soggetto interessato), al fine di inibire pratiche commerciali sleali, prevenire violazioni delle normative a tutela dei consumatori e vietare l'impiego di condizioni generali inefficaci".

<sup>55</sup> L'impiego della locuzione "danno materiale" e "danno immateriale" in luogo di "danno patrimoniale" e "danno non patrimoniale" nella versione italiana del regolamento è chiaramente frutto di una traduzione inaccurata: v., al riguardo, E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno Resp.*, 2020, p. 440.

<sup>56</sup> Nel senso che ciò imponga di tenere in considerazione la giurisprudenza della Corte di giustizia in materia di danni relativi ad ambiti diversi da quello in oggetto v. E. PELLINO, *Le tutele e il danno risarcibile*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pp. 597-598.

<sup>57</sup> Rileva come siffatte violazioni "sono costituite dalle attività di trattamento che vengono svolte in spregio allo statuto protettivo dell'interessato in questa materia, quindi in spregio al consenso o senza altra base idonea, ovvero in violazione dei principi posti per la legittimità del trattamento agli artt. 5 e 6, o dei diritti dell'interessato ex artt. 12 ss. e fino agli artt. 22 e 23 13. E sono costituite altresì dalle condotte poste in violazione della normativa sulla sicurezza dei dati nel senso più ampio del termine, e alla luce del principio dell'accountability", C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *juscivile*, 2020, 3, p. 793.

<sup>58</sup> Sul punto v., anche, M. RATTI, *La responsabilità da illecito trattamento dei dati personali*, cit., p. 777. In tal senso v., con riguardo all'ormai abrogato art. 15 del Codice dei dati personali, si vedano Cass., 8 gennaio 2019, n. 208; Cass., 25 gennaio 2017, n. 1931; Cass., 23 maggio 2016, n. 10638; Cass., 5 marzo 2015, n. 4443. Per l'opinione contraria v., però, E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno Resp.*, 2020, pp. 435-436.

<sup>59</sup> E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, p. 34.

<sup>60</sup> G.M. RICCIO, *Art. 82 - Diritto al risarcimento e responsabilità*, cit., p. 600; E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., p. 438.

<sup>61</sup> C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *juscivile*, 2020, 3, p. 797.

### 3. Il private enforcement nell'ambito di controversie di carattere transnazionale: la questione della giurisdizione

Considerata la natura globale di Internet e l'immediatezza dei flussi informativi sulla Rete, è tutt'altro che inverosimile che azioni inibitorie e/o risarcitorie promosse da privati nei confronti di titolari (o responsabili) del trattamento riguardino rapporti o situazioni di carattere transnazionale. Un elemento di estraneità della fattispecie, banalmente, sussiste nell'ipotesi in cui l'interessato, pregiudicato da un illecito trattamento dei propri dati personali, risieda in uno Stato diverso rispetto a quello di stabilimento del titolare (e/o del responsabile) del trattamento o nell'ipotesi in cui l'illecito trattamento sia posto in essere in uno Stato diverso rispetto a quello in cui l'evento-danno si concretizza.

Ciò premesso, ben si comprende quanto rilevante sia sul piano pratico la dimensione internazionalprivatistica della tutela dei dati personali; appare pertanto indispensabile fornire al lettore qualche spunto di riflessione circa il problema dell'individuazione del giudice internazionalmente competente e della legge applicabile con riguardo alle azioni di *private enforcement* del GDPR.

Per quanto concerne il profilo della giurisdizione, va sottolineato come l'ontologica dimensione "cross-border" della protezione dei dati personali sia stata tenuta in debita considerazione dal legislatore dell'Unione. Nell'ambito del regolamento, infatti, non solo è reperibile una disciplina sostanziale *ad hoc* in materia di trasferimento di dati personali all'estero<sup>62</sup>, ma è individuabile una disposizione preordinata a ripartire la giurisdizione tra i giudici degli Stati membri in relazione alle controversie scaturenti da azioni intentate ai sensi dei succitati artt. 79, par. 1 e art. 82.

L'art. 79, par. 2, segnatamente, prevede che le azioni nei confronti del titolare del trattamento o del responsabile del trattamento siano promosse "dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo

---

<sup>62</sup> Cfr. artt. 44-50. La disciplina dettata dal GDPR è chiaramente funzionale a far sì che, come auspicato dalla Corte di giustizia "la continuità del livello elevato di protezione delle libertà e dei diritti fondamentali riconosciuti dal diritto dell'Unione sia garantita in caso di trasferimento di dati personali dall'Unione a un paese terzo. Anche se le misure dirette ad assicurare un siffatto livello di protezione possono essere diverse da quelle attuate all'interno dell'Unione al fine di garantire il rispetto degli obblighi risultanti dal diritto dell'Unione, tali misure devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione" [Parere della Corte di giustizia 1/15 del 26 luglio 2017, *Accordo PNR UE-Canada*, EU:C:2017:592, punto 136; sentenza della Corte di giustizia del 6 ottobre 2015, Causa C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, EU:C:2015:650, punti da 72 a 74]. Per approfondimenti sul trasferimento dei dati personali all'estero nell'ambito del GDPR v. G. COLLINA, *Il GDPR in una prospettiva cross-border. Cenni all'applicazione del nuovo regolamento a tutela della privacy svizzera*, in P. BERTOLI, F. FERRARI, G. RIPAMONTI E G. TIBERI (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, cit., p. 128 ss.; M.C. MENEGHETTI, *I trasferimenti di dati personali all'estero*, in G. FINOCCHIARO (a cura di), *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 994 ss.; R. PANETTA, *Il trasferimento all'estero dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, cit., p. 357.

che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri<sup>63</sup>.

Il primo dato che emerge dalla lettura della disposizione in esame è che il regolamento distingue le controversie *inter privatorum* dalle controversie intentate nei confronti di autorità pubbliche sul fondamento dell'esercizio da parte di queste ultime di una potestà d'imperio. È evidente al riguardo la scelta di continuità rispetto all'orientamento tracciato dalla Corte di giustizia<sup>64</sup> – e da ultimo recepito nell'art. 1, par. 1, del regolamento n. 1215/2012 (cd. regolamento Bruxelles I bis)<sup>65</sup> – circa l'interpretazione da dare alla nozione di materia “civile e commerciale” ai fini dell'applicazione delle norme di diritto internazionale processuale di derivazione europea. Alla luce di tale allineamento, non sembra improprio sostenere che l'interprete, laddove utile, possa attingere all'abbondante giurisprudenza della Corte di giustizia in materia<sup>66</sup>.

<sup>63</sup> Si tratta di una norma unicamente preordinata a disciplinare il profilo della giurisdizione e che non incide sulla portata dei sistemi nazionali di riparto della competenza territoriale, posto che l'art. 82, par. 6, del GDPR chiarisce che “le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, par. 2”. Per un'articolata indagine sulla portata di tale norma e sulla sua interazione con gli strumenti internazionalprivatistici in vigore nello spazio giudiziario europeo v. 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. 448 ss.; O. FERACI, *Questioni internazionalprivatistiche in tema di azioni di risarcimento del danno proposte a seguito di violazioni del regolamento (UE) n. 2016/679 sulla protezione dei dati personali*, in P. BERTOLI, F. FERRARI, G. RIPAMONTI E G. TIBERI (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, cit., p. 167 ss.; P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, Antwerp, Portland, 2016, p. 81 ss.

<sup>64</sup> V. sentenza del 15 febbraio 2007, *Lechouritou e altri c. Rep. Fed. Germania*, Causa C-292/05, ECLI:EU:C:2007:102, punto 37; sentenza del 5 febbraio 2004, *Frabuil c. Assitalia*, ECLI:EU:C:2004:77, punto 21; sentenza del 15 maggio 2003, *Préservatrice foncière Tiard c. Stato olandese*, ECLI:EU:C:2003:282, punti 22-23; sentenza del 14 novembre 2002, *Gemeente Steenberghe c. Baten*, ECLI:EU:C:2002:656, punto 30; sentenza del 1° ottobre 2002, *Verein für Konsumenteninformation c. Henkel*, EU:C:2002:555, punto 26; sentenza del 16 dicembre 1980, *Stato olandese contro Ruffer*, ECLI:EU:C:1980:291, punto 8; sentenza del 14 ottobre 1976, *LTU c. Eurocontrol*, ECLI:EU:C:1976:137, punto 4.

<sup>65</sup> Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, *concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale*, in *GUUE* L 351 del 20 dicembre 2012, pp. 1–32. Per un'approfondita analisi del regolamento Bruxelles I bis, anche alla luce delle criticità evidenziate nella prassi applicativa v. S. M. CARBONE, C. E. TUO, *Il nuovo spazio giudiziario europeo in materia civile e commerciale: il regolamento UE n. 1215/2012*, Torino, 2016; F. FERRARI, F. RAGNO, *The Brussels I Recast Regulation as a panacea?*, Padova, 2015; A. LEANDRO, *Prime osservazioni sul regolamento (UE) n. 1215/2012 (“Bruxelles I bis”)*, in *Giusto proc. civ.*, 2013, p. 583 ss.; A. MALATESTA (a cura di), *La riforma del regolamento di Bruxelles I. Il regolamento (UE) n. 1215/2012 sulla giurisdizione e l'efficacia delle decisioni in materia civile e commerciale*, Milano, 2016; F. SALERNO, *Giurisdizione ed efficacia delle decisioni straniere nel Regolamento (UE) n. 1215/2012 (Rifusione). Evoluzione e continuità del «sistema Bruxelles-I» nel quadro della cooperazione giudiziaria in materia civile*, Padova, 2015; C. SILVESTRI, *Recasting Brussels I: il nuovo regolamento n. 1215 del 2012*, in *Riv. trim. dir. proc. civ.*, 2013, p. 677 ss.; F.C. VILLATA, *Rapporto sull'applicazione in Italia del Regolamento (CE) n. 44/2001 del 22 dicembre 2000 (e Bruxelles I) e del Regolamento (UE) n. 1215/2012 del 12 dicembre 2012 (Bruxelles I bis), concernenti la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale*, in S. BARIATTI, I. VIARENGO, F.C. VILLATA (a cura di), *La giurisprudenza italiana sui regolamenti europei in materia civile e commerciale e di famiglia*, Padova, 2016, p. 3 ss.

<sup>66</sup> Si vedano, di recente, sentenza del 17 maggio 2020, *LG c. Rina SpA e Ente Registro Italiano Navale*, ECLI:EU:C:2020:349; sentenza del 5 dicembre 2019, *Ordre des avocats du barreau de Dinant c. JN*, ECLI:EU:C:2019:1053; sentenza del 28 febbraio 2019, *BUAK Bauarbeiter-*

Il secondo dato, cruciale in una prospettiva di *private enforcement* del GDPR, riguarda la posizione di evidente *favor* riconosciuta a chi assume l'iniziativa giudiziaria per far valere una violazione del regolamento. Allorché la pretesa azionata nei confronti del titolare del trattamento o del responsabile del trattamento abbia natura privatistica, l'attore può infatti decidere, a propria discrezione, di incardinare la lite nello Stato membro in cui il convenuto ha uno stabilimento *oppure* nello Stato membro della sua residenza abituale.

Se si considera che vi è convergenza sul fatto che la nozione di stabilimento vada interpretata in senso ampio<sup>67</sup> – tenendo conto dell'indirizzo tracciato dalla Corte di giustizia al fine di definire l'ambito di applicazione della disciplina europea sulla protezione dei dati personali<sup>68</sup> e valorizzando il disposto dell'art. 27 che richiede ai titolari (o ai responsabili) di Stati terzi soggetti al GDPR di designare un proprio rappresentante all'interno dell'Unione in relazione agli obblighi su essi gravanti<sup>69</sup> –, se ne desume che il *forum rei*, così come configurato dall'art. 79, par. 2, non sia tanto concepito per consentire un effettivo contemperamento dell'esigenza della difesa della parte convenuta con quella dell'efficienza della potestà giurisdizionale<sup>70</sup>, ma sembri più che altro funzionale a dilatare il più possibile la sfera di giurisdizione degli Stati membri in un'ottica di tutela del *data subject*.

L'approccio protezionistico del legislatore dell'Unione è ancor più evidente se si considera che il *forum actoris* introdotto nella norma in esame sembrerebbe, in conformità alla lettura che viene data al foro del consumatore, così come delineato dall'art. 18 del regolamento Bruxelles I bis<sup>71</sup>, 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<sup>72</sup>.

