*ARTICLE*

**NIPR 2023-12**

# Issues of conflicting laws – a closer look at the EU's approach to artificial intelligence

**Kirsten Henckel***

**Abstract**

*While newly emerging technologies, such as Artificial intelligence (AI), have a huge potential for improving our daily lives, they also possess the ability to cause harm. As part of its AI approach, the European Union has proposed several legislative acts aiming to accommodate and ensure the trustworthiness of AI. This article discusses the potential private international law impact of these legislative proposals. In doing so, it – inter alia – addresses how the newly proposed legislative acts interact with existing private international law instruments, such as the Rome II Regulation. In addition, it questions whether there is a need for specific rules on the private international law of AI.*

## 1. Introduction

Recent years have seen an unprecedented growth in new and advanced technologies, such as artificial intelligence (AI). AI has moved from science fiction to playing an increasingly important role in our daily lives. In fact, the use of AI appears more and more ubiquitous, ranging from travelling in a self-driving vehicle, to automated dispute settlement or using a chatbot to write a thesis. While AI presents many opportunities that will better daily life[1] and contribute to solving the world's most pressing problems,[2] it also presents new possibilities for harm. Traffic accidents involving self-driving vehicles[3] and financial loss or business devaluation caused by failed algorithms[4] are telling examples.

---

* Dr. K.C. Henckel LL.M. is assistant professor of private international law at the University of Groningen.

1 White Paper on artificial intelligence – A European approach to excellence and trust (COM(2020) 65 final).

2 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics' (COM(2020) 64 final), para. 1.3.

3 A. Pato, 'The EU's Upcoming Regulatory Framework on Artificial Intelligence and Its Impact on PIL', EAPIL Blog, 12 July 2021, available online at: https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/ (accessed 26 May 2023); M. Roe, 'Who's Driving That Car: An Analysis of Regulatory and Potential Liability Frameworks for Driverless Cars', *Boston College Law Review* (60) 2019, pp. 317 et seq.; T. Kadner Graziano, 'Cross-border traffic accidents in the EU – the potential impact of driverless cars', Study for the Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs [2016], available online at: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571362/IPOL_STU(2016)571362_EN.pdf (accessed 26 May 2023).

4 R. Metz, 'Zillow's home-buying debacle shows how hard it is to use AI to value real estate', *CNN Business*, 9 November 2021, available online at: https://edition.cnn.com/2021/11/09/tech/zillow-ibuying-home-zest

The advent of AI and its potential for harm as well as the possibility of ensuing cross-border liability disputes has not gone unnoticed by the European legislator. In September 2022, the European Commission published an eagerly-awaited proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).[5] This proposal – which follows a call to action by the Council[6] and the European Parliament[7] – is intended to ensure that citizens enjoy the same rights and level of protection, regardless of whether harm is caused by an AI system.[8] It is part of a larger package of legislative reform on AI that is intended to foster the use and application of AI while at the same time addressing its risks. This legislative package consists of three elements:[9]

- An EU framework for AI addressing fundamental rights and safety risks known as the AI Act;
- A civil liability framework, consisting of an AI Liability Directive[10] and a revision of the Product Liability Directive;[11]
- A revision of sectoral safety legislation, including changes to the Machinery Directive[12] and the General Product Safety Directive.[13]

This article seeks to address the conflict of laws implications of this new set of legislation. It questions whether there is a need for specific rules on the private international law of AI. In answering this question, it – *inter alia* – discusses how the newly proposed legislative acts interact with existing private international law mechanisms, notably the Rome II Regulation.[14]

---

imate/index.html; A. Polyakov, 'What Harm Can AI Do? Plenty, But We Can Minimize It Together', *Forbes*, 15 June 2022, available online at: https://www.forbes.com/sites/forbestechcouncil/2022/06/15/what-harm-can-ai-do-plenty-but-we-can-minimize-it-together/?sh=1ad31d7a1e77 (both accessed 26 May 2023).

5 Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.

6 Council conclusions on shaping Europe's digital future, 9 June 2020, 8711/20, note 23.

7 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). For a full overview of events and documentation leading up to the proposal see sect. 4 below.

8 COM(2022) 496 final (*supra* note 5), p. 1.

9 Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence, COM(2021) 205 final, pp. 31-32.

10 COM(2022) 496 final (*supra* note 5).

11 Proposal for a directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495.

12 Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021) 202.

13 Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, COM(2021) 346 final.

14 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), *OJ* 2007, L 199/40.

The following sections will first address the definition of AI (sect. 2), followed by a closer look at each of the legislative proposals: the AI Act (sect. 3), the AI Liability Directive (sect. 4), the Product Liability Directive (sect. 4), the Machinery Regulation (sect. 5) and the General Product Safety Regulation (sect. 5). Subsequently, the article will show how the existing rules of private international law, especially the Rome II Regulation, are impacted by the proposed legislative package (sect. 6).

## 2. What is AI? (definition)

Before looking into the various legislative proposals and how they might impact private international law, it is important to have a clear understanding of what is meant by artificial intelligence.[15] In essence, an understanding of the challenges that private international law faces when it comes to AI requires a demystified view of what AI entails and how it might be applied.[16] Yet, defining AI is not an easy task. At present, a uniform definition of AI does not exist. The difficulty in defining AI lies in the fact that it is an umbrella term for a constantly evolving discipline that includes many different approaches and techniques.[17]

In everyday usage AI is often described as the use of technology to automate tasks that require some form of human intelligence.[18] In fact, the resemblance to human intelligence, such as the ability to reason or learn from past experience, is a common denominator in explaining AI. Most definitions emphasize the use of technology that enables the automation of specific tasks. Simply put, AI involves techniques that mimic the problem-solving and decision-making abilities of the human mind.[19]

Although AI systems are sometimes described as 'intelligent' or 'thinking machines', it is important to understand that while most work in AI involves problems that cannot be solved by

15 The term itself was first coined by John McCarthy in 1955 (J. McCarthy et al., 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence', 31 August 1955) but the underlying idea dates back to a 1950 paper by Alan Turing, in which he proposed a test for determining whether machines could think, known as the Turing Test or Imitation Game. See: A.M. Turing, 'Computing Machinery and Intelligence', *Mind* 1950, pp. 433-460.

16 Cf. A. Bertolini & F. Episcopo, 'The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment', *European Journal of Risk Regulation* 2021, p. 648.

17 Cf. B. Kleinhout & J.L. Naves, 'Het voorstel voor een Europese AI-verordening en de betekenis daarvan voor Nederlandse overheden' ['The Proposal for a European AI Regulation and the significance thereof for the Dutch authorities'], *NTB* 2022/38, pp. 67-68.

18 The Oxford English Dictionary describes AI as 'the capacity of computers or other machines to exhibit or simulate intelligent behaviour', whereas Encyclopaedia Brittanica describes AI as 'the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings', available online at https://www.britannica.com/search?query=artificial+intelligence (accessed 26 May 2023).

19 Cf. S. Russell & P. Norvig, *Artificial Intelligence: A Modern Approach*, Hoboken: Pearson 2021, pp. 1-5; B. Cappiello, *AI systems and non-contractual liability: A European private international law analysis*, Turin: Giappichelli 2022, pp. 8-12.

the human mind,[20] present-day AI systems do not 'think' as humans do. This difference relates to the distinction between so-called weak – or narrow – AI and strong – or general – AI.[21] Weak AI is technology that is intended to perform certain well-defined tasks whereas strong AI relates to an artificial super intelligence that is self-aware and has the ability to solve problems and set its own goals.[22] Whereas the existence of strong AI remains a remote ideal, weak AI is readily applied. It is precisely this form of AI that the European legislator seeks to regulate.[23]

In its 2018 Communication on AI the European Commission defined AI as referring to 'systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals'.[24] This definition was subsequently expanded by the High-Level Expert Group on AI to include both AI as a scientific discipline and as a technology. The Expert Group attributes certain capabilities to AI systems, such as reasoning, data acquisition, analysis, decision-making, adaptation to behaviour and the achievement of specific goals.[25] Yet in analysing the newly proposed legislative package on AI, it is not this definition that is key. What is of relevance is the definition in each individual piece of legislation. Interestingly, these definitions – although mutually aligned – differ from the definition provided by the High-Level Expert Group on AI.

The term 'AI system' forms the core of the EU's legislative package. The legal definition of this term can be found in Article 3(1) of the draft AI Act, which states that 'AI system' means:

> 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.'

Annex 1 of the draft AI Act provides a list of techniques and approaches that are currently used for the development of AI. Accordingly, the notion of 'AI system' includes technologies that utilise machine-learning approaches, logic- and knowledge-based approaches as well as

20 J. McCarthy, 'What is artificial intelligence?', 2007, available online at: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf (accessed 26 May 2023).

21 McCarthy 2007, pp. 4-5 (*supra* note 20); S. Harnad, 'Mind, Machines and Searle II: What's Wrong and Right About Searle's Chinese Room Argument?', in: M. Bishop & J. Preston, *Essays on Searle's Chinese Room Argument*, Oxford: Oxford University Press 2001; E. Kumar, *Artificial Intelligence*, New Delhi: I.K. International Publishing House 2008, p. 14.

22 Kumar 2008, pp. 13-14 (*supra* note 21); K. Xivuri & H. Twinomurinzi, 'A systematic review of fairness in artificial intelligence algorithms', in: A. Griva et al., *Responsible AI and Analytics for an Ethical and Inclusive Digitized Society*, Cham: Springer international 2021, p. 271.

23 White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final.

24 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25 April 2018, COM(2018) 237 final.

