L'IRCOCERVO
PRIMA RIVISTA ELETTRONICA ITALIANA DI METODOLOGIA GIURIDICA - TEORIA GENERALE DEL DIRITTO E DOTTRINA DELLO STATO
FIRST ITALIAN DIGITAL JOURNAL OF LEGAL METHODOLOGY - GENERAL THEORY OF LAW AND DOCTRINE OF THE STATE

Liability for Damage Caused to the Data Subject in the Event of GDPR Violation "by Artificial Intelligence": Between Legal Discrepancies and Policy Questions

Radosław Strugała

Uniwersytet Wrocławski

Abstract: **Liability for Damage Caused to the Data Subject in the Event of GDPR Violation "by Artificial Intelligence": Between Legal Discrepancies and Policy Questions**
The paper discusses the topic of liability for data breach by AI. It aims at tracing the reason of rare application of the article 82 of the GDPR and proposes predictions of how its application may change with the potential enactment of special liability regime for AI-inflicted damage. The paper offers insight into how such a regime may interplay with the GDPR by pointing out the risks linked to the potential overlap thereof and offering a way to remedy such risk.

Keywords: The GDPR, Personal Data, Artificial Intelligence, Data Breach.

Summary: 1. Introduction – 2. Legal Nature of Liability Under the Article 82 of the GDPR, the Preconditions to Liability – 3. GDPR Violations in the Course of Personal Data Processing by AI – 4. AI and Damage – 5. Damage Consequent Upon Data Breach and Damage Caused by AI – 6. Concluding Remarks: Policy Choices.

1. Introduction

The issue posed in the title remains on the margins of a lively discussion on both the legal aspects of the use of artificial intelligence and the protection of personal data.

When it comes to the latter, the discussion focuses mostly on the General Data Protection Regulation (GDPR) compliance. Much weight is given to the interpretation of the GDPR provisions aimed at establishing the content of controllers' and processors' duties in order to secure that personal data processing be in line with GDPR in individual cases. Undoubtedly this interpretation emerges to be more challenging where personal data is processed with the help of AI (or "by AI"). And the AI act coming into force adds to the complexity of the picture of the controllers' and processors' duties. Whereas as far as the legal consequences of GDPR non-compliance are concerned, public sanctions (administrative fines as provided in the article 83 of the GDPR) are in the centre of interest in the legal

writing. Hardly ever extended analysis is made in Academia concerning private law measures applicable in the case of GDPR violations, albeit the GDPR expressly provides for the private enforcement tool in the form of compensatory remedies (article 82 of the GDPR). This state of legal thought reflects the common perception of practical importance of public and private remedies available under the GDPR. While the administrative fines imposed by national supervisory authorities (be it *Il Garante per la Protezione dei Dati Personali*, *Prezes Urzędu Ochrony Danych Osobowych*, *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) are perceived as effective and thus become practically important, commonly applied sanctions of the GDPR infringements, the article 82 of the GDPR is rarely invoked to remedy GDPR violations.

As regards to the legal aspects of AI functioning, liability for damage caused by artificial intelligence (or by the use of AI systems) undoubtedly remains among the central issues discussed by the legal scholars. However, the focus in the discussion is primarily on "classic damage" being a consequence of the violation of traditionally recognised legally protected interests, such as life, health or property of the injured person. In the course of the debate the problem of damage resulting from the unlawful processing of personal data is hardly ever addressed, if it is touched upon at all. The same holds true for the legislative proposals that are successively presented by the EU institutions with aim to harmonise liability for damage caused by AI at the EU level. