


## Applicable Law Concerning Obligations Arising from the Infringements of Personal Data Laws Due to the Use of Artificial Intelligence Systems


Marek Świerczyński

Dr. habil., Associate Professor, Institute of Legal Studies, the Cardinal Stefan Wyszyński University in Warsaw; correspondence address: ul. Wóycickiego 1/3, 01-938 Warszawa, b. 17, Poland; e-mail: [m.swierczynski@uksw.edu.pl](mailto:m.swierczynski@uksw.edu.pl)

 <https://orcid.org/0000-0002-4079-0487>

Zbigniew Więckowski

Dr., Assistant Professor, Institute of Legal Studies, the Cardinal Stefan Wyszyński University in Warsaw; correspondence address: ul. Wóycickiego 1/3, 01-938 Warszawa, b. 17, Poland; e-mail: [z.wieckowski@uksw.edu.pl](mailto:z.wieckowski@uksw.edu.pl)

 <https://orcid.org/0000-0001-7753-3743>

### Keywords:

AI, personal data,  
data protection law,  
conflict-of-laws

**Abstract:** An issue that is characteristic of AI is data processing on a massive scale (*giga data*, Big Data). This issue is also important because of the proposition to require manufacturers to equip AI systems with a means to record information about the operation of the technology, in particular the type and magnitude of the risk posed by the technology and any negative effects that logging may have on the rights of others. Data gathering must be carried out in accordance with the applicable laws, particularly data protection laws and trade secret protection laws. Therefore, it is necessary to determine the applicable law in line with existing conflict-of-law regulations.

### 1. Introductory remarks

The scope of application of the Rome II Regulation excludes ‘non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation’ (Article 1(2)(g)), so the issues of protection of privacy and infringements made using AI algorithms requires a separate

discussion<sup>1</sup>. There are also no corresponding provisions in the GDPR. That regulation contains only fragmentary provisions concerning international civil procedure (Article 79 et seq.)<sup>2</sup>. This results in a significant gap in the EU data protection regime<sup>3</sup>. Due to the increasingly widespread use of algorithms, AI requires urgent legislative intervention. To determine the proper law (a statute ancillary to the GDPR), courts must apply national legislation applicable to private international law<sup>4</sup>, which regulates privacy protection in different ways.

This issue is becoming increasingly practical as lawsuits for compensation or redress for a damage suffered are starting to be initiated. An example is the judgment of the Circuit Court in Warsaw of 6 August 2020, case file XXV C 2596/19. This was the first judgment in Poland that granted compensation for unlawful disclosure of personal data. It was also a precursor to further proceedings, which will necessarily also concern cases of automated processing of personal data<sup>5</sup>. Despite the complexity of the case, which involved not only the GDPR but also sector-specific regulations, the court correctly applied the personal data protection regulations and drew the right conclusions. The difficulty in properly adjudicating cases will be greater for cross-border disputes, due to the fact that the automated data processing

<sup>1</sup> See further: Marek Świerczyński, "Prawo właściwe dla zobowiązań deliktowych wynikających z naruszenia zasad ochrony danych osobowych przyjętych w RODO," *Problemy Prawa Prywatnego Międzynarodowego* 27 (2019): 39–59.

<sup>2</sup> Marek Świerczyński, "Jurysdykcja krajowa w świetle rozporządzenia ogólnego o ochronie danych osobowych," *Europejski Przegląd Sądowy* 12 (2016): 15–20.

<sup>3</sup> Cf.: Andrzej Calus, "Znaczenie rozporządzenia Rzym II dla unifikacji prawa właściwego dla czynów niedozwolonych w państwach członkowskich Unii Europejskiej," in *Czyny niedozwolone w prawie polskim i w prawie*, ed. Mirosław Nesterowicz (Warsaw: Wolters Kluwer: 2012), 110–145.

<sup>4</sup> Maja Brkan, "Data Protection and Conflict-of-Laws: A Challenging Relationship," *European Data Protection Law Review* 2, no. 3 (2016): 337.