25 Also see the operational definition provided by the Joined Research Centre: S. Samoili et al., *AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, EUR 30117 EN, Publications Office of the European Union, Luxembourg, 2020, doi:10.2760/382730, JRC118163.

statistical approaches.[26] The definition proposed by the Commission is intended to ensure legal certainty, while at the same time providing the flexibility to accommodate future technological and market developments.[27] In part, legal certainty is to be provided by the Annex, which is to be kept up to date in line with technological advances.[28]

In its current phrasing, the proposed definition of 'AI system' is much broader than the one provided by the High-Level Expert Group on AI. Moreover, it exceeds what is understood as AI in common parlance. It is this broad definition that endangers the AI Act of capturing more traditional software systems that are generally not considered to be AI.[29] Capturing simple automation processes seems contrary to the primary purpose of the Act. In addition, an overly broad scope may lead to legal uncertainty on the part of those involved in the development and use of various kinds of software.[30] As such, it is unsurprising that the definition of AI system has attracted much criticism.[31] In fact, it is one of the most controversial subject matters of the entire Act, with some proposing a broader[32] and some a narrower[33] definition. Advocating the

---

26 Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.

27 Recital 6 draft AI Act; para. 5.2.1 Explanatory memorandum draft AI Act.

28 Recital 6 draft AI Act; para. 5.2.1 Explanatory memorandum draft AI Act.

29 D. Bomhard & M. Merkle, 'Europäische KI-Verordnung. Der aktuelle Kommissionsentwurf und praktische Auswirkungen', *Recht Digit*. 2021, pp. 276-283; M. Ebers et al., 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', *Multidisciplinary Scientific Journal* (*J)* 2021, p. 590.

30 Kleinhout & Naves 2022, p. 68 (*supra* note 17); Ebers et al. 2021, p. 590 (*supra* note 29).

31 Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 12 September 2022, 2021/0106(COD), pp. 4, 21; Draft opinion of the Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 3 March 2022, 2021/0106(COD); Bomhard & Merkle 2021, pp. 276-283 (*supra* note 29); L. Bertuzzi, 'AI regulation filled with thousands of amendments in the European Parliament', *Euractiv*, 2 June 2022, available online at: https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/ (accessed 26 May 2023).

32 R. Dufour et al., 'AI or More? A Risk-based Approach to a Technology-based Society', Oxford Business Law Blog, 16 September 2021, available online at: https://blogs.law.ox.ac.uk/business-law-blog/blog/2021/09/ai-or-more-risk-based-approach-technology-based-society (accessed 26 May 2023). Cf. Bertuzzi 2022 (*supra* note 31); T. van der Linden, 'Regulating Artificial Intelligence: Please apply existing Regulation', *Amsterdam Law Forum* (13/3) 2021, pp. 3-9.

33 Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 12 September 2022, 2021/0106(COD), p. 4; European Parliament, Draft Opinion of

latter view, the Council of the EU proposed a narrower definition of AI system in its general approach on the draft AI Act. Accordingly, the notion of 'AI system' should refer to a system that is capable of determining how to achieve a given set of human-defined objectives through learning, reasoning or modelling.[34] This taxonomy change is intended to increase legal certainty and to prevent the unnecessary inclusion of simpler software systems.[35] Still, the definition of AI or AI system will likely be amended prior to the acceptance or entry into force of the AI Act, as the Act is still undergoing a detailed legislative process.

Although the substantive scope of each legislative instrument and the definition of AI is of key importance to the application of the proposed acts, it is the essence of these instruments and how they might impact private international law that forms the primary object of this article. As such, the following sections will detail the proposed legislative acts as well as their effects on private international law.

## 3. AI Act

On 21 April 2021, the European Commission published a proposal for a Regulation on Artificial Intelligence, known as the AI Act. The proposal provides harmonised rules for the development, placement on the market and use of AI systems within the European Union. With this first-ever horizontal framework on AI the European Commission aims to facilitate the development and use of trustworthy AI systems within the EU. In addition, the Act seeks to achieve a number of specific objectives: (1) ensure that AI systems placed on the EU market are safe and respect existing laws on fundamental rights and Union values, (2) ensure legal certainty to facilitate investment and innovation in AI, (3) enhance governance and effective enforcement of existing law, and (4) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.[36] In essence, the Act seeks to promote the advance of AI while addressing the risks associated with its use.

Curiously, the AI Act itself does not address any issues of liability nor does it provide individual rights, a private enforcement regime or any appropriate rules on private international law

---

the Committee on Industry, Research and Energy for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Rapporteur: E. Maydell) 2022, 2021/0106(COD); Bomhard & Merkle 2021, pp. 276-283 (*supra* note 29); B. Benifei & I.D. Tudorache, 'Draft Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD))', Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs, 20 April 2022. Cf. Bertuzzi 2022 (*supra* note 31).

34 Cf. Changes to Recital 6.

35 Council of the EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach, 25 November 2022, available online at: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ (accessed 26 May 2023).

36 For a more detailed overview see AI Act, Framework of the Proposal, para. 1.4.

(see below sect. 3.2).[37] Instead, it sets out the requirements that providers, operators and users of AI systems have to comply with when (and/or before) placing an AI system on the European market, or putting the AI system into service, or using it – or its output – within the EU.[38] In doing so, the Act follows a risk-based approach that imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety.[39] It introduces a risk pyramid that distinguishes between AI systems that pose an (1) unacceptable risk, (2) high risk, (3) limited risk and (4) minimal risk. Accordingly, stricter regulation applies as risk increases.

Systems that pose an unacceptable risk are prohibited, whereas high-risk systems – e.g. facial recognition or automated credit scoring – are subject to certain mandatory obligations and a market-entry conformity assessment. Limited-risk systems are subject to transparency obligations – e.g. when using a chatbot, users should be made aware that they are communicating with a machine – whereas minimal-risk systems may be used freely.

In order to ensure compliance with its requirements the Act not only requires adequate risk management, it also requires Member States to appoint national competent authorities tasked with the enforcement of the Act at a national level. Such supervisory authorities will be able to issue effective, proportionate and dissuasive penalties for non-compliance with the provisions of the Act.[40]

All in all, the AI Act is an instrument that is based on public rather than private law as it primarily holds market-entry requirements rather than introducing rights and obligations to regulate the relationship between private parties.[41] As such, the private international law implications of the Act remain limited. Even though AI systems have a huge potential for harm, which may be exacerbated by non-compliance with the provisions of the AI Act, it is only when the provisions of the Act are invoked in civil liability proceedings that issues of private international law come into play. With this in mind, Article 2 of the Act – which sets out its extraterritorial scope – proves most interesting from a private international law perspective.

### *3.1 Extraterritorial scope*

The territorial scope of the AI Act is set out in Article 2 and is reminiscent of that of the General Data Protection Regulation (GDPR)[42] in terms of its extraterritorial reach. By incorporating

37 Also see: J. von Hein, 'Forward to the Past. A Critical Evaluation of the European Approach to Artificial Intelligence in Private International Law', in: S. Voeneky, *The Cambridge Handbook of Responsible Artificial Intelligence. Interdisciplinary Perspectives*, Cambridge: Cambridge University Press 2022, p. 226.

38 Art. 2(1) AI Act.

39 AI Act, Explanatory Memorandum, para. 2.3.

40 Art. 71 AI Act.

41 A.G. Grasso, 'Private (and substantive) international law aspects of European law on artificial intelligence', March 2022, available online at: https://www.researchgate.net/publication/359175058_Private_and_substantive_international_law_aspects_of_European_law_on_artificial_intelligence (accessed 26 May 2023), p. 5. Cf. Von Hein 2022, p. 226 (*supra* note 37).

42 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* 2016, L 119/1-88.

a unilateral scope rule, the Act indicates directly when it is to apply. Pursuant to Article 2(1), the rules on AI are to apply to:

a) providers placing AI systems on the market or putting them into service in the EU;
b) users of AI systems located within the EU; and
c) providers and users of AI systems located in a third country, when the output of the AI systems is used in the EU.

According to the Commission, the extended territorial scope is needed to 'ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union'.[43] With this scope, the application of the AI Act is extended beyond the territory of the EU and equally applies to third state providers and users whenever the use of the AI system – or its output – is tied to the EU.

#### 3.1.1 'Placing on the market' or 'putting into service'

In accordance with Article 2(1)(a), the Act first applies to providers who place AI systems on the market or put them into service in the EU, regardless of where these providers are established. The Act provides a definition of 'placing on the market' or 'putting into service' that is in line with the definition in other harmonised EU legislation and follows traditional free movement of goods language.[44] Accordingly, an AI system is placed on the EU market whenever it is first made available there.[45] An AI system is 'put into service' whenever it is supplied 'for first use directly to the user or for own use on the Union market for its intended purpose'.[46]

#### 3.1.2 Users located within the EU

Article 2(1)(b) extends the application of the Act to users of AI systems located within the EU. The Act provides a rather counterintuitive definition of 'user' in Article 3(4). Accordingly, a 'user' is any natural or legal person *using an AI system under its authority*, except where the AI system is used in the course of a personal non-professional activity. The term 'user' therefore refers to the person deploying the AI system and excludes those using the system for personal reasons. It does not refer to the end-user of the system or the person affected by the system, e.g. as a data subject.[47]

The Act remains silent on when users are located within the EU. A clear and predictable application of the Act would surely require a proper definition of the elements that trigger its application, including the concept of location. Hence, a clarification of the notion of location

43 Recital 10 AI Act.

44 See Commission notice, 'The "Blue Guide" on the implementation of EU product rules 2022', *OJ* 2022, C 247, pp. 19 et seq.

45 Art. 3(9) AI Act.

46 Art. 3(11) AI Act.

47 L. Edwards, 'The EU AI Act: a summary of its significance and scope', Ada Lovelace Institute, April 2022, available online at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf (accessed 26 May 2023), p. 8.

would be a much-needed addition to the Act.[48] After all, the lack of a proper definition gives rise to several questions, such as whether a temporary presence within a particular territory is sufficient to trigger application of the Act, or whether it requires a more permanent presence akin to traditional private international law concepts such as domicile or habitual residence. An additional concern is how to define the notion of location when it comes to legal persons: does it , for example, relate to 'statutory seat', 'place of business' or 'headquarters'?