La norma in esame, valorizzando titoli di giurisdizione uniformi che eludono l'annoso problema di adattare connessioni di carattere territoriale a uno spazio virtuale e non fisico qual è il web<sup>73</sup>, è evidentemente preordinata a garantire una tutela giurisdizionale effettiva

*Urlaubs- u. Abfertigungskasse c. Gradbeništvo Korana d.o.o.*, ECLI:EU:C:2019:16; sentenza del 9 marzo 2017, Causa C-551/15, *Pula Parking d.o.o. c. Sven Klaus Tederahn Pula Parking*, EU:C:2017:193; sentenza dell'11 aprile 2013, Causa C-645/11, *Land Berlin c. Ellen Mirjam Sapir e altri*, EU:C:2013:228.

<sup>67</sup> P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, cit., p. 100.

<sup>68</sup> P. DE MIGUEL ASENSIO, *Conflict of Laws and the Internet*, Cheltenham, 2020, p. 155.

<sup>69</sup> C. KOHLER, *Conflict of law issues in the 2016 Data protection regulation of the European Union*, cit., p. 668.

<sup>70</sup> Nel senso che tale contemperamento rappresenti la *ratio* del criterio del *forum rei*, v., nella giurisprudenza della Corte di giustizia, sentenza del 19 febbraio 2002, Causa C-256/00, *Besix c. Wasserreinigungsbau Alfred Kretzschmar GmbH & Co. KG (WABAG) e Planungs- und Forschungsgesellschaft Dipl. Ing. W. Kretzschmar GmbH & Co. KG (Plafog)*, punto 52; Corte di Giust., sentenza del 13 luglio 2000, C-412/98, *Group Josi Reinsurance Company SA c. Universal General Insurance Company (UGIC)*, ECLI:EU:C:2000:399, punti 34 e 35.

<sup>71</sup> Al riguardo sia consentito rinviare a F. RAGNO, *Il foro del consumatore: dalla Convenzione di Bruxelles del 1968 al Regolamento (CE) n. 44/01*, in *Contratto e impresa/Europa*, 2009, p. 235.

<sup>72</sup> Diverso è il discorso qualora l'attore muti la propria residenza abituale successivamente all'inizio del processo; in virtù del principio della *perpetuatio fori* la competenza giurisdizionale del giudice adito, in un siffatto scenario, non verrebbe minimamente intaccata.

<sup>73</sup> Questo problema è emerso in particolare allorché i giudici sono stati chiamati ad accertare il luogo dell'evento dannoso in relazione ad un illecito perpetrato a mezzo Internet; al riguardo v. la fondamentale sentenza della Corte di giustizia del 25 ottobre 2011, Cause riunite C-509/09 e C-161/10, *eDate Advertising GmbH e a. c. X e Société MGN LIMITED*, ECLI:EU:C:2011:685. In generale, sulle sfide che Internet pone al diritto internazionale privato v. U. DRAETTA, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2005, p. 207 ss.; G. IORIO FIORELLI, *Il contratto elettronico tra armonizzazione materiale e diritto internazionale privato*, Padova, 2006, p. 134 ss.; S. SAVINI, *Delocalizzazione del contratto stipulato su Internet. Problemi di giurisdizione e legge applicabile*,

del diritto fondamentale alla protezione dei dati personali<sup>74</sup>; va tuttavia osservato che, ai sensi del combinato disposto delle norme di cui al capo VIII del GDPR, essa è suscettibile di operare a prescindere dal fatto che l'iniziativa giudiziaria sia assunta dall'interessato o da altri soggetti. Anche laddove si nutrissero dubbi sulla possibilità che il diritto al risarcimento di cui all'art. 82 possa essere invocato da terzi danneggiati<sup>75</sup>, va ricordato, infatti, che l'art. 80, par. 1 e 2, del GDPR prevede espressamente che azioni di *private enforcement* possano essere promosse “da un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali” su mandato degli interessati<sup>76</sup> o – laddove il diritto nazionale lo preveda – anche in assenza di tale mandato<sup>77</sup>. Se ne desume che la scelta del legislatore dell'Unione sia stata quella di estendere il privilegio del foro anche all'ipotesi di ricorsi o azioni di carattere collettivo, in totale contrapposizione rispetto alla logica sottesa alla decisione della Corte di giustizia nel caso *Schrems* contro *Facebook*.<sup>78</sup>

Lo sbilanciamento tra le posizioni giuridiche dell'attore e del convenuto appare eccessivamente accentuato<sup>79</sup>, soprattutto se si considera che lo scarno regime giurisdizionale tracciato dal GDPR è in grado di fagocitare i titoli di giurisdizione del regolamento Bruxelles

---

in *Contr. impr. Eur.*, 2002, p. 1149 ss.; A. ZANOBETTI, *Contract law in international electronic commerce*, in *International Business Law Journal*, 2000, p. 545 ss.

<sup>74</sup> P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, cit., p. 85.

<sup>75</sup> V. *supra*.

<sup>76</sup> Si noti che per quanto concerne le azioni risarcitorie ex art. 82 del GDPR l'art. 80 subordina il meccanismo di rappresentanza dell'interessato alla condizione che detto meccanismo sia previsto dagli ordinamenti nazionali. Per quanto riguarda il diritto italiano, l'art. 10 del d.lgs. 1° settembre 2011, n. 150, come modificato dall'art. 17 del d.lgs. 10 agosto 2018, n. 101, prevede che, ai fini delle azioni esperibili ai sensi degli artt. 78, 79 e 82 del GDPR, “l'interessato possa dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n.117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile”.

<sup>77</sup> Si osservi, comunque, che l'art. 80, par. 2 esclude tale possibilità con riguardo alle azioni risarcitorie.

<sup>78</sup> Cfr. sentenza del 25 gennaio 2018, Causa C-498/16, *Maximilian Schrems c. Facebook Ireland Limited*, ECLI:EU:C:2018:37. In tale sentenza, come noto, la Corte di giustizia aveva ritenuto che i criteri imperativi di giurisdizione a tutela dei consumatori non potessero essere invocati da chi agisce non per far valere diritti propri, ma diritti ceduti da altri consumatori. Come segnalato dall'avvocato generale nelle conclusioni rese nell'ambito di tale procedimento (Conclusioni dell'Avvocato Generale Michal Bobek presentate il 14 novembre 2017, ECLI:EU:C:2017:863), una diversa soluzione “permetterebbe una concentrazione delle domande e la possibilità di scegliere, per le azioni collettive, il luogo in cui si trovano i giudici più favorevoli, cedendo tutti i diritti a un consumatore domiciliato in tale giurisdizione. Come osserva la resistente, siffatta soluzione potrebbe determinare una cessione mirata senza limiti ai consumatori in una giurisdizione che offra una giurisprudenza più favorevole, costi più contenuti o contributi alle spese giudiziali più generosi generando un sovraccarico di lavoro dei suddetti giudici”.