<sup>5</sup> Cf.: Guido Noto La Diega, "Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 3 (2018): 11–16; Antoinette Royvroy, *Of Data and Men. Fundamental Rights and Freedoms in a World of Big Data. Report for the Bureau of the Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*, Council of Europe, TD-PD-BUR 2016, accessed February 7, 2023, <https://rm.coe.int/16806a6020>.

performed by AI algorithms is carried out by corporations domiciled in other countries<sup>6</sup>.

We believe it is essential that the adjudicating body in each case – regardless of the member state where it operates – apply the same law to assess the data subject's claims concerning AI infringements related to data processing<sup>7</sup>. The conflict-of-law mechanism adopted that protects privacy should ensure a balance between the parties. Solutions that provide excessive protection to only one party should be avoided<sup>8</sup>. An example of a solution that is flawed in our opinion is adoption as proper law of the law of the state where the injured party's habitual residence is located. Despite its simple application, this solution raises concerns about its neutrality and reasonableness in the event of an infringement of the personal data protection regime.

## 2. In search of the proper legal basis

According to Article 16(1) of the Polish Act on private international law adopted in 2011, an individual's personal rights are governed by the law of his or her country. That law determines the catalogue of personal rights and accompanying subjective rights, as well as their emergence, content, scope, and cessation. On the other hand, the proper law for the protection of personal rights must be identified by applying the provisions of Article 16(2 and 3). Pursuant to Article 16(2), an individual whose personal rights are threatened by an infringement or has been infringed may demand protection under the law of the country in the territory of which the event causing the threatened infringement or infringement took place, or the law

---

<sup>6</sup> E.g. in the context of profiling, see: Natalia Domagała, Bartłomiej Oręziak, Marek Świerczyński, "Profiling in the recruitment of subjects for clinical trials in the light of GDPR," *Zeszyty Prawnicze* 20, no. 2 (2020): 265–280; cf.: Dimitra Kamarinou, Christopher Millard, Jatinder Singh, "Machine Learning with Personal Data," Queen Mary School of Law Legal Studies Research Paper no. 247/2016: 1–23.

<sup>7</sup> Cf.: judgments of the Court of Justice of the European Union of 30 November 1976 in case 21/76, *Handelskwekerij G.J. Bier BV v. Mines de potasse d'Alsace SA*; of 7 March 1995 in case C-68/93, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA* and of 25 November 2011 in joined cases C509/09 *eDate Advertising GmbH v. X* and C161/10 *Olivier Martinez, Robert Martinez v. MGN Limited*.

<sup>8</sup> Ornella Feraci, «La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria,» *Rivista di diritto internazionale*, no. 4 (2009): 1020–1085.

of the country in the territory of which the consequences of the infringement occurred. Thus, proper law can be indicated according to one of two options<sup>9</sup>. If an infringement on the GDPR principles is classified as a violation of personal rights (privacy), the data subject may make this indication, which increases the risk of manipulation of the proper law.

However, it is not clear whether the above provisions will or should apply to infringements of the data protection regime established in the GDPR. Before applying the provisions in question, it is first necessary to make a conflict-of-law classification of GDPR infringements. It is well known that the GDPR is separate from regulations aimed to protect personal rights<sup>10</sup>. This is highlighted by the creation of separate grounds for claims by data subjects, both in the text of the GDPR and under the new Polish Act on personal data protection of 2018<sup>11</sup>. This leads to the question of whether the conflict-of-law rules set forth in the Rome II Regulation should be applied to determine the applicable law<sup>12</sup>.

<sup>9</sup> Cf.: Justyna Balcarczyk, "Wybrane problemy związane z projektem ustawy – Prawo prywatne międzynarodowe," *Rejent*, no. 7–8 (2009): 140.

<sup>10</sup> Cf.: Joanna Braciak, *Prawo do prywatności* (Warsaw: Wydawnictwo Sejmowe, 2004), 92.

<sup>11</sup> Journal of Laws of 2018, item 1000, consolidated text: Journal of Laws of 2019, item 1781.