The ambiguity of the notion of location has not gone unnoticed at a European level. In its general approach on the draft AI Act the Council of the EU proposed replacing the notion of 'location' with 'physical presence or establishment'. At first glance, tying the application of the Act to a physical presence in the EU appears drastic and subject to unexpected change once a user ventures outside the territory of the EU. However, given that the notion of user is tied to professional use, its application may be less problematic. To clarify, the location of the user only changes whenever he takes up the professional use of the AI system at a new location, ruling out a change in location via e.g. a simple holiday abroad.

Although the suggestion of the Council is an improvement upon the undefined notion of location, it still requires additional clarification when it comes to defining 'establishment'. One could imagine a definition in line with the GDPR in accordance with which an establishment implies the 'effective and real exercise of activity through stable arrangements'.[49]

### 3.1.3 Third-state providers and users when the output of the AI system is used in the EU

Finally, pursuant to Article 2(1)(c), the Act applies to providers and users of AI systems located outside the EU, when the output of those systems is used in the EU. This subsection is meant to prevent a circumvention of the Act and to ensure an effective protection of natural persons located within the EU. For example, when an EU-based company outsources certain services to an operator of an AI system outside the EU it might provide that operator with data lawfully collected in the EU. The third-state operator may subsequently process such data with the use of an AI system, before transferring its output to the EU-based company for use in the EU. In such cases, neither the provider nor the user of the AI system is located within the EU, while the output is used within EU territory. In such situations, the Commission deems it desirable that the AI Act applies. As such, whenever the output of an AI system is used in the EU, those systems fall within the scope of the Act, regardless of where its providers and users are located. This subsection has one exclusion, namely public authorities of third countries and international organisations which act within the framework of an international agreement concluded for law enforcement and judicial cooperation with the Union or its Member States.

The AI Act does not include an independent definition of the concept of 'output'. Instead, the notion of output forms part of the definition of AI system. This definition introduces a non-exhaustive list of potential forms of output, namely: content, predictions, recommendations and decisions. Given that the application of the Act, in Article 2(1)(c), is tied to the notion

48 Also see: Pato 2021 (*supra* note 3); Ebers et al. 2021, p. 591 (*supra* note 29).

49 Recital 22 GDPR; Recital 19 of Directive 95/46/EC; CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*); CJEU 1 October 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*). For a clear outline of what is meant by the effective and real exercise of activity through stable arrangements see: P. de Miguel Asensio, *Conflict of laws and the internet*, Cheltenham: Edward Elgar 2020, paras. 3.44-3.48.

of 'output' one would expect a clearer definition of the concept than a mere list of examples. Even if the notion of output is to be interpreted broadly in order to withstand technological advances one could imagine a definition of output that aligns with its definition in everyday language, in accordance with which the notion of output concerns that whatever the AI system produces.

### *3.2 Private international law impact*

As outlined above, Article 2 of the AI Act provides an express unilateral scope rule with extraterritorial effect. Under private international law theory, the application of such rules results in the displacement of the traditional – multilateral – conflict of laws reference. Where that is the case, it is the scope rule that determines when a particular rule or act applies, not the private international instruments. Still, the impact of Article 2 on private international law is limited as the Act is not geared towards civil liability or the introduction of individual rights. From a private international law perspective, Article 2 becomes relevant in cases of private enforcement, i.e. where the AI Act is invoked in civil liability proceedings (see sect. 4). In such situations, the application of the Act is dependent on Article 2 and not on the existing mechanisms of private international law such as the Rome II Regulation. Still, one would need the Rome II Regulation to establish the applicable liability regime (the law applicable to the non-contractual obligation in question) as this is an issue that is not covered by the AI Act (see below sects. 4 and 6).

In addition, ensuring a proper private enforcement of the provisions of the AI Act would require rules on jurisdiction that are tailored to AI and the extraterritorial scope of the Act. In the absence of any specific rules on jurisdiction, private enforcement actions would befall the Brussels Ia Regulation.[50] This Regulation primarily attributes jurisdiction to Member State courts in civil and commercial matters[51] whenever the defendant is domiciled within a Member State. It does not apply to defendants domiciled in third states except in a limited number of cases.[52] In order to sue third-state providers, operators and users of AI systems before a Member State court claimants will therefore have to rely on the national rules of private international law, which vary greatly, making it difficult to truly predict *à priori* where one might be sued. Moreover, the application of national rules on jurisdiction to third-state defendants may potentially leave claimants without any recourse to a Member State court. This is a natural consequence of the fact that Member States have traditionally been reluctant to extend the application of the Brussels Ia Regulation to third-state defendants – only allowing jurisdiction whenever there is a true connection between the defendant and the territory of a Member State.[53] Yet, where an

50 Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *OJ* 2012, L 351/1.

51 See Art. 79(2) GDPR.

52 These cases involve a choice of court (Art. 25), exclusive jurisdiction (Art. 24), consumer contracts (Art. 18(1)) and employment contracts (Art. 21(2)).

53 The inclusion of third-state defendants in the Brussels regime was explored during the revision of the Brussels I Regulation, but this was ultimately abandoned because of a need for further research and political debate as well as concerns regarding recognition and enforcement, reciprocity and international comity. Still, the debate continues in light of the upcoming evaluation of the Brussels Ia Regulation. See: European

instrument – such as the AI Act – aims to apply to third-state defendants, such extraterritorial application is negated if claimants are unable to have access to a court with relevant jurisdiction.

A comparison with the GDPR shows that the introduction of a private enforcement regime and an accompanying rule on jurisdiction that is aligned with the territorial scope of the instrument are effective ways to ensure that individuals are able to enforce their rights before a Member State court. Although the GDPR has been deservedly criticised for failing to properly address its relationship with the Brussels Ia Regulation, resulting in a simultaneous application of both instruments and a patchwork of potential fora, it has succeeded in providing an effective jurisdictional basis for cases falling within its scope.[54] By comparison, including a jurisdictional provision in the AI Act that aligns with its territorial scope would surely ensure access to justice for those seeking to enforce the provisions of the Act. Yet, taking into account the shortcomings of the GDPR, such a provision should take note of the decades-old Brussels regime and should ensure a proper delineation to avoid a multitude of potential fora. A solution to a possible concurrence in application would be to apply the maxim of *lex specialis derogat legi generali* or to limit the application of a potential jurisdictional provision to cases falling outside the scope of the Brussels Ia Regulation, notably cases involving third-state defendants.

At present, the AI Act neither provides a civil liability regime, nor any provisions on private enforcement, allowing individuals to hold operators of AI systems liable for a failure to comply with the provisions of the AI Act.[55] In fact, despite referencing the right to an effective remedy as an important procedural fundamental right in Recital 38, the Act does not include any express individual rights for those impacted by AI systems, nor does it expressly allow for

---

Parliament resolution of 7 September 2010 on the implementation and review of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (2009/2140(INI)), para. 15; Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, COM(2010) 748 final; Green Paper on the review of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, COM(2009) 175 final; Art. 79 Brussels Ia Regulation. Cf. M. Poesen, 'Civil litigation against third-country defendants in the EU: effective access to justice as a rationale for European harmonization of the law of international jurisdiction', *Common Market Law Review* 2022, pp. 1597-1632.

54 G. van Calster, 'Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit au respect de la vie privée', *L'Observateur de Bruxelles* 2017, p. 30; 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"', *Cuadernos de Derecho Transnacional* 2017, pp. 448-464; I. Revolidis, 'Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism"?', *Masaryk University Journal of Law and Technology* 2017, pp. 21-36; J. Hörnle, 'Juggling more than three balls at once: multilevel jurisdictional challenges in EU Data Protection Regulation', *International Journal of Law and Information Technology* 2019, pp. 145 et seq. Also see on the interaction with the rules on jurisdiction concerning representative actions: D. Agulló Agulló, 'The interplay of data, consumer and Private International law rules in the area of collective access to justice in the European Union', *Cuadernos de Derecho Transnacional* 2022, pp. 85 et seq. Cf. on the extraterritorial scope of the GDPR: C. Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', *International Data Privacy Law* 2015, pp. 241 et seq.; D.J.B. Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws', *International Data Privacy Law* 2013, p. 278.

55 See Recital 2 AI Liability Directive.

individual or collective redress. In order to address this issue, several stakeholders, including European consumer organisation BEUC, have advocated the inclusion of individual rights and rules on access to justice by means of individual and collective redress[56] for those adversely affected by an AI system.[57] To a limited extent these concerns are addressed by the civil liability regime consisting of the AI Liability Directive[58] and the revised Product Liability Directive.[59] These legislative acts are meant to complement the AI Act and will be discussed in the following section.

## 4. Civil liability framework

On 28 September 2022, the European Commission adopted two proposals aiming to regulate civil liability in relation to AI systems: the AI Liability Directive[60] and the Product Liability Directive.[61] Both directives include rules on liability for those who are adversely affected by an AI system. Whereas the AI Liability Directive addresses liability claims against producers, operators and users of AI systems under national fault-based liability regimes, the Product Liability Directive covers a producer's no-fault liability for defective products. Together, these directives form a single package of legislation on civil liability intended to complement the AI Act. Their conjoined aim is to promote trust in AI by ensuring that those harmed by AI systems are effectively compensated if damage occurs.[62]

Although both directives deal with redress in the event of harm caused by an AI system, they do not contain any complementary private international law provisions aimed at facilitating access to justice or addressing issues of conflicting laws. Issues of private international law therefore befall the existing private international law rules, such as the Brussels Ia Regulation or the Rome II Regulation. Still, the proposed directives may affect private international law when it comes to e.g. the types of claims and the redress that they facilitate. The following sections will outline the AI Liability Act (sect. 4.1) and the Product Liability Act (sect. 4.2) and address their potential impact on private international law.

---

56 BEUC, 'Regulating AI to protect the consumer. Position Paper on the AI Act', BEUC-X-2021-088, available online at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf (accessed 26 May 2023), pp. 2-3, 23.