<sup>79</sup> Per l'idea secondo cui l'art. 79, par. 2 rischia di “pregiudicare eccessivamente, a favore del soggetto che si pretenda leso, la parità delle armi tra i litiganti, che è parte integrante del diritto all'equo processo tutelato dall'art. 6, par. 1, della Convenzione europea dei diritti dell'uomo e, trattandosi dell'applicazione, nell'un caso come nell'altro, di un atto dell'Unione europea, dall'art. 47 della Carta dei diritti fondamentali” v. 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”*, cit., p. 456.

I *bis* fondati sul principio di prossimità<sup>80</sup> e di prevedibilità del foro competente<sup>81</sup>. Come si evince dal considerando n. 147<sup>82</sup>, invero, i criteri di giurisdizione di cui alla normativa “generale” (regolamento Bruxelles I bis) possono rilevare solo nella misura in cui non pregiudicano l’applicazione della disciplina “speciale” (GDPR). Se ne ricava che nell’ipotesi di concorso tra i predetti strumenti, le uniche norme del regolamento Bruxelles I *bis* che possono trovare applicazione – *a latere* dell’art. 79, par. 2 – paiono essere<sup>83</sup> quelle che disciplinano la connessione attributiva (art. 8, par. 1), l’accettazione della giurisdizione (art. 26) ed eventualmente la scelta del foro (art. 25), ma solo nella misura in cui il foro prorogato dalle parti rappresenti un foro ulteriore attivabile per scelta attorea<sup>84</sup>.

L’altro grande limite della disciplina della giurisdizione di cui al GDPR è rinvenibile nella sua lacunosità; l’art. 79, par. 2 nulla dispone allorché sia il titolare dei dati ad essere convenuto dal titolare (o dal responsabile) del trattamento.

Al di là dell’osservazione per cui la protezione di un soggetto considerato ontologicamente debole, sul piano giurisdizionale, non può esclusivamente risolversi nell’attribuirgli facoltà di scelta rispetto ai fori attivabili, ma deve necessariamente tradursi in meccanismi di garanzia anche sul lato passivo, va evidenziato come la miopia del GDPR sia suscettibile di creare conseguenze assai perniciose rispetto alle finalità di tutela giurisdizionale effettiva perseguite. Si pensi all’ipotesi in cui sia il titolare del trattamento a convenire l’interessato (domiciliato in uno Stato membro) con un’azione di accertamento negativo volta a far valere la propria irresponsabilità alla luce del fatto che il trattamento posto in essere fosse necessario ad adempiere un obbligo legale al primo ascrivibile (art. 6, par. 1, lett. c). Visto che tale azione esula dal campo di applicazione del GDPR, la fonte normativa rilevante dovrebbe essere individuata nel regolamento Bruxelles I *bis*<sup>85</sup>. Ebbene, poiché, secondo

<sup>80</sup> Quali, ad esempio, il foro dell’illecito (sentenza della Corte di giustizia del 21 maggio 2015, Causa C-352/13, *Cartel Damage Claims (CDC) Hydrogen Peroxide SA c. Akzo Nobel NV*, EU:C:2015:335, punto 40; sentenza del 10 settembre 2015, Causa C-47/14, *Holterman Ferbo Exploitatie BV e a. c. F.L.F. Spies von Büllersheim*, EU:C:2015:574, punto 74) o il foro del contratto (Corte di giustizia, sentenza del 17 ottobre 2017, Causa C-194/16, *Bolagsupplysningen OÜ e Ingrid Ilsjan c. Svensk Handel ABBolagsupplysningen e Ilsjan*, EU:2017:766, punto 26; sentenza del 20 febbraio 1997, Causa C-106/95, *Mainschiffahrts-Genossenschaft eG (MSG) c. Les Gravières Rhénanes SARL*, EU:C:1997:70, punto 29; sentenza del 6 ottobre 1976, Causa 12/76, *Industrie Tessili Italiana Como c. Dunlop AG*, EU:C:1976:133, punto 13).

<sup>81</sup> Come sottolineato dalla Corte di giustizia, il regolamento Bruxelles I *bis* persegue “un obiettivo di certezza del diritto consistente nel rafforzare la tutela giuridica delle persone stabilite nell’Unione europea, consentendo al contempo al ricorrente di individuare agevolmente il giudice al quale può rivolgersi e al convenuto di prevedere ragionevolmente quello dinanzi al quale può essere citato” (Corte di giustizia, sentenza del 14 luglio 2016, Causa C-196/15, *Granarolo SpA c. Ambrosi Emmi France SA*, ECLI:EU:C:2016:559, para. 16; nonché sentenza del 23 aprile 2009, Causa C-533/07, *Falco Privatstiftung e Thomas Rabitsch c. Gisela Weller-Lindhorst*, EU:C:2009:257, punti 21 e 22). In dottrina v. P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, cit., p. 87.

<sup>82</sup> Tale considerando appare speculare all’art. 67 del regolamento Bruxelles I bis, che afferma il carattere cedevole delle proprie norme a fronte di normative speciali: “(i)l presente regolamento non pregiudica l’applicazione delle disposizioni che, in materie particolari, disciplinano la competenza, il riconoscimento e l’esecuzione delle decisioni e che sono contenute negli atti dell’Unione o nelle legislazioni nazionali armonizzate in esecuzione di tali atti”.

<sup>83</sup> 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”*, cit., pp. 451-452.

<sup>84</sup> P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, cit., p. 108.

<sup>85</sup> 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”*, cit., p. 451.

L'orientamento dalla Corte di giustizia, il presunto danneggiante può avvalersi del criterio del *forum delicti* nell'intentare un'azione di accertamento negativo volta a far dichiarare l'assenza di responsabilità da illecito civile doloso o colposo<sup>86</sup>, la lite potrebbe essere intentata, a discrezione dell'attore, nel luogo ove sono state sofferte le conseguenze pregiudizievoli dell'illecito (e quindi, verosimilmente, nel caso di illeciti perpetrati a mezzo Internet, nel luogo in cui l'interessato ha il proprio centro interessi<sup>87</sup>) ovvero nel luogo dell'evento generatore del danno (ovvero nel luogo del trattamento)<sup>88</sup>. Ne consegue che qualora il trattamento sia stato effettuato nello Stato membro in cui il titolare è stabilito, la giurisdizione potrebbe legittimamente incardinarsi in uno Stato diverso da quello in cui l'interessato ha la propria residenza abituale (o il proprio centro di interessi principale).