<sup>12</sup> The Rome II Regulation is the subject of many publications. A majority of them express critical opinions about the exclusion of torts related to privacy from the scope of the Regulation. In particular, see: Andrew Dickinson, *The Rome II Regulation* (Oxford: Oxford University Press, 2010), 1–1076; Richard Plender, Michael Wilderspin, *European Private International Law of Obligation* (London: Sweet & Maxwell, 2020), 1–854; John Ahern, William Binchy, *Rome II Regulation on Law Applicable to Non-Contractual Obligations* (Leiden: Brill, 2009), 1–477; James Fawcett, Janeen Carruthers, Peter North, *Private International Law* (Oxford: Oxford University Press, 2017), Part IV:20; Galf-Peter Calliess, ed., *Rome Regulations: Commentary on the European Rules of the Conflict of law. Part Two*, [b.m.] (2011), 358–654; *Rome II Regulation*, ed. Peter Huber, (Munich, 2011); Adam Rushworth, Andrew Scott, "Rome II: Choice of law for non-contractual obligations," *LMCLQ* (2008): 274–306; Trevor Hartley, "Choice of Law for Non-Contractual Liability: Selected Problems under the Rome II Regulation," *ICLQ* 57, (2008): 899–908; Carine Briere, "Le règlement (CE) no 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II)," *Journal de droit international* 135 (2008): 31; Stefan Leible, Matthias Lechmann, "Die neue EG-Verordnung über außervertragliche Schuldverhältnisse anzuwendende Recht (Rom II)," *Recht der Internationalen Wirtschaft* 53, (2007): 721; Thomas Graziano, Das auf außervertragliche Schuldverhältnisse anzuwendende Recht nach Inkrafttreten der Rom II – Verordnung, *RabelsZ* 73, (2009): 1–177; Tim Dornis, "When in Rome, do as the Romans do? – a defense of the lex domicilii communis: in the Rome II Regulation," *European Legal*

This solution has significant advantages, which arise from the modern, balanced, and flexible rules of the determination of the proper law adopted in the Rome II Regulation. A key argument is the possibility of convergent interpretation of the criteria adopted for the application of the GDPR (Article 3) and the general connecting factors of the conflict-of-law norms of the Rome II Regulations, which is crucial in the case of AI infringements.

### 3. The provisions of the GDPR

It must be emphasised that the GDPR does not lead to the exclusion of the application of the existing provisions of private international law (conflict-of-law rules). The fact that the EU legislator tried to define the scope of application of the GDPR as precisely as possible (in some places even casuistically) does not mean that this regulation constitutes a complete legal system. It is not a complete (exhaustive) regulation or a substitute for national legal systems in terms of civil-law consequences of infringements of personal data protection principles. A supporting statute (domestic law) is required to resolve specific issues. An example is the rules for granting compensation (redress) to a person whose rights and freedoms have been violated due to an unauthorised processing of his or her personal data. However, applying the conflict-of-law rules in isolation from the applicability criteria adopted in the GDPR undermines the international effectiveness and protective nature of this regulation. Failure to adequately clarify the relationship of these provisions leads to differences in case law. For example, courts of one country may apply their domestic law, justifying it by the provisions of the GDPR, while courts of another country apply their own domestic law, justifying it by the provisions of private international law.

There should be no doubt that the basis for determining the proper law is not the provisions of Article 82(6) of the GDPR. The article indicates that court proceedings concerning compensation shall be brought before the court having jurisdiction under the domestic law of the member

---

*Forum* 4 (2007): 152–159; Symeon Symeonides, “Rome II and Tort Conflicts: A Missed Opportunity,” *AJCL* 56, no. 1 (2008): 173–222; Phaedon Kozyris, “Rome II: Tort Conflicts on the Right Track! A Postscript to Symeon Symeonides’ Missed Opportunity,” *AJCL* 56 (2008): 471–497; Janeen Carruthers, Elizabeth Crawford, “Variations on a theme of Rome II. Reflections on proposed choice of law rules for non-contractual obligations: Part I,” *Edinburgh Law Review* 9 (2005): 65–97; Part II, *Edinburgh Law Review* 9 (2005): 238–266.

state referred to in Article 79(2) of the GDPR. Despite its ambiguous wording, this provision does not constitute a conflict-of-law rule that determines the proper law for compensation for unlawful processing of personal data, but instead it merely extends the jurisdictional rules set forth in Article 79(2) (concerning legal remedies) to include actions for compensation.