57 A. Bogucki et al., 'The AI Act and emerging EU digital acquis. Overlaps, gaps and inconsistencies', *CEPS* September 2022; M.E. Kaminski, 'Regulating the Risks of AI', University of Colorado Law Legal Studies Research Paper No. 22-21, 2023, p. 80, available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066 (accessed 26 May 2023); BEUC 2021, pp. 2-3, 23 (*supra* note 56); N. Smuha et al., 'How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act', LEADS Lab, August 2021, available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991, pp. 44-45.

58 COM(2022) 496 final (*supra* note 5).

59 COM(2022) 495 (*supra* note 11).

60 COM(2022) 496 final (*supra* note 5).

61 COM(2022) 495 (*supra* note 11).

62 Explanatory Memorandum AI Liability Directive, p. 2.

### *4.1 AI Liability Directive*

The AI Liability Directive intends to harmonise national non-contractual fault-based liability rules for damages incurred by AI-enabled products and services, especially when damage is the result of non-compliance with the AI Act. The primary objective of the directive is to promote the use of trustworthy AI within the internal market by ensuring that victims of AI systems are protected in the same way as victims of traditional technologies.[63]

In traditional fault-based liability systems the burden of proof lies with the claimant who has to establish a causal link between the harm suffered and the wrongdoing by the defendant. The special characteristics of AI systems, such as their complexity, autonomy and opacity, can make it difficult for a claimant to prove fault and establish such a causal link.[64] The opacity of an AI system, known as the black box effect, means that the system is so complex that its decision-making process cannot be easily explained or understood by humans. In such cases, establishing a causal link places an unfair evidentiary burden on the claimant.[65] To ease this burden, the directive introduces two distinct measures: (1) the right to access evidence (Art. 3) and (2) a presumption of causality (Art. 4).

Under Article 3, claimants will have the right to request relevant evidence from providers or users of high-risk AI systems about a specific high-risk AI system that is suspected of having caused damage. Member State courts will have the power to order such disclosure, and may assume non-compliance with a newly introduced 'duty of care' for AI systems if the defendant does not comply with the disclosure order. Article 4 includes a presumption of causality if the claimant can demonstrate that the provider or user of an AI system was at fault[66] for the damage caused by the output of the AI system[67] and that it can be considered reasonably likely that the fault influenced such output.[68] Under Article 4(1)(a) fault is considered to exist in the event of a failure to comply with a duty of care existing in national or EU law, such as the AI Act.

The AI Liability Directive mostly imposes substantive law provisions that have little impact on private international law. Yet, some of its provisions may be of relevance in a private international law context, such as the fact that it clarifies a right to redress for harm resulting from non-compliance with the AI Act and expressly allows for individual (including by succession and subrogation) and collective redress (see below sect. 4.1.2).[69] Still, it is startling that while most AI systems operate in a cross-border context, the directive fails to address any issues of jurisdiction or conflicting laws, even more so since the directive is a direct response to a Parlia-

63 This is described by the Commission as promoting 'the rollout of trustworthy AI to harvest its full benefits for the internal market', Explanatory Memorandum AI Liability Directive, p. 2.

64 Explanatory Memorandum AI Liability Directive, pp. 1-2.

65 S. Whittam, 'Mind the compensation gap: towards a new European regime addressing civil liability in the age of AI', *International Journal of Law and Information Technology* 2022, p. 251.

66 Art. 4(1)(a) AI Liability Directive.

67 Art. 4(1)(c) AI Liability Directive.

68 Art. 4(1)(b) AI Liability Directive.

69 Art. 2(6) AI Liability Directive.

ment resolution,[70] which in an accompanying draft Regulation on liability for the operation of AI systems (hereafter: Draft Regulation) did appear to propose rules on the conflict of laws.[71]

#### 4.1.1 Proposal for a Regulation

In October 2020, the European Parliament adopted a resolution which urged the European Commission to take action with regard to AI liability.[72] As outlined above, this resolution included a noteworthy Draft Regulation on AI liability which *inter alia* contained specific conflict of laws rules for AI liability.[73] Primarily, the Draft Regulation introduced substantive rules on liability. In doing so, it distinguished between high-risk AI systems[74] and other AI systems involving a lower risk.[75] It introduced an independent strict liability regime for high-risk AI systems,[76] while subjecting other AI systems to fault-based liability.[77] Article 2(1) of the Draft Regulation included a unilateral scope rule, which linked the application of the Regulation to harm caused by a physical or virtual activity, device or process driven by an AI system on the territory of the EU.[78] In doing so, Article 2(1) appeared to make the application of the Regulation contingent upon the location of the harm, thus applying a *lex loci damni* approach akin to the Rome II Regulation. A similar approach could be found in Article 9 of the Draft Regulation, which subjected limitation periods and compensation amounts for damage caused by non-high-risk AI systems to 'the law of the Member State in which the harm or damage occurred'. Both provisions have been criticised for introducing a regime that shows little flexibility and leaves the parties (especially the victim) less well off than under the existing Rome II

70 European Parliament resolution of 20 October 2020 (2020/2014(INL)) (*supra* note 7); Explanatory memorandum AI Liability Directive.

71 For a discussion on whether Art. 2(1) of the Draft Regulation should be read as a unilateral scope rule see: E. Lein et al., 'Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations', JUST/2019/JCOO_FW_CIVI_0167, European Union 2021, available online at: https://op.europa.eu/en/publication-detail/-/publication/11043f63-200c-11ec-bd8e-01aa75ed71a1 (accessed 26 May 2023), pp. 72-73.

72 European Parliament resolution of 20 October 2020 (2020/2014(INL)) (*supra* note 7). In this own-initiative resolution under Art. 225 of the Treaty on the Functioning of the European Union (TFEU) the European Parliament requested the Commission to adopt a proposal for a civil liability regime for AI based on Art. 114 TFEU.

73 Von Hein 2022, p. 211 (*supra* note 37). Cf. European Parliament, Draft Report 2020/2014(INL), 27 April 2020, available online at: www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf (accessed 16 May 2023).

74 Art. 3(c) Draft Regulation; Art. 4 Draft Regulation.

75 Art. 8 Draft Regulation.

76 Art. 4 Draft Regulation.

77 Art. 8 Draft Regulation.

78 Art. 2(1) Draft Regulation.

Regulation.[79] After all, the draft provisions failed to allow a choice of law,[80] nor did they include any exceptions[81] or escape clauses.[82] Moreover, they did not provide any special rules on specific torts, such as product liability.[83]

Despite the existence of conflict of laws provisions in the Draft Regulation (regardless of their potential defaults), no conflict of laws provision has been introduced in the AI Liability Directive. On the one hand, this is surprising since the directive is intended as a follow-up to the European Parliament resolution. On the other hand, this may have been expected given that the Rome II Regulation was not included in the list of provisions that the European Parliament had regard to in drafting its resolution.[84] Yet, given the inflexibility of the conflict of laws provisions in the Draft Regulation, the fact that similar provisions have not been introduced in the AI Liability Directive may be a blessing in disguise, as it enables the (full) application of the Rome II Regulation (see below sect. 6).[85]

#### 4.1.2 Private international law impact

Although rules on private international law remain notably absent from the AI Liability Directive, the directive nonetheless provides certain provisions and insights that are of relevance when it comes to private international law. First, the directive provides for a harmonisation of the laws of the Member States when it comes to AI liability.[86] As with any directive, it does not directly confer rights on individuals.[87] Instead, it requires the Member States to transpose the rules of the directive into their national laws. In other words: the directive does not have horizontal direct effect. As such, it is for the rules of private international law, predominantly the Rome II Regulation, to determine which Member State law (including the provisions transposing the AI Liability Directive) applies in the event of damage caused by an AI system.

Second, the directive ensures that individuals are able to initiate a civil claim for damage caused by the output of an AI system, especially in the event of non-compliance with the AI Act. From a private international law perspective, the fact that the directive relies heavily on the AI Act and any non-compliance therewith results in a congruence between the AI Liability Directive and the AI Act. This revives the discussion that was held above, in section 3.2, with regard to the unilateral scope rule contained in Article 2 of the AI Act. There, it was argued

79 Von Hein 2022, pp. 222-224 (*supra* note 37); Lein et al. 2021, pp. 72-73 (*supra* note 71); J. von Hein, 'Forward to the Past: A Critical Note on the European Parliament's Approach to Artificial Intelligence in Private International Law', *Conflictoflaws.net*, 22 October 2020, available online at: https://conflictoflaws.net/2020/forward-to-the-past-a-critical-note-on-the-european-parliaments-approach-to-artificial-intelligence-in-private-international-law/; Pato 2021 (*supra* note 3).

80 Cf. Art. 14 Rome II Regulation.

81 Cf. Art. 4(2) Rome II Regulation.

82 Cf. Art. 4(3) Rome II Regulation.

83 Art. 5 Rome II Regulation.

84 Von Hein 2022 (*supra* note 37).

85 Lein et al. 2021, pp. 72-73 (*supra* note 71); Von Hein 2020 (*supra* note 79).

86 More specifically, the directive harmonises certain national non-contractual fault-based liability rules.

87 Cf. CJEU 18 January 2022, Case C-261/20, ECLI:EU:C:2022:33 (*Thelen Technopark Berlin)*, para. 32; CJEU 24 June 2019, Case C-573/17, ECLI:EU:C:2019:530 (*Popławski*), para. 59.

that this rule is of relevance only where the AI Act is invoked in cases of civil liability.[88] In such cases, the scope rule contained in Article 2 of the AI Act determines when the provisions of the Act apply. This bypasses the conflict of laws reference contained in e.g. the Rome II Regulation. Yet, the impact of this circumvention is limited, as multilateral rules of private international law will remain applicable in determining the applicable liability regime – an issue that is not covered by the AI Act.

Third, ensuring a proper private enforcement of the provisions of the AI Act in cases involving third-state defendants would require rules on jurisdiction that are tailored to the AI Act and its extraterritorial scope (see sect. 3.2).