La possibile frustrazione degli obiettivi di tutela perseguiti dal regolamento appare ancor più macroscopica se si pensa che, indipendentemente dal fatto che trovi applicazione il GDPR (art. 81) o il regolamento Bruxelles I bis (art. 29)<sup>89</sup>, il criterio della prevenzione temporale valorizzato al fine di risolvere il problema della litispendenza potrebbe incentivare

---

<sup>86</sup> Sentenza del 25 ottobre 2012, Causa C-133/11, *Folien Fischer AG e Fofitec AG c. Ritrama SpA*, ECLI:EU:C:2012:664, punto 42 ss.: “la particolarità di un'azione di accertamento negativo si fonda sul fatto che l'attore chiede di accertare l'assenza dei presupposti della responsabilità da cui risulterebbe il diritto al risarcimento a favore del convenuto. Ciò premesso, come rilevato dall'avvocato generale al paragrafo 46 delle sue conclusioni, un'azione di accertamento negativo implica quindi un'inversione dei ruoli abitualmente conosciuti in materia di illeciti civili, in quanto l'attore è il debitore potenziale di un'obbligazione fondata su un illecito, mentre il convenuto è la pretesa vittima di tale atto. Tuttavia, tale inversione dei ruoli non è tale da escludere l'azione di accertamento negativo dalla sfera di applicazione dell'articolo 5, punto 3, del regolamento n. 44/2001. Infatti, gli obiettivi di prevedibilità del foro e di certezza del diritto, perseguiti da tale disposizione e reiteratamente ricordati dalla giurisprudenza (...), non attengono né all'attribuzione dei rispettivi ruoli di attore e convenuto né alla tutela dell'uno o dell'altro. Più in particolare, l'articolo 5, punto 3, del regolamento n. 44/2001 non persegue lo stesso obiettivo delle norme di competenza di cui alle sezioni 3-5 del capo II del regolamento medesimo, volte ad offrire tutela rafforzata alla parte più debole (...)”.

<sup>87</sup> V. sentenza del 25 ottobre 2011, Cause riunite C-509/09 e C-161/10, *eDate Advertising*, cit., punti 48-50: “la vittima di una lesione di un diritto della personalità per mezzo di Internet può adire un foro, a seconda del luogo di concretizzazione del danno cagionato da detta lesione nell'Unione europea, per la totalità di tale danno. Poiché l'impatto, sui diritti della personalità di un soggetto, di un'informazione messa in rete può essere valutata meglio dal giudice del luogo in cui la presunta vittima possiede il proprio centro di interessi, l'attribuzione di competenza a tale giudice corrisponde all'obiettivo di una buona amministrazione della giustizia (...) Il luogo in cui una persona ha il proprio centro di interessi corrisponde, in via generale, alla sua residenza abituale. Tuttavia, una persona può avere il proprio centro di interessi anche in uno Stato membro in cui non risiede abitualmente, ove altri indizi, quali l'esercizio di un'attività professionale, possano dimostrare l'esistenza di un collegamento particolarmente stretto con tale Stato”.

<sup>88</sup> Ciò in quanto la Corte di giustizia, in sede di esegesi del *forum delicti* in relazioni a illeciti caratterizzati da una dissociazione temporale tra il momento della condotta illecita e il momento dell'evento dannoso ha aderito alla cd. teoria dell'ubiquità, conferendo all'attore la possibilità di proporre la domanda dinanzi al giudice del “luogo della realizzazione del danno” oppure dinanzi al giudice “del fatto generatore che è all'origine del danno”: v. sentenza del 16 giugno 2016, Causa C-12/15, *Universal Music International Holding BV c. Michael Tétéreault Schilling*, punto 28; sentenza del 10 settembre 2015, Causa C-47/14, *Holterman Ferbo Exploitatie BV e a. c. F.L.F. Spies von Büllersheim*, EU:C:2015:574, punto 72; sentenza del 5 giugno 2014, Causa C-360/12, *Coty Germany GmbH c. First Note Perfumes*, EU:C:2014:1318, punto 46; sentenza del 7 marzo 1995, Causa C-68/93, *Fiona Shevill e altri c. Presse Alliance SA*, ECLI:EU:C:1995:61; sentenza del 30 novembre 1976, Causa 21/76, *Handelskvekerij G. J. Bier BV c. Mimes de potasse d'Alsace SA*, EU:C:1976:166, punti 24 e 25.

<sup>89</sup> Sulla questione v. 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”*, cit., p. 458 ss.

i titolari (o responsabili) del trattamento a “precipitarsi ad instaurare la lite per evitare che l'avversario la instauri davanti ad altro giudice a lui più vicino” (cd. *forum running*)<sup>90</sup>.

#### 4. *Il private enforcement nell'ambito di controversie di carattere transnazionale: la questione della legge applicabile*

Una volta affermata la propria giurisdizione sulla base delle norme ora richiamate, l'autorità giurisdizionale – adita ex artt. 79, par. 2 e 82 del GDPR, – sarà chiamata a individuare la legge applicabile alla fattispecie dedotta in giudizio. Ebbene, se è vero che la disciplina sostanziale uniforme delineata nel GDPR potrebbe, in linea teorica, rendere superfluo il ricorso al diritto internazionale privato in virtù del fondamentale principio per cui “*ohne Rechtskollision kein Kollisionsrecht*”<sup>91</sup>, è altrettanto evidente che il sistema regolatorio tracciato dal regolamento non è auto-sufficiente, ma necessita in più punti di un'integrazione da parte delle legislazioni nazionali<sup>92</sup>.

Tale aspetto è particolarmente evidente se si considera la responsabilità risarcitoria di cui all'art. 82. Sebbene il regime delineato dalla norma abbia una valenza centrale nel sistema di *private enforcement* del GDPR<sup>93</sup>, esso è ben lungi dall'aver carattere esaustivo. Nulla è detto, ad esempio, circa i termini di prescrizione<sup>94</sup> o circa la latitudine del danno risarcibile<sup>95</sup>.