The provisions of the GDPR with respect to civil-law aspects of privacy protection are rudimentary (an example is Article 82 of the GDPR, which provides a direct basis for pursuing tort claims<sup>13</sup>). When assessing a case from the standpoint of Polish conflict-of-law rules, it must be noted that the provisions of the GDPR are predominantly public-law provisions. Their primary purpose is to impose certain public-law obligations on the data controller and the entity processing data on its behalf (data processor). In order to effectively achieve this objective, the EU legislator sought to clearly define the scope of application of the GDPR<sup>14</sup>. Most personal data of individuals residing in the EU is processed outside of the EU, but the laws of third countries do not provide protection that is in line with the GDPR<sup>15</sup>.

Article 3 of the GDPR shows that three main connecting factors (criteria) are used to determine the scope of application of the GDPR: 1) existence of an organisational unit within the EU; 2) offering goods and services within the EU to persons residing within the EU; and 3) monitoring their behaviour. These criteria also serve to determine the scope of application of national laws that supplement the GDPR<sup>16</sup>, including the Polish Act on personal data protection of 10 May 2018. Correct interpretation of the above criteria is facilitated by the existing case law of the CJEU on the protection of data subject.<sup>17</sup>

<sup>13</sup> More information can be found in: Paweł Litwiński, commentar

<sup>14</sup> Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Cham: Springer, 2017), 22.

<sup>15</sup> Gérard Haas, *La réglementation sur la protection des données personnelles* (St Herblain: Éditions ENI, 2018), 20.

<sup>16</sup> More information can be found in: Heinrich Wolff; Stefan Brink, ed., *Beck'scher Online-Kommentar Datenschutzrecht*, (Munich: C.H. Beck, 2017), Rn. 1–46.

<sup>17</sup> Michał Czerniawski, “Zakres terytorialny a pojęcie ‘jednostki organizacyjnej’ w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu,” in *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, ed. Grzegorz Sibiga (Warsaw 2016), 22–23.

It is not without reason that the first criterion listed in the GDPR is the flexible<sup>18</sup> criterion of the location of an organisational unit of the personal data processor<sup>19</sup>. It should be understood more broadly than the existing domicile criterion<sup>20</sup>. In fact, the GDPR refers with this new (in the Polish language version) concept to a flexible interpretation of domicile in private international law. Its interpretation, however, is very problematic<sup>21</sup>. The use of the term ‘organisational unit’ itself is questionable. The GDPR does not provide its definition. Recital 22 of the preamble merely indicates that the processing of personal data in the context of activities carried out by an organisational unit of a data controller or processor in the EU should be carried out in accordance with the GDPR, regardless of whether the processing itself takes place in the EU. Additionally, it is stated that the term ‘organisational unit’ implies an effective and actual conduct of business through stable structures. The legal form of such structures, whether a branch or an incorporated subsidiary, is not a determining factor in this regard<sup>22</sup>.

Even if a data processor does not have an organisational unit in the EU, it will have to apply the provisions of the GDPR as long as it offers goods and services in the EU to persons located in the EU<sup>23</sup>. This issue is addressed by the second criterion provided in Article 3 of the GDPR.

<sup>18</sup> Voigt, von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, 22.

<sup>19</sup> As emphasised from the beginning at the stage of drafting of the regulation; see: Paul de Hert, Vagelis Papakonstantinou, “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals,” *Computer Law & Security Review* 28, no. 2 (April 2012): 130–142.

<sup>20</sup> Dan Svantesson, “Article 4(1)(A) ‘Establishment of the Controller,’ in EU Data Privacy Law – Time to Rein in this Expanding Concept?,” *International Data Privacy Law* 6, no. 3, (2016): 210.

<sup>21</sup> Paul De Hert, Michał Czerniawski, “Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context,” *International Data Protection Law* 6, no. 3 (2016): 230.

<sup>22</sup> Cf.: Voigt, von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, 23.