Finally, Article 2(6) of the directive ensures that claims for damages can be brought by the injured party as well as persons that have succeeded in or have been subrogated into the injured party's rights. For example, in addition to the victim, heirs and insurance companies (by means of subrogation) will be able to initiate a claim for damages caused by AI systems. Moreover, the directive allows for collective redress, allowing victims of damage caused by AI systems to enforce their rights through representative actions.[89] From a private international law perspective, issues of subrogation and collective redress are not new.[90] Their inclusion in cases involving AI liability means that some of the existing issues regarding (especially) collective redress will be extended to cases involving AI. This for example includes potential problems relating to overlapping claims, which may not be fully addressed by the provisions on *lis pendens* and related actions that exist under the Brussels regime.[91]

### *4.2 Product Liability Directive*

The newly proposed Product Liability Directive repeals the Product Liability Directive of 1985 (Directive 85/374/EEC). The proposal lays down a strict liability regime for harm caused by defective products. In order to ensure that AI systems and AI-enabled goods are subject to the directive in the same way as non-technological products, the directive introduces several rules. First, it extends the notion of a 'product' to include AI systems and AI-enabled goods. This

88 Insofar as it concerns private international law. Surely, when it comes to issues of public (international) law, Art. 2(1) is relevant beyond issues of civil liability.

89 The directive, in Art. 6, amends the Annex to Directive (EU) 2020/1828 accordingly.

90 See e.g. A. Flessner & H.L.E. Verhagen, *Assignment in European Private International Law. Claims as Property and the European Commission's 'Rome I Proposal'*, Munich: Sellier European Law Publishers 2006; V. Behr, 'Rome I Regulation: A – Mostly – Unified Private International Law of Contractual Relationships within – Most – of the European Union', *Journal of Law and Commerce* (29/2) 2011, pp. 233 et seq.; P. Leupold, 'Private International Law and Cross-Border Collective Redress. A Legal Analysis of Jurisdiction, Applicable Law, Pendency, Recognition and Enforcement under the Representative Actions Directive 1828/2020', August 2022, available online at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-085_Private_International_Law_and_Cross-Border_Collective_Redress.pdf (accessed 26 January 2023); B. Hess, 'Reforming the Brussels Ibis Regulation. Perspectives and Prospects', Max Planck Institute Luxembourg for Procedural Law Research Paper Series, N° 2021(4), available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3895006 (accessed 31 May 2023).

91 Rb. Amsterdam [District Court of Amsterdam] 5 February 2020, ECLI:NL:RBAMS:2020:555, *NIPR* 2020-241; N. Touw, 'Conference Report: The Netherlands: a forum conveniens for collective redress?', *NIPR* 2021, pp. 53-67; Leupold 2022 (*supra* note 90); Hess 2021 (*supra* note 90).

means that those harmed by a defective AI have recourse to compensation without having to prove the manufacturer's fault.[92] Second, the proposal ensures that software manufacturers and providers of digital services that affect how the product works – such as navigation services for self-driving vehicles – can be held liable equally to hardware manufacturers. It also ensures that manufacturers can be held liable for changes that they make to products that are already placed on the market, when such changes are the result of software updates or machine learning. Finally, it aims to lessen the burden of proof in complex cases, including those involving harm caused by defective AI systems, when products fail to comply with safety requirements.

#### 4.2.1 Private international law impact

Although the Product Liability Directive does not include any provisions on the conflict of laws, the extension of the notion of product to include AI systems and AI-enabled goods raises some questions of scope and definition in private international law. The Rome II Regulation on the law applicable to non-contractual obligations contains a special provision on product liability in Article 5. Under Article 5, the definition of 'product' is tied to the Product Liability Directive.[93] As such, the extended notion of product – to include AI systems and AI-enabled goods – will equally apply to Article 5 Rome II. As a result, any claim against the manufacturer or provider of a defective AI system[94] is subject to Article 5 Rome II. In some EU Member States, like the Netherlands, the 1973 Hague Product Liability Convention takes precedence over the Rome II Regulation.[95] Whether liability for damage caused by defective AI systems is included under this Convention[96] is not fully clear. In accordance with Article 1(1) the Convention determines 'the law applicable to the liability of the manufacturers and other persons specified in Article 3 for damage caused by a product'. This provision is to be read in conjunction with Article 2, which, in paragraph a, provides a definition of 'product'. Accordingly, a product includes natural and industrial products, whether raw or manufactured and whether movable or immovable. This broad definition is understood to include defective raw materials as well as liquids and gases and applies to finished products as well as component parts.[97] The definition does not, however, make any reference – direct or indirect – to intangibles, such as software or AI. This is not surprising given the (state of technological developments at the) time when the Convention was concluded. Yet the fact that the Convention was not drafted with AI in mind should not automatically disqualify its application in cases involving liability arising from dam-

92 Explanatory Memorandum, COM(2022) 495 (*supra* note 11), para. 1.3.

93 Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations ('Rome II'), COM(2003) 427 final, p. 13; F. Ibili, *GS Onrechtmatige daad* [*Green Series on Wrongful Acts*], Art. 5 Rome II, note 3.

94 Recital 12 Proposed Product Liability Directive equates the provider of an AI system to a manufacturer.

95 Art. 28 Rome II Regulation.

96 Convention of 2 October 1973 on the Law Applicable to Products Liability.

97 Asser/Kramer & Verhagen 10-III 2022/1086; W.L.M. Reese, *Convention on the Law Applicable to Products Liability. Explanatory Report*, HccH 1974 (hereafter: Reese Report), available online at: https://assets.hcch.net/docs/d842b133-cf76-480c-9cc8-631439b2a4b2.pdf (accessed 26 May 2023), p. 14. Compared to the Product Liability Directive, the Convention uses a broader definition of a product. See: H. Duintjer Tebbens & M. Zilinsky, *Productaansprakelijkheid* [*Product Liability*], Apeldoorn: Maklu 2009, p. 97.

age caused by defective AI systems. The Explanatory Memorandum to the Convention, known as the Reese Report, first clarifies that the Convention is intended to cover all products.[98] It then goes on to expand this clarification to 'all products that have been manufactured or in any way changed by the hand of man'.[99] The latter part of this addition may be problematic when it comes to AI as these systems generally possess the ability to reason, make predictions and/or adapt their behaviour on the basis of past experience without any human intervention. Still AIs are – *ab initio* – created by man setting specific parameters. It would thus be in the spirit of the Convention to include cases involving liability for damage caused by AI systems or AI-enabled goods.

## 5. Sectoral safety regulations

As a final element of the AI legislative package, the European Commission has proposed a revision of the sectoral safety regulations, such as the Machinery Directive and the General Product Safety Directive. The latter two proposals will be discussed in the following sections.

### *5.1 Machinery Directive*

As part of the AI package, the European Commission presented a Machinery Regulation in April 2021.[100] This Regulation will revise the existing Machinery Directive in order to address the emerging risks and challenges posed by new technologies. The Regulation is intended to ensure that machinery is safe by introducing requirements for its design and construction.[101] In doing so, it considers the interaction between machinery components and AI systems. The Regulation addresses both industrial machinery and consumer machinery products. In essence, the aim of the Regulation is fourfold: it seeks to (1) ensure that machines are safe and increase users' trust in new technologies, (2) reduce administrative burdens and costs of manufacturers, (3) foster legal certainty, and (4) establish more effective market surveillance.[102]

On 15 December 2022, the European Parliament and the Council of the European Union reached a political agreement on the Regulation. Surprisingly, the compromise text of the Regulation has dispensed with any link between the Regulation and the AI Act.[103] Moreover, the agreed text deletes any reference to 'AI systems'. Instead, the term 'AI system' is replaced

98 Reese Report 1974 (see note 97), p. 9.

99 Reese Report 1974 (see note 97), p. 14.

100 COM(2021) 202 final (*supra* note 12).

101 See Art. 1 Draft Machinery Regulation (compromise text).

102 European Commission Press Release, 'Commission welcomes political agreement on new rules to ensure the safety of machinery and robots', 15 December 2022, available online at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7741; Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on machinery 2021/0105 (COD), Compromise Text, 25 January 2023, available online at: https://data.consilium.europa.eu/doc/document/ST-5617-2023-INIT/en/pdf (both accessed 26 May 2023).

103 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on machinery 2021/0105 (COD), Compromise Text, 25 January 2023, available online at: https://data.consilium.europa.eu/doc/document/ST-5617-2023-INIT/en/pdf (accessed 26 May 2023).

by 'self-evolving behaviour using machine learning approaches', which seems to refer to the machine-learning capabilities of AI systems. As such, despite the removal of the term, the Machinery Regulation still covers AI systems. For example, it requires a conformity assessment for machinery that uses AI to ensure safety functions.[104] Thus, removing the link with the AI Act (and excluding the use of the term AI system) is unfortunate, as it may lead to incoherence between the AI component of the Machinery Regulation and the AI Act.[105]

#### 5.1.1 Private international law impact

The Machinery Regulation is intended to apply to all machinery and related products made available or put into service on the EU market.[106] It is primarily a public law instrument that contains market entry requirements[107] and introduces rules on free movement[108] as well as rules on Union market surveillance.[109] It does not confer any direct rights on individuals (consumers or professionals) or include any rules on civil liability. As such, the private international law impact of the instrument is limited.

### *5.2 General Product Safety Directive*

On 30 June 2021, the European Commission adopted a proposal for a General Product Safety Regulation.[110] This Regulation will replace the existing General Product Safety Directive and address the product safety challenges of emerging technologies – such as AI and connected devices – and online sales. In doing so, it *inter alia* creates obligations for online marketplaces and introduces a single market surveillance regime for consumer products. In addition, it extends the recall rules, includes consumer remedies and requires the Member States to lay down penalties for infringements. When it comes to AI, the proposal intends to provide a safety net for products and risks to the health and safety of consumers that do not fall within the scope of application of the AI Act.[111]

The proposal contains several provisions that are especially tailored to AI. This starts with the definition of product in Article 3(1). This broad definition includes 'any item, interconnected or not to other items (…) which is intended for consumers or can, under reasonably foreseeable conditions, be used by consumers even if not intended for them'. As such, the definition of product appears to cover standalone AIs as well as AIs that are connected to other items, such

104 Art. 21 and Annex I, Part A, no. 24 Draft Machinery Regulation (compromise text).

105 The risk of incoherence was already addressed by the European Parliament in its draft resolution on the proposal for a Machinery Regulation, see: Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on machinery products (COM(2021)0202 – C9-0145/2021 – 2021/0105(COD)), Recital 19, available online at: https://www.europarl.europa.eu/doceo/document/A-9-2022-0141_EN.html (accessed 26 May 2023).