L'esistenza di lacune da riempire attraverso le normative nazionali impone all'interprete di svolgere un ragionamento internazionalprivatistico che non può che muovere dal problema della qualificazione della fattispecie in esame. Invero, la dottrina civilistica si è diffusamente interrogata sulla natura contrattuale o extracontrattuale della responsabilità in oggetto, proponendo dotte e affascinanti ricostruzioni dogmatiche<sup>96</sup>. Ai nostri fini, tuttavia,

---

<sup>90</sup> Per la richiamata definizione del *forum running* v. G. BROGGINI, *La Convenzione di Lugano: introduzione e interpretazione; la competenza giurisdizionale*, in *Studi di diritto internazionale privato e comunitario*, Napoli, 2007, Tomo II, p. 763. Per osservazioni simili v. N. BOSCHIERO, *Forum destinatae solutionis e norme materiali uniformi sulla vendita internazionale*, in A.E. VON OVERBACK, F. POCAR, K. SIEHR (a cura di), *Collisio Legum. Studi di diritto internazionale privato per Gerardo Broggin*, Milano, 1997, pp. 70-71.

<sup>91</sup> K. ZWEIGERT, U. DROBNIG, *Einheitliches Kaufgesetz und internationales Privatrecht*, in *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 1965, p. 147.

<sup>92</sup> Sulla valenza del diritto internazionale privato nel contesto degli strumenti di diritto sostanziale uniforme v., per tutti, F. FERRARI, *CISG and Private International Law*, in F. FERRARI (a cura di), *The 1980 Uniform Sales Law. Old Issues Revisited in the Light of Recent Experiences*, Milano/Monaco di Baviera, 2003, p. 19 ss.

<sup>93</sup> P. DE MIGUEL ASENSIO, *Conflict of Laws and the Internet*, cit., p. 152.

<sup>94</sup> Sottolinea come il diritto internazionale europeo propenda per una qualificazione della prescrizione in senso sostanziale, in ciò distinguendosi dall'approccio seguito nei Paesi di *common law*, F. MARONGIU BUONAIUTI, *Le obbligazioni con contrattuali nel diritto internazionale privato*, Milano, 2013, p. 95.

<sup>95</sup> In questo senso v. F. BRAVO, *Riflessioni critiche sulla natura della responsabilità del trattamento illecito dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, Milano, 2019, p. 391; P. FRANZINA, *Jurisdiction Regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation*, cit., p. 98.

<sup>96</sup> V., ad esempio, F. BRAVO, *Riflessioni critiche sulla natura della responsabilità del trattamento illecito dei dati personali*, cit., p. 383 ss.

è necessario ricordare che la qualificazione<sup>97</sup> e – in via preliminare<sup>98</sup> – l’interpretazione delle nozioni e delle categorie contenute nelle norme di derivazione europea vanno condotte in chiave autonoma<sup>99</sup>, valorizzando il contesto sistematico in cui si collocano e gli orientamenti interpretativi della Corte di giustizia.

Rispetto alla questione *de qua*, segnatamente, non sembra possibile prescindere dal contributo che i giudici del Kirchberg hanno fornito, ancorché in relazione a profili di giurisdizione, nel ricostruire il *discrimen* tra materia contrattuale e materia non contrattuale. Come noto la Corte, in sede di esegesi della nozione di «materia contrattuale» di cui all’art. 7, punto 1, lettera a), del regolamento Bruxelles I bis (e delle previgenti norme) ha chiarito che essa presuppone la determinazione di un obbligo giuridico assunto liberamente da un soggetto nei confronti di un altro e su cui si fonda l’azione del ricorrente<sup>100</sup>. Conformemente a ciò la Corte ha ritenuto che laddove le pretese si fondino sull’inadempimento di un obbligo imposto dalla legge – senza alcuna possibilità di scelta o di deroga – esse non possano connotarsi come “contrattuali”<sup>101</sup>. In relazione ad un’azione aquiliana intentata contro una controparte contrattuale, la Corte ha altresì chiarito che la sussistenza di un vincolo negoziale tra le parti non implica affatto che la pretesa azionata possa essere ascritta – *ipso iure* – alla materia contrattuale<sup>102</sup>: perché ciò accada è necessario che il comportamento contestato possa essere considerato un inadempimento delle “obbligazioni contrattuali quali possono essere determinate tenuto conto dell’oggetto del contratto”. Secondo i giudici dell’Unione questa situazione ricorre “a priori se l’interpretazione del contratto che vincola il convenuto al ricorrente appare indispensabile per stabilire la liceità o, al contrario, l’illiceità del comportamento che il primo rimprovera al secondo”.

Vista la sinergia sussistente tra il regolamento Bruxelles I bis e i regolamenti dell’Unione (regolamento cd. Roma I<sup>103</sup> e regolamento cd. Roma II<sup>104</sup>) che hanno uniformato

<sup>97</sup> Cfr. R. BARATTA, *The Process of Characterization in the EC Conflict of Laws: Suggesting a Flexible Approach*, *Yearbook of Private International Law*, 2004, p. 155 ss.; S. BARIATTI, *Qualificazione e interpretazione nel diritto internazionale privato comunitario: prime riflessioni*, *Riv. dir. int. priv. proc.*, 2006, p. 361 ss.

<sup>98</sup> Sulla distinzione tra operazione di qualificazione della fattispecie e procedimento di interpretazione della norma giuridica v. A. MALATESTA, *La cessazione del credito nel diritto internazionale*, Padova, 1996, pp. 28-29.

<sup>99</sup> Sull’interpretazione autonoma delle norme di diritto internazionale privato come funzionale “non soltanto al conseguimento degli obiettivi sui quali si fondano le norme da applicare, ma anche alla tenuta e allo sviluppo della stessa integrazione europea” v. A. DI BLASE, *Sull’interpretazione delle convenzioni e delle norme dell’Unione europea in materia di diritto internazionale privato*, *Riv. dir. int. priv. proc.*, 2020, p. 8; in tema v., altresì, L. SANDRINI, *L’interpretazione del diritto internazionale privato dell’Unione europea*, Roma, 2018, p. 41. Sulla necessità di interpretare autonomamente i criteri di collegamento contenuti nelle norme di conflitto di derivazione europea v., nella giurisprudenza della Corte di giustizia, sentenza del 15 marzo 2011, causa C-29/10, *Heiko Koelzsch c. État du Grand-Duché de Luxembourg*, ECLI:EU:C:2011:151, punto 32.