<sup>23</sup> Cf.: William Long, Géraldine Scali, Francesca Blythe, Alan Raul, “European Union overview,” in *Data Protection and Cybersecurity Law Review*, ed. Alan Raul (London: The Law-Reviews, 2015), 12.

According to Article 3(2)(a) of the GDPR and recital 23 of its preamble, in order for natural persons not to be deprived of the protection afforded to them under that Regulation, the processing of the personal data of data subjects located in the EU by a data controller or processor who does not have an organisational unit in the EU should be subject to the GDPR if the processing activities are connected with offering of goods or services to such persons, whether or not this entails payment.

In order to determine whether a data controller or processor offers goods or services to data subjects located in the EU, it is necessary to establish whether it is clear that the data controller or processor plans to offer services to data subjects in at least one member state of the EU<sup>24</sup>. The availability in the EU of the controller's, processor's, or intermediary's website, email address, or other contact details, or the use of a language commonly spoken in a third country in which the controller's organisational unit is located, is not sufficient to establish such intent<sup>25</sup>. However, factors such as the use of a language or currency commonly used in at least one EU member state and the ability to order goods and services in that language, or a mention of customers or users located in the EU are relevant<sup>26</sup>.

The processing of personal data of persons located in the EU by a data controller or processor who does not have an organisational unit in the European Union is subject to the GDPR also in cases where it involves monitoring of the behaviour of such persons, as long as that behaviour takes place within the EU. This is the third criterion specified in Article 3 of the GDPR. To establish whether processing can be considered as 'monitoring of the behaviour' of persons, it must be determined whether the activities of natural persons are observed in any way (e.g. Internet activity tracked through cookies or information provided by search engines, physical movements tracked through data provided by cell phones, etc.)<sup>27</sup>. It should be emphasised that the above criterion will be met regard-

---

<sup>24</sup> Frédéric Lecomte, *Nouvelle donne pour les données; le RGPD en quelques principes pour être prêt le 25 mai 2018* (Paris: Fauves, 2018), 24–25.

<sup>25</sup> Haas, *La réglementation sur la protection des données personnelles*, 18–20.

<sup>26</sup> Cf.: Voigt, von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, 26.

<sup>27</sup> Cf.: Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Copenhagen: Ex Tuto Publishing, 2013), 226; Prudence Cadio, Thomas Livenais, "Photographie du champ territorial



less of whether data processing techniques involving profiling of natural persons are later applied to the data so collected, in particular to make a decision concerning the person or to analyse or predict the person's personal preferences, behaviour, and attitudes<sup>28</sup>.

Due to interpretive difficulties, in late 2019 the European Data Protection Board (EDPB) published guidance on the territorial scope of application of the GDPR<sup>29</sup>. These guidelines take into account the specific characteristics of AI only to a small extent.

As can be seen, as technology advances, the interpretation of the criteria for determination to which international situations the GDPR applies is broadening, which indeed must affect the process of determination of the proper law in case of a breach of the protective regime established in the GDPR. What we have in mind is not only the location of the infringer itself (establishing its domicile or its organisation unit), but also the 'location' of its activity resulting in a breach of the GDPR and giving rise to tort liability on the part of the infringer. There is a need for uniform use of the aforementioned guidance, for the purpose of determination of both the scope of application of the GDPR and the civil-law consequences of an infringement of the data protection principles adopted therein. The above circumstances further justify recourse to the codified conflict-of-law rules set forth in the Rome II Regulation and adoption of an interpretation of the connecting factors used therein in the spirit of the criteria adopted in Article 3 of the GDPR.

#### 4. Summary and conclusions

The future model of liability for AI damages should cover also infringements relating to data privacy protection. The inclusion of this issue in the future convention of the Council of Europe on Artificial Intelligence is a natural consequence of the application of the modernised Convention 108+ and the Council of Europe's Guidelines on Artificial Intelligence and

---

du reglement données personnelles: de nouveaux opérateurs concernées?," in *Le RGDP*, ed. Stéphanie Prévost and Erwan Royer (Paris: Dalloz, 2018), 33–35.