106 See Art. 1, Art. 3(11) and Art. 3(12) Draft Machinery Regulation (compromise text).

107 See e.g. Chapters II and III Draft Machinery Regulation (compromise text).

108 See Art. 4 Draft Machinery Regulation (compromise text).

109 See Chapter VI Draft Machinery Regulation (compromise text).

110 COM(2021) 346 final (*supra* note 13).

111 Explanatory Memorandum, COM(2021) 346 final (*supra* note 13), para. 1.

as an AI connected to care robots.[112] In accordance with Article 5, economic operators are only allowed to place – or make available – safe products on the Union market. In assessing whether a product is safe, the evolving, learning and predictive functionalities of a product should be taken into account.[113] This assessment aspect relates directly to the special characteristics of AI systems. In essence, the proposed Regulation seeks to ensure the safety of consumer products placed on the European market – which extends to AI systems and AI-enabled items.

#### 5.2.1 Private international law impact

The proposed Regulation lays down specific substantive law rules, including consumer rights,[114] and does not contain any express conflict of laws provisions. Still, the scope of the Regulation gives rise to some interesting thoughts. Substantively, the Regulation 'lays down essential rules on the safety of consumer products placed or made available on the market'.[115] Which market this entails is not apparent from Article 1, which provides the substantive scope of the Regulation. Article 2, entitled 'scope', does not lay down any territorial delineation. Instead, the term 'market' is described as the 'Union market' by the definitions of 'making available on the market' and 'placing on the market' provided in Article 3.[116] From its phrasing, which is in line with the definition in other harmonised EU legislation,[117] the reference to the Union market appears to be intended as an internal market consideration, rather than an express unilateral scope rule that is to impact private international law. On the other hand, the Regulation intends to be applicable whenever products are placed or made available on the Union market. Such territorial application might conflict with the result of the conflict of laws reference. Since the Regulation does include an express conflict of laws provision, it is difficult to say whether the scope of the Regulation counts as a Community conflict of laws provision that takes precedence over the Rome I[118] and the Rome II Regulations.[119] However, an answer to a possible conflict between the General Product Safety Regulation and the Rome Regulations appears to lie in the recitals to the latter Regulations. In accordance with Recital 40 Rome I Regulation[120] and Recital 35 Rome II Regulation, those Regulations do not prejudice the application of instruments that are 'designed to contribute to the proper functioning of the internal market in so far as they

112 Cf. European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)), *OJ* 2020, C 449/37; E. Fosch Villaronga & T. Mahler, 'Cybersecurity, safety and robots: strengthening the link between cybersecurity and safety in the context of care robots', *Computer Law And Security Review* 2021, pp. 1-13; D. Giansanti & R. Alfio Gulino, 'The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives', *Healthcare* 2021, 9, 1653, para. 4.1.

113 Art. 7(1)(i) Proposed General Product Safety Regulation.

114 See e.g. Art. 35 Proposed General Product Safety Regulation.

115 Art. 1 Proposed General Product Safety Regulation.

116 Art. 3(6) and Art. 3(7) Proposed General Product Safety Regulation.

117 See Commission notice, 'The "Blue Guide" on the implementation of EU product rules 2022', *OJ* 2022, C 247, pp. 19 et seq.

118 Art. 23 Rome I Regulation.

119 Art. 27 Rome II Regulation.

120 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), *OJ* 2008, L 177/6.

cannot be applied in conjunction with the law designated by the rules' of these Regulations. As such, it appears that the provisions of the General Product Safety Regulation take precedence over the resulting conflict of laws reference in the event of a conflict.

Article 4 contains a special provision for distance sales. In accordance with this provision 'products offered for sale online or through other means of distance shall be made available on the market if the offer is targeted at consumers in the Union'. An offer for sale is considered to target EU consumers 'if the relevant economic operator directs, by any means, its activities to one or several Member State(s)'. In determining whether an economic operator directs its activities at consumers within the EU, the Article provides a non-exhaustive list of criteria to be taken into account. This list consists of (a) the use of an official language or currency of the Member States, (b) a domain name registered in one of the Member States, and (c) the geographical areas to which the products can be dispatched. The wording of Article 4 bears great similarity to Article 17(1)(c) Brussels Ia Regulation and Article 6 Rome I Regulation, which require a professional to direct its activities at a (Member) State or several (Member) States, including that (Member) State,[121] in order for the consumer protective provisions to apply. Moreover, the non-exhaustive list provided in Article 4 closely resembles the *Pammer/Alpenhof* test[122] established by the Court of Justice of the European Union (CJEU) within the confines of the Brussels regime. In *Pammer/Alpenhof* the CJEU addressed the interpretation of the 'directing at' or 'targeting' criterion. In this judgment, the Court ruled that the mere accessibility of a website in other Member States does not lead to the conclusion that the professional directs his activities at the consumer's domicile.[123] The will of the professional is decisive in this context. What is required is that he has manifested his intention to enter into commercial relations with consumers in (*inter alia*) the domicile of the relevant consumer.[124] In order to establish this intention, it is necessary to examine whether there were indications before the conclusion of the contract that the professional intended to trade with consumers domiciled in other Member States, including the one where the consumer is domiciled.[125] To facilitate this examination the CJEU presented a non-exhaustive list of factors that may indicate whether the professional's activity is directed at the consumer's domicile.[126] These included, *inter alia*, the international character of the activity, the language or currency used, and the use of a top-level domain name other than that of the Member State where the professional is established.[127]

Whereas the 'directing at' approach and the *Pammer/Alpenhof* test are established parts of private international law, both were absent from the earlier General Product Safety Directive. In addition, their inclusion remains undiscussed in the Explanatory Memorandum to the Proposed General Product Safety Regulation. In Article 4 of the proposed Regulation, the European legislator appears to have borrowed from private international law, largely aligning

121 Given the universal formal scope (Art. 2 Rome I) of the Rome I Regulation, Art. 6 Rome I Regulation refers to a country instead of a Member State.

122 CJEU 7 December 2010, Joined Cases C-585/08 and C-144/09, ECLI:EU:C:2010:740, *NIPR* 2011-78 (*Pammer/Alpenhof*).

123 Ibid., para. 69.

124 Ibid., para. 75.

125 Ibid., para. 76.

126 Ibid., para. 83.

127 Ibid., paras. 83-84.

the application of the Regulation in cases of distance sales with the consumer definition in Article 17(1)(c) Brussels Ia and Article 6 Rome I Regulation.

## 6. AI in the existing conflict of laws framework

In the absence of any specific conflict of laws provisions in the proposed legislative package on AI, any claim relating to harm caused by AI befalls the existing rules of private international law. Such claims are not subject to a single private international law instrument or reference category. It is the type of claim and the underlying legal relationship combined with the existing factual circumstances that determine the proper conflict of laws category in each case. When it comes to AI, these factual circumstances relate, for example, to the nature of the AI system and the resulting harm. Whereas claims relating to AI may either be contractual or non-contractual in nature, this article, in line with the EU's legislative package on AI, primarily addresses non-contractual harm.

There are various ways in which an AI system may – intentionally or unintentionally – cause harm.[128] The primary example is the situation in which an AI fails to do what it is designed to do, e.g. due to faulty updates, software malfunctions, false input or undesired learned behaviour. As a result, an AI may for example provide a false medical diagnosis,[129] provide incorrect financial advice,[130] violate someone's privacy[131] or infringe upon someone's intellectual property.[132] In other instances, an AI system may have the intention to cause damage, for example, when it is used for tailored phishing – the fraudulent practice of sending messages claiming to be from reputable companies in order to induce parties to reveal e.g. passwords and credit card numbers – or to produce fake news.[133]

---

128 See e.g. Lein et al. 2021, pp. 66-69 (*supra* note 71).

129 See e.g. T. Makino et al., 'Differences between human and machine perception in medical diagnosis', *Scientific Reports* 2022, 12:6877; A.J. DeGrave et al., 'AI for radiographic COVID-19 detection selects shortcuts over signal', *Nature Machine Intelligence* 2021, pp. 610-619.

130 See e.g. J. Lee, 'Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry', *European Business Organization Law Review* 2020, pp. 731-757; G. Northey et al., 'Man vs machine: how artificial intelligence in banking influences consumer belief in financial advice', *International Journal of Bank Marketing* 2022, pp. 1182-1199.

131 See e.g. D. Milmo, 'Italy's privacy watchdog bans ChatGPT over data breach concerns', *The Guardian*, 1 April 2023, available online at: https://www.theguardian.com/technology/2023/mar/31/italy-privacy-watchdog-bans-chatgpt-over-data-breach-concerns (accessed 26 May 2023); K. Manheim & L. Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy', *Yale Journal of Law and Technology* 2019, pp. 106 et seq.

132 C.R. Davies, 'An evolutionary step in intellectual property rights – Artificial intelligence and intellectual property', *Computer Law & Security Review* 2011, pp. 601-619.

133 See e.g. M. Caldwell et al., 'AI-enabled future crime', *Crime Science* 2020, pp. 9-14; T.C. Kind et al., 'Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions', *Science and Engineering Ethics* 2020, pp. 89-120; T.F. Blauth et al., 'Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI', *IEEE Access* 2022, pp. 77110-77122; P. Yeoh, 'Artificial intelligence: accelerator or panacea for financial crime?', *Journal of Financial Crime* 2019, pp. 634-646.