<sup>100</sup> Sentenza dell’8 maggio 2019, Causa C-25/18, *Brian Andrew Kerr c. Pavlo Postnov e Natalia Postnova*, ECLI:EU:C:2019:376, punti 24-25; sentenza del 21 aprile 2016, Causa C-572/14, *Austro-Mechana Gesellschaft zur Wahrnehmung mechanisch-musikalischer Urheberrechte Gesellschaft mbH c. Amazon EU Sàrl e a.*, EU:C:2013:490, punto 36; sentenza del 14 marzo 2013, Causa C-419/11, *Česká spořitelna, a.s. c. Gerald Feichter*, EU:C:2013:165, punto 47. Per approfondimenti v., in dottrina, P. FRANZINA, *La giurisdizione in materia contrattuale. L’art. 5 n. 1 del regolamento n. 44/2001/CE nella prospettiva dell’armonia delle decisioni*, Padova, 2006, p. 177 ss.

<sup>101</sup> Corte di giustizia, sentenza del 5 dicembre 2019, Causa C-421/18, *Ordre des avocats*, cit., punto 32.

<sup>102</sup> Corte di giustizia, sentenza del 13 marzo 2014, Causa C-548/12, *Marc Brogitter c. Fabrication de Montres Normandes EURL e Karsten Fräjsdorf*, ECLI:EU:C:2014:148, punti 23-25.

<sup>103</sup> Regolamento (CE) n. 593/2008 del 17 giugno 2008, *sulla legge applicabile alle obbligazioni contrattuali (Roma I)*, in *GUUE* L 177 del 4 luglio 2008, pp. 6-16.

<sup>104</sup> Regolamento (CE) n. 864/2007 dell’11 luglio 2007, *sulla legge applicabile alle obbligazioni extracontrattuali (cd. regolamento “Roma II”)*, in *GUUE* L 199 del 31 luglio 2007, pp. 40-49.

le norme sui conflitti di legge in relazione alle obbligazioni contrattuali e non contrattuali<sup>105</sup>, il ricordato *acquis* giurisprudenziale dovrebbe indurre a ritenere che le pretese risarcitorie di cui all'art. 82 del GDPR gravitino nell'orbita extracontrattuale. Qualche dubbio, per la verità, potrebbe sorgere nell'ipotesi – non necessariamente frequente vista la perdita di centralità del consenso nel sistema regolatorio del GDPR<sup>106</sup> – in cui l'illiceità del trattamento fatta valere riposi sul mancato rispetto dei termini del consenso manifestato dall'interessato nell'ambito di un rapporto contrattuale; ad avviso di chi scrive, tuttavia, una qualificazione contrattuale dovrebbe essere esclusa alla luce della natura autorizzatoria e non negoziale del consenso<sup>107</sup>.

Posto il predetto inquadramento, sembrerebbe logico ricercare le norme di conflitto funzionali ai fini in esame nel regolamento Roma II. Ciò, tuttavia, presupporrebbe che detto strumento trovi applicazione alla fattispecie in esame, il che non è affatto scontato se si considera che le difficoltà di bilanciamento tra il diritto alla riservatezza e la libertà di informazione emerse nei lavori preparatori hanno portato a espungere dal campo di applicazione del regolamento Roma II (art. 1, par. 2, lett. g) “le obbligazioni extracontrattuali che derivano da violazioni della vita privata e dei diritti della personalità, compresa la diffamazione”. Invero, la dottrina è pressoché univoca nel ritenere che le obbligazioni risarcitorie scaturenti da una violazione del GDPR ricadano nella sfera di operatività dell'esclusione in esame<sup>108</sup>.

Tale granitica posizione, che evidentemente muove dal presupposto per cui il diritto alla tutela dei dati personali andrebbe ricondotto nel novero dei diritti della personalità<sup>109</sup>, non pare, per la verità, inoppugnabile. Si pensi al già menzionato caso in cui a invocare la tutela risarcitoria di cui all'art. 82 sia un concorrente che lamenti il fatto che la violazione del regolamento (in ipotesi trattamenti effettuati senza il previo consenso degli interessati e senza che ricorrano i presupposti di liceità di cui all'art. 6 del GDPR) abbia posto il titolare del trattamento in una posizione di vantaggio competitivo rispetto alla parte attrice, che si è invece attenuta rigorosamente agli obblighi di *compliance* imposti dal regolamento. L'esclusione di cui all'art. 1, par. 2, lett. g) del regolamento Roma II non sembrerebbe rilevare nel caso di specie. Nello scenario prospettato

<sup>105</sup> Tale sinergia è attestata dall'auspicio di coerenza espresso nel considerando n. 7 del regolamento Roma I [“(i) campo di applicazione materiale e le disposizioni del presente regolamento dovrebbero essere coerenti con il regolamento Bruxelles I e con il regolamento Roma II (Roma II)”] e del regolamento Roma II [“(i) campo d'applicazione materiale e le disposizioni del presente regolamento dovrebbero essere coerenti con il regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale («Bruxelles I»), e con gli strumenti relativi alla legge applicabile alle obbligazioni contrattuali]. In giurisprudenza v. Corte di giustizia, sentenza del 21 gennaio 2016, cause riunite C-359/14 e C-475/14, “ERGO Insurance” SE c. “If P&C Insurance” AS e “Gjensidige Baltic” AAS c. “PZU Lietuva” UAB DK, ECLI:EU:C:2016:40, punto 43. Sul punto, da ultimo, v. le Conclusioni dell'avvocato generale

<sup>106</sup> Sulla perdita di centralità del consenso nel GDPR e sulla sua riconducibilità ad una sorta di presa d'atto dell'inevitabilità del trattamento di dati personali che l'evoluzione tecnologica comporta v. G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e big data*, in E. TOSI (a cura di), *Privacy Digitale – Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, pp. 451-453. Sul tema v., anche, C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., p. 873 ss.

<sup>107</sup> Sulla questione v. la lucida analisi di F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali*, in *Il Nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 135 ss.

<sup>108</sup> P. DE MIGUEL ASENSIO, *Conflict of Laws and the Internet*, cit., p. 167; O. FERACI, *Questioni internazionalprivatistiche in tema di azioni di risarcimento del danno proposte a seguito di violazioni del regolamento (UE) n. 2016/679 sulla protezione dei dati personali*, cit., p. 185.