<sup>28</sup> Voigt, von dem Bussche, *The EU General Data Protection*, 27.

<sup>29</sup> Accessible: accessed May 8, 2022, [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en).

Data Protection. However, this will not exclude the necessity to determine the applicable law in line with current conflict-of-law rules.

The lack of consistency in the liability model among different states could be further augmented due to the lack of inclusion of the applicable conflict-of-law regulations to the existing legal framework and their relevance to the determination of the principles of liability for damages caused by AI systems. In the European Parliament submitted draft on the principles of civil liability for damages caused by AI systems<sup>30</sup>, one can notice that there is no reference to the Rome II Regulation concerning the applicable law to non-contractual obligations. The same concerns Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence 2022/0303(COD). This constitutes a significant gap. Both documents follows outdated view on conflict-of-law solutions instead of the modern and differentiated ones adopted in the Rome II Regulation. In further stages of the work on draft Directive, the indicated shortcomings should be eliminated.

## References

- Ahern, John, and Wiliam Binchy. *Rome II Regulation on Law Applicable to Non-Contractual Obligations*. Leiden: Brill, 2009.
- Balcarczyk, Justyna. “Wybrane problemy związane z projektem ustawy – Prawo prywatne międzynarodowe.” *Rejent*, no. 7–8 (2009): 9–25.
- Braciak, Joanna. *Prawo do prywatności*. Warsaw: Wydawnictwo Sejmowe, 2004.
- Briere, Carine. “Le reglement (CE) no 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II).” *Journal de droit international* 135 (2008): 31–74.
- Brkan, Maja. “Data Protection and Conflict-of-Laws: A Challenging Relationship. *European Data Protection Law Review* 2, no. 3 (2016): 324–341. <https://doi.org/10.21552/EDPL/2016/3/8>.
- Cadio, Prudence, and Thomas Livenais. “Photographie du champ territorial du reglement données personnelles: de nouveaux opérateurs con-

---

<sup>30</sup> *Civil liability regime for artificial intelligence*, resolution of the European Parliament, 20.10.2020, accessed February 7, 2023, [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html)

- cernées?." In *Le RGDP*, edited by Stéphanie Prévost, Erwan Royer, 31–36. Paris: Dalloz, 2018.
- Całus, Andrzej. "Znaczenie rozporządzenia Rzym II dla unifikacji prawa właściwego dla czynów niedozwolonych w państwach członkowskich Unii Europejskiej." In *Czyny niedozwolone w prawie polskim i w prawie porównawczym* edited by Mirosław Nesterowicz, 146–110. Warsaw: Wolters Kluwer, 2012.
- Carruthers, Janeen, and Elizabeth Crawford. "Variations on a theme of Rome II. Reflections on proposed choice of law rules for non-contractual obligations: Part I." *Edinburgh Law Review* 9 (2005): 65–97; Part II, *Edinburgh Law Review* 9 (2005): 238–266.
- Czerniawski, Michał. "Zakres terytorialny a pojęcie 'jednostki organizacyjnej' w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu." In *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, edited by Grzegorz Sibiga, 22–28. Warsaw: C.H. Beck, 2016.
- de Hert, Paul, and Michał Czerniawski. "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." *International Data Protection Law* 6, no. 3 (2016): 230–243. <https://doi.org/10.1093/idpl/ipw008>.
- de Hert, Paul, and Papakonstantinou, Vagelis. "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals." *Computer Law & Security Review* 28, no. 2 (April 2012): 130–142. <https://doi.org/10.1016/j.clsr.2012.01.011>.
- Dickinson, Andrew. *The Rome II Regulation*. Oxford: Oxford University Press, 2010.
- Domagała, Natalia, Bartłomiej Oręziak and Marek Świerczyński, "Profiling in the recruitment of subjects for clinical trials in the light of GDPR." *Zeszyty Prawnicze* 20, no. 2 (2020): 265–280. <https://doi.org/10.21697/zp.2020.20.2.14>.
- Dornis, Tim. "When in Rome, do as the Romans do? – a defense of the *lex domicilii communis*: in the Rome II Regulation." *European Legal Forum* 4 (2007): 152–159.
- Fawcett, James, and Janeen Carruthers, and Peter North. *Private International Law*. Oxford: Oxford University Press, 2017.
- Feraci, Ornella. "La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria." *Rivista di diritto internazionale*, no. 4 (2009): 1020–1085.