### *6.1 Rome II Regulation*

The applicable law to non-contractual obligations is determined on the basis of the Rome II Regulation.[134] In situations involving damage caused by AI systems, the application of the Rome II Regulation mostly gives rise to familiar problems that are complicated by the virtual setting in which AI systems tend to operate. Yet this complication is mitigated by the fact that the Rome II Regulation tends to favour the *locus damni* over the *locus actus*.[135] As such, locating the *locus actus* as the place where the event giving rise to the damage occurs (e.g. by locating the AI itself, the place where it made a faulty decision or where it malfunctioned) is of little relevance.[136] Instead, one must locate the place where the direct damage occurs (*locus damni*). In many cases an AI system will cause actual damage that is sustained by a real-world person. In such cases, the damage is at least tangentially connected to a specific country. In essence, the application of the Rome II Regulation causes some problems that are not unique to AI but stem from whether the damage occurs in a physical or virtual setting.

#### 6.1.1 Scope

Apart from some exceptions, the majority of cases involving liability arising from AI systems fall within the substantive scope of the Rome II Regulation. These exceptions include (1) liability arising out of state acts and omissions in the exercise of state authority[137] and (2) violations of privacy and rights relating to personality, including defamation.[138] As such, the use of AI for military operations or situations where an AI violates a person's privacy are subject to national conflict of laws rules. The Netherlands remits such issues to the Rome II Regulation by reason of Article 10:159 of the Dutch Civil Code (DCC). Obligations arising from the exercise of Dutch public authority are however subject to Dutch law.[139]

#### 6.1.2 General rule

As a general rule, the Rome II Regulation applies the law of the country where the damage occurs (*locus damni*).[140] Locating this damage will be relatively easy in situations where AI systems cause physical damage, e.g. when a self-driving vehicle causes a traffic accident. This may be different where harm is caused in a virtual setting, e.g. where an AI provides false investment advice or causes damage to a person's reputation, e.g. by creating deep fakes. The first example

134 Art. 1 Rome II Regulation.

135 See Recitals 15 and 16 Rome II Regulation. Cf. BeckOK BGB/Spickhoff VO (EG) 864/2007 Art. 4 Rn. 40, 41, which offers some specific insights in relation to damage caused online.

136 There are some exceptions, e.g. Art. 6 Rome II on environmental damage under which the claimant has the choice to initiate a claim on the basis of the laws of the *locus actus* or the laws of the *locus damni*.

137 Art. 1(1) Rome II Regulation.

138 Art. 1(2)(g) Rome II Regulation.

139 See Art. 10:159 Dutch Civil Code. As such, the question whether the State of the Netherlands is liable for damage caused by the use of AI for military operations is subject to Dutch law.

140 Art. 4(1) Rome II Regulation. The law chosen by the parties in accordance with Art. 14 Rome II takes precedence over this provision.

gives rise to questions that typically occur in cases of pure financial loss. Does the loss occur at the place where the investment is made?[141] Is it sustained at the place where the victim has his bank account?[142] Or might it be tied to the victim's habitual residence or centre of interests?[143]

Although the second example falls outside the scope of the Rome II Regulation, the Netherlands applies Article 4 Rome II to these scenarios by reason of Article 10:159 DCC. The difficulty in applying Article 4 in the context of online defamation is that damage is caused by content that is available on a worldwide basis. As such, damage may occur in multiple countries, resulting in the application of a patchwork of different laws. This mosaic approach[144] has been rejected by the Dutch courts.[145] Instead, they apply the centre of interests approach developed by the CJEU in *eDate/Martinez*.[146] Accordingly, the law that is applicable to a claim for damages resulting from the online infringement of personality rights or a violation of privacy is wholly subject to the laws at the centre of interest of the alleged victim.

The most difficult issue in localising the damage occurs in situations where an AI causes damage to virtual assets, e.g. when it harms another AI or when it is involved in the theft of cryptocurrency. In such cases, the asset itself has no real-world component, nor is it stored at any one location. For example, AIs are generally not stored on a single server, whereas cryptocurrencies are frequently registered on a blockchain that is stored on a multitude of *nodes* (computers) that can be located anywhere in the world. In such cases, one might consider seeking a connection to the domicile or centre of interest of the alleged victim.[147] Although these places are generally not considered to be the most suitable connecting factors when establishing the location of the damage,[148] such a connection seems appropriate in cases involving damage

---

141 Cf. BeckOGK/Rühl Rom II-VO Art. 4 Rn. 68;

142 CJEU 28 January 2015, Case C-375/13, ECLI:EU:C:2015:37, *NIPR* 2015-50 (*Kolassa)*; BeckOK BGB/Spickhoff, 65. Ed. 1.5.2022, VO (EG) 864/2007 Art. 4 Rn. 7.

143 See K. Siehr, 'Geldwäsche im IPR – Ein Anknüpfungssystem für Vermögensdelikte nach der Rom II-VO', *IPRax* 2009, p. 436; BeckOK BGB/Spickhoff, 65. Ed. 1.5.2022, VO (EG) 864/2007 Art. 4 Rn. 7.

144 See e.g. ECJ 7 March 1995, C-68/93, ECLI:EU:C:1995:61, *NIPR* 1995-533 (*Shevill e.a./Presse Alliance*); CJEU 21 December 2021, Case C-251/20, ECLI:EU:C:2021:1036, *NIPR* 2022-117 (*Gtflix Tv/DR*); T. Lutzi, 'Internet cases in EU private international law – developing a coherent approach', *International & Comparative Law Quarterly* 2017, pp. 687-721; M.H. ten Wolde, 'De plaats van het Erfolgsort in het forum delicti van het EEX. Is de puzzel gelegd?' ['The place where the damage occurred in the forum delicti of the Brussels I Regulation. Has the puzzle been set?'], *NIPR* 2020, pp. 251-275; Asser/Kramer & Verhagen 10-III 2022/1000:1000 Meervoudige locus: mozaïek-benadering [A multitude of loci: a mosaic approach].

145 *Hoge Raad* [Netherlands Supreme Court] 3 June 2016, ECLI:NL:HR:2016:1054, *NIPR* 2016-278 (*Dahabshiil*); Asser/Kramer & Verhagen 10-III 2022/1001:1001 Onrechtmatige daad via online content [A wrongful act via online content].

146 CJEU 25 October 2011, Joined Cases C-509/09 and C-161/1, ECLI:EU:C:2011:685, *NIPR* 2011-475 (*eDate/Martinez*), paras. 48-52.

147 See e.g. CJEU 19 April 2012, Case C-523/10, ECLI:EU:C:2012:220, *NIPR* 2012-350 (*Wintersteiger*).

148 CJEU 10 June 2004, Case C-168/02, ECLI:EU:C:2004:364, *NIPR* 2004-249 (*Kronhofer*). Cf. M.H. ten Wolde, *Handboek international privaatrecht* [*Handbook on private international law*], Zuthpen: Uitgeverij Paris 2021, p. 327; M. Lehmann 'Internationales Privat- und Zivilprozessrecht', in: S. Omlor & M. Link (eds.), *Kryptowährungen und Token*, Frankfurt am Main: Deutscher Fachverlag, Fachmedien Recht und Wirtschaft 2021, p. 246; M. Lehmann & F. Krysa, 'Blockchain, Smart Contracts und Token aus der Sicht des (Internationalen) Privatrechts', *Bonner Rechtsjournal* 2019, p. 96; MüKoBGB/Lehmann, 8. Aufl. 2021,

to virtual assets.[149] A justification for such a connection stems from the fact that the unique characteristics of such assets preclude locating the damage at another location.[150]

### 6.1.3 Special provisions

The application of the general rule of Article 4 Rome II does not cause any problems that are unique to AI. The same holds true for the specific provisions of the Regulation, such as the rules on product liability and intellectual property infringements. Article 5 Rome II includes a complicated reference system for product liability. Barring a common habitual residence, the Article seeks a connection to the place where the product was marketed, if that place coincides with (a) the habitual residence of the victim or, failing that, (b) the country in which the product was acquired or, failing that, (c) the country where the damage occurs. However, the law of the person claimed to be liable applies if he could not reasonably foresee marketing in the countries referred to under (a), (b) and (c). Finally, Article 5(2) provides an escape clause in the event of a manifestly more closer connection with another country. In general, establishing whether an AI-related product is marketed in a specific country is subject to the same difficulties as the marketing of other products. AI-specific difficulties may however arise in relation to the foreseeability criterion. After all, an AI might independently decide, due to its machine-learning capabilities, to market a product in a particular country.[151] Yet, even where that is the case, the manufacturer may have foreseen such marketing given the global nature in which AIs operate. Moreover, a manufacturer could have introduced limitations, e.g. as to language or geographical location in the AI's code, in order to avoid marketing in specific countries.

Issues of intellectual property infringement are covered by Article 8 Rome II. In situations where an AI infringes upon someone's intellectual property, the law of the country for which protection is claimed generally applies. This is different for unitary Community intellectual property rights; these are governed by the relevant Community instrument. Yet, where the case involves a question that is not governed by this instrument, the law of the country in which the act of infringement was committed will apply. Although issues of AI do not create any specific problems under Article 8, locating the place where the infringement was committed

---

Internationales Finanzmarktprivatrecht, Rn. 605; A. Held & M. Lehmann, 'Hacked crypto-accounts, the English tort of breach of confidence and localising financial loss under Rome II', *Butterworths Journal of International Banking and Financial Law* 2021, p. 708. Cf. Asser/Kramer & Verhagen 10-III 2022/989 who feel that applying the law of the domicile of the alleged victim is undesirable in cases of pure financial loss.

149 Cf. K.C. Henckel, 'Cryptovaluta in het conflictenrecht: een verkenning' ['Cryptocurrency in private international law: an exploration'], *NIPR* 2022, pp. 25-26; Lehmann 2021, p. 246 (*supra* note 148); Lehmann & Krysa 2019, p. 96 (*supra* note 148); MüKoBGB/Lehmann, 8. Aufl. 2021, Internationales Finanzmarktprivatrecht, Rn. 605; *Fetch.AI Ltd v. Persons Unknown* [2021] EWHC 2254 (Comm).