<sup>109</sup> Sul punto v. S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Eur. dir. priv.*, 2004, p. 2 ss.; G. ALPA, *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati – Riflessioni sul GDPR*, cit., p. 13 ss.

l'illecito trattamento dei dati personali non è fatto valere da un interessato che lamenti una lesione del proprio diritto fondamentale, ma assurge a mera questione preliminare rispetto a quella principale sollevata in giudizio<sup>110</sup>; poiché la questione della liceità del trattamento è esaustivamente disciplinata dal GDPR, nulla osta a che la disciplina sostanziale chiamata ad integrare il regime di responsabilità di cui all'art. 82 possa essere individuata ricorrendo al regolamento Roma II e, più precisamente, alla norma di conflitto che il regolamento detta in materia di concorrenza sleale<sup>111</sup>. Tale interpretazione pare suffragata dalla giurisprudenza della Corte di giustizia; nel noto caso *Konsumenteninformation* contro *Amazon*<sup>112</sup>, i giudici dell'Unione hanno ritenuto che la legge applicabile ad un'azione inibitoria promossa da un'associazione di tutela dei consumatori e diretta contro l'impiego di clausole contrattuali asseritamente abusive da parte di *Amazon* dovesse essere determinata in conformità all'art. 6, par. 1, del regolamento Roma II, a prescindere dal fatto che alcune tra le predette clausole si ponessero in evidente contrasto con la (prevalente) disciplina europea sul trattamento dei dati personali<sup>113</sup>. Così facendo la Corte si è allineata alle posizioni dell'avvocato generale che, nelle proprie conclusioni, aveva proposto per un'interpretazione autonoma della nozione di concorrenza sleale tale da far convogliare nell'alveo dell'art. 6, par. 1 del regolamento Roma II "qualsiasi atto idoneo ad alterare le relazioni tra i partecipanti su un mercato, tra concorrenti o nei confronti dei consumatori collettivamente"<sup>114</sup>.

##### 5. Osservazioni conclusive

L'ambivalenza dei dati personali, oggetto di un diritto fondamentale, da una parte, e bene giuridico economicamente valutabile e avente valenza strategica nel contesto dell'economia digitale, dall'altra, ha inevitabilmente condizionato le scelte del legislatore

---

<sup>110</sup> Sul controverso problema della legge applicabile alle questioni preliminari v., di recente, A. BONOMI, *Incidental (preliminary) question*, in J. BASEDOW, G. RÜHL, F. FERRARI, P. DE MIGUEL ASENSIO (a cura di), *Encyclopedia of Private International Law*, vol. I, Cheltenham/Northampton, 2017, p. 913 ss.; U. VILLANI, *La questione preliminare*, in U. VILLANI, M. DI FABIO, F. SBORDONE (a cura di), *Nozioni di diritto internazionale privato – Parte generale e obbligazioni*, Napoli, 2013, p. 40 ss.

<sup>111</sup> Ai sensi dell'art. 6, par. 1 e 2, del regolamento Roma II, "(l)a legge applicabile all'obbligazione extracontrattuale che deriva da un atto di concorrenza sleale è quella del Paese sul cui territorio sono pregiudicati, o rischiano di esserlo, i rapporti di concorrenza o gli interessi collettivi dei consumatori. Qualora un atto di concorrenza sleale leda esclusivamente gli interessi di un dato concorrente, si applica l'articolo 4".

<sup>112</sup> Sentenza del 28 luglio 2016, Causa C-191/15, *Verein für Konsumenteninformation c. Amazon EU Sàrl*, ECLI:EU:C:2016:612.

<sup>113</sup> V. anche, J. VON HEIN, A. BIZER, *Social Media and the Protection of Privacy: Current Gaps and Future Directions in European Private International Law*, in *International Journal of Data Science and Analytics*, 2018, p. 235: "The CJEU decided that the Rome II Regulation remained applicable to claims relating to unfair competition (article 6 Rome II) although privacy or personality rights are affected as an incidental question. Therefore, it can be stated that the already existing uniform regulations are interpreted in a sense to diminish the consequences of the incomplete scope of Rome II".

<sup>114</sup> V. Conclusioni dell'avvocato generale Henrik Saugmandsgaard Øe presentate il 2 giugno 2016, ECLI:EU:C:2016:388, punto 73. Sulla valenza dell'art. 6, par. 1, del regolamento Roma II rispetto a pratiche di un'impresa che configurano al contempo una violazione della normativa sui dati personali e atti di concorrenza sleale v., altresì, Bundesgerichtshof, sentenza del 14 gennaio 2016 - I ZR 65/14, reperibile al sito: <<http://juris.bundesgerichtshof.de>>, punto 21: nel caso di specie la Corte suprema federale tedesca aveva inibito *Facebook* dall'utilizzare una funzione (*Friends finder*) giudicata incompatibile con la già richiamata legge tedesca sulla concorrenza sleale e con la normativa europea di protezione dei dati personali.

dell'Unione allorché si è trovato a delineare il regime di *enforcement* del GDPR. Accanto a strumenti di tutela di carattere pubblicistico, hanno trovato ingresso rimedi e azioni di natura privatistica invocabili anche da soggetti diversi rispetto all'interessato e suscettibili di impiego anche in relazione a situazioni o rapporti transnazionali.

L'analisi ha messo in luce come il regolamento si sia rapportato alla dimensione *cross-border* del cd. *private enforcement* in modo essenzialmente ambiguo. Per quanto concerne il profilo della giurisdizione, si è privilegiata una posizione interventista (ancorché sfociata in una regolamentazione lacunosa); per quanto concerne il profilo della legge applicabile, di contro, si è mantenuto un atteggiamento di indifferenza (difficilmente spiegabile se si considerano i frequenti richiami al diritto nazionale rinvenibili nel contesto del regolamento).

Ad ogni buon conto, ciò che emerge con chiarezza dall'analisi del GDPR è che ai profili internazionalprivatistici non è stata dedicata particolare attenzione. La scarsa sensibilità manifestata dal legislatore dell'Unione appare criticabile non solo perché non tiene in debito conto che la natura globale di Internet, quale "meta-territorio" in cui i flussi informativi trascendono i confini nazionali, genera assai frequentemente situazioni che non si esauriscono all'interno di un unico ordinamento, ma soprattutto perché costringe l'interprete a operare un non sempre agevole raccordo tra fonti normative eterogenee e improntate a logiche profondamente diverse.