- Gömann, Merlin. "The new territorial scope of EU data protection law: deconstructing a revolutionary achievement." *Common Market Law Review* 54, no. 2 (2017): 567–690. <https://doi.org/10.54648/cola2017035>.
- Graziano, Thomas. "Das auf aufservertragliche Schuldverhältnisse anzuwendende Recht nach Inkrafttreten der Rom II – Verordnung." *RabelsZ* 73 (2009): 1–177.
- Haas, Gérard. *La réglementation sur la protection des données personnelles*. St Herblain: Éditions ENI, 2018.
- Hartley, Trevor. "Choice of Law for Non-Contractual Liability: Selected Problems under the Rome II Regulation." *ICLQ* 57 (2008): 899–908.
- Kamarinou, Dimitra, and Christopher Millard, Jatinder Singh. "Machine Learning with Personal Data." *Queen Mary School of Law Legal Studies Research Paper*, no. 247(2016): 1–23.
- Kozyris, Phaeton. "Rome II: Tort Conflicts on the Right Track! A Postscript to Symeon Symeonides' Missed Opportunity." *AJCL* 56 (2008): 471–497.
- Lecomte, Frédéric. *Nouvelle donne pour les données; le RGPD en quelques principes pour être prêt le 25 mai 2018*. Paris: Fauves, 2018.
- Leible, Stefan, and Matthias Lechmann. "Die neue EG-Verordnung über aufervertragliche Schuldverhältnisse anzuwendende Recht (Rom II)." *Recht der Internationalen Wirtschaft* 53 (2007): 721–734.
- Litwiński, Paweł, and Maciej Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warsaw: Wolters Kluwer, 2017.
- Long, William, and Géraldine Scali, Francesca Blythe, Alan Raul. "European Union overview." In *Data Protection and Cybersecurity Law Review*, edited by Alan Raul Raul, 25–26. London: The Law Reviews, 2015.
- Noto La Diega, Guido. "Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 9, no. 1 (2018): 3–34.
- Plender, Richard, and Michael Wilderspin. *European Private International Law of Obligation*. London: Sweet and Maxwell, 2020.
- Royvroy, Antoinette. "Of Data and Men. Fundamental Rights and Freedoms in a World of Big Data. Report for the Bureau of the Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data." Council of Europe, TD-PD-BUR 2016. Accessed February 7, 2023. <https://rm.coe.int/16806a6020>.
- Rushworth, Adam, and Andrew Scott. "Rome II: Choice of law for non-contractual obligations." *LMCLQ* (2008): 274–306.

- Svantesson, Dan. "Article 4(1)(A) 'Establishment of the Controller' in EU Data Privacy Law – Time to Rein in this Expanding Concept?." *International Data Privacy Law* 6, no. 3, (2016): 210–221. <https://doi.org/10.1093/idpl/ipw013>.
- Symeonides, Symeon. "Rome II and Tort Conflicts: A Missed Opportunity." *AJCL* 56, no. 1 (2008): 173–222.
- Świerczyński, Marek. "Jurysdykcja krajowa w świetle rozporządzenia ogólnego o ochronie danych osobowych." *Europejski Przegląd Sądowy* 12 (2016): 21–28.
- Świerczyński, Marek. "Prawo właściwe dla zobowiązań deliktowych wynikających z naruszenia zasad ochrony danych osobowych przyjętych w RODO." *Problemy Prawa Prywatnego Międzynarodowego* 27 (2019): 39–59. <https://doi.org/10.31261/PPPM.2020.27.02>.
- Voigt, Paul, and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR). A Practical Guide* Cham: Springer, 2017.
- Wolff, Heinrich, and Stefan Brink, ed. *Beck'scher Online-Kommentar Datenschutzrecht*, Munich: C.H. Beck, 2017, Rn. 1–46.