150 Cf. CJEU 28 January 2015, Case C-375/13, ECLI:EU:C:2015:37, *NIPR* 2015-50 (*Kolassa*); Henckel 2022, pp. 25-26 (*supra* note 149); Lehmann 2021, p. 246 (*supra* note 148); Lehmann & Krysa 2019, p. 96 (*supra* note 148); M. Schellekens et al., *Blockchain en het recht. Een verkenning van de reguleringsbehoefte* (WODC-rapport) [*Blockchains and the law. Exploring the need for regulation*], Tilburg: Tilburg University 2019, p. 60. Also see: F. Guillaume, 'Aspects of private international law related to blockchain transactions', in: D. Kraus e.a., *Blockchains, smart contracts, decentralised autonomous organisations and the law*, Cheltenham: Edward Elgar Publishing 2019, pp. 64-65.

151 See Lein et al. 2021, p. 81 (*supra* note 71); Cappiello 2022, pp. 193-197 (*supra* note 19).

may prove difficult in the event of an infringement that occurs solely in a virtual setting.[152] Here, one might consider seeking a connection to the case law of the CJEU in cases involving online trademark infringements under the Brussels regime. In *Wintersteiger* the Court ruled that the place of e.g. a server cannot, by reason of its uncertain location, be considered the place where the event giving rise to the damage occurred.[153] Instead, the Court sought a connection to the place of establishment of the person who decides to initiate the infringement process.[154] In cases involving AI such application may be difficult as AIs frequently create works using automated decision-making. These AIs most often operate in a virtual setting and do not have a real-world place of establishment. This is different for the user/operator or the manufacturer/programmer of the AI. One may wonder whether these persons may be responsible for initiating the infringement process, e.g. by allowing the AI to 'borrow' from existing works; seeking a connection to their place of establishment would solve any problems of localisation.

### 6.1.4 Relationship to other instruments

Special Community conflict of laws provisions operate as a *lex specialis* to the Rome II Regulation.[155] As such, the AI Act may for example take precedence over the Rome II Regulation by reason of the express scope rule contained in Article 2 of the Act (see above, sect. 3).

Pursuant to Article 28 Rome II, the Regulation does not affect the application of existing international conventions to which one or more Member States are a party. This notably includes the Hague Convention on the Law Applicable to Traffic Accidents[156] and the Hague Convention on the Law Applicable to Products Liability. Both Conventions apply in multiple EU Member States, including the Netherlands. As such, the law that is applicable to two important aspects of tort remains fragmented throughout the EU,[157] an issue that has been criticised on many occasions.[158] Despite this criticism and the proper functioning of the Rome II Regulation for close to 15 years, none of the participating Member States has been inclined to withdraw from the Conventions.[159]

---

152 Lein et al. 2021, p. 83 (*supra* note 71).

153 CJEU 19 April 2012, Case C-523/10, ECLI:EU:C:2012:220 (*Wintersteiger*), para. 36.

154 CJEU 19 April 2012, Case C-523/10, ECLI:EU:C:2012:220 (*Wintersteiger*), paras. 37-38.

155 Art. 27 Rome II Regulation.

156 Convention of 4 May 1971 on the Law Applicable to Traffic Accidents.

157 See Recital 36 Rome II Regulation, which allows this fragmentation in honour of the international commitments of the Member States.

158 See e.g. Von Hein 2022, pp. 215-216 (*supra* note 37); Kadner Graziano 2016, pp. 21-27 (*supra* note 3); T. Kadner Graziano, 'The Rome II Regulation and the Hague Conventions on Traffic Accidents and Product Liability – Interaction, Conflicts and future perspectives', *NIPR* 2008, pp. 425-429; also see M. Hellner, 'The Relationship between the Rome II Regulation and the 1973 Hague Convention', *Oslo Law Review* 2019, pp. 72-74.

159 See: Von Hein 2022, p. 215 (*supra* note 37); A Staudinger, 'Das Konkurrenzverhältnis zwischen dem Haager Straßenverkehrsübereinkommen und der Rom IIVO', in: D. Baetge et al., *Die richtige Ordnung, Festschrift für Jan Kropholler zum 70. Geburtstag*, Tübingen: Mohr Siebeck 2008, p. 671.

### 6.2 Hague Traffic Accidents Convention

The Hague Traffic Accidents Convention determines the applicable law to non-contractual liability arising from traffic accidents. Among its Contracting States are thirteen EU Member States.[160] The Convention does not apply to the liability of the manufacturer of a vehicle; it primarily covers actions against the owner.[161] The Convention applies to owners of self-driving vehicles in the same way as it does to owners of any other vehicle. The application of the Convention does not raise any issues that are specific to AI. As a general rule, the law of the place where the accident occurred applies.[162] In exception to the general rule, the law of the state of registration of the vehicle applies in a number of situations, *inter alia* in cases of owner liability where only one vehicle is involved in the accident and the vehicle is not registered in the state where the accident occurred.[163]

### 6.3 Hague Products Liability Convention

The Hague Products Liability Convention applies in seven EU Member States.[164] Whether AI systems and AI-enabled goods are covered by the Convention is not fully clear. Yet, their inclusion would be in line with the spirit of the Convention, which intends to apply to liability arising from 'all products that have been manufactured or in any way changed by the hand of man' (see above, sect. 4.2.1).[165] Article 5 of the Convention provides the general rule.[166] In accordance with this provision the law of the state of habitual residence of the person directly suffering the damage applies, provided that that place coincides with (a) the principal place of

160 Austria, Belgium, Croatia, the Czech Republic, France, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Slovakia, Slovenia and Spain. In addition, it applies to the countries succeeding the former Socialist Federal Republic of Yugoslavia as well as Switzerland, Morocco, Belarus and the Ukraine. In the latter three countries, the Convention only applies between them and such Contracting States that have declared acceptance of their accession.

161 See Art. 2 Hague Traffic Accidents Convention; E.W. Essén, 'Convention on the law applicable to traffic accidents. Explanatory Report' (hereafter: the Essén Report), available online at: https://assets.hcch.net/docs/826ac363-4725-484a-9435-0f10802ba2b3.pdf (accessed 26 May 2023), pp. 11-13.

162 Art. 3 Hague Traffic Accidents Convention. The drafters of the Convention did not consider it necessary to devote specific attention to the location of the damage as they believed that the location of the tortious act, in cases of traffic accidents, almost always concurs with the place where the damage occurs. See: the Essén Report, pp. 13-14 (*supra* note 161).

163 See Arts. 4 and 5 Hague Traffic Accidents Convention; Vonken, *T&C Vermogensrecht*, commentaar op art. 4 Haags Verkeersongevallenverdrag [*Text and Commentary on the law of property*, commentary on Art. 4 Hague Traffic Accidents Convention]; Vonken, *T&C Vermogensrecht*, commentaar op art. 5 Haags Verkeersongevallenverdrag [*Text and Commentary on the law of property*, commentary on Art. 5 Hague Traffic Accidents Convention]; Kadner Graziano 2016, pp. 21-27 (*supra* note 3).

164 Croatia, Finland, France, Luxembourg, the Netherlands, Slovenia and Spain. In addition, it applies in Norway and the countries succeeding the former Socialist Federal Republic of Yugoslavia.

165 Reese Report 1974, p. 14 (see note 97).

166 According to its wording, Art. 5 prevails over Art. 4. It states: 'notwithstanding Article 4'. See: F. Ibili, *GS Onrechtmatige daad*, regeling Haags produktenaansprakelijkheidsverdrag [*Green Series on Wrongful Acts*, regulation under the Hague Products Liability Convention], note 7.

business of the person claimed to be liable, or (b) the place where the product was acquired by the person directly suffering damage. Under Article 4, the law of the place of injury applies, if that state is also (a) the place of habitual residence of the person directly suffering damage, or (b) the principal place of business of the person claimed to be liable, or (c) the place where the product was acquired by the person directly suffering damage. The majority of these connecting factors do not give rise to any problems when applied to cases involving AI. Still, determining the place of injury may be difficult in cases involving virtual damage.[167] After all, virtual damage is not tied to any particular territory. According to the Reese Report the term 'place of injury' refers to the 'place where the defendant's wrongful act had its first impact upon the person directly suffering damage.' As such, the term is given a broad interpretation. One may wonder whether this interpretation can be so broad that it extends to the place where the virtual damage has a real-world effect. In most cases, the latter place would equate to the habitual residence of the person sustaining damage.

## 7. Final remarks

Whilst AI systems operate in a global landscape, express provisions of private international law remain notably absent from the EU's AI package. From a conflict of laws perspective, this is hardly problematic since the existing mechanisms of private international law, such as the Rome II Regulation, tend to function well in relation to (damage caused by) AI systems. This is largely due to the fact that these instruments mostly utilise connecting factors that do not refer to the (location of the) AI itself. The specific characteristics of AI, such as its complexity, opacity and semi-autonomous behaviour, have little bearing on private international law. Yet, the virtual nature of AI and the damage that it causes may give rise to some problems of localisation. These problems are not unique to AI and may be solved by creating a legal fiction and seeking a connection to a real-world component.

A different situation exists with regard to the AI Act. The proposed Act and its accompanying civil liability regime fail to introduce rules on jurisdiction that are tailored to the extraterritorial scope of the Act. In doing so, the proposals fail to ensure proper private enforcement in cases against third-state providers, operators and users of AI systems. Since actions against third-state defendants fall outside the scope of the Brussels Ia Regulation, this may leave claimants without recourse to a Member State court. A proper private enforcement for all cases falling within the scope of the AI Act requires rules on access to justice. In finalising the proposed acts the European legislator should therefore take note of the existing EU rules on private international law, predominantly the Brussels Ia Regulation.

167 For more on the difficulty of localising damage in a virtual context see above, sect. 6.1.2.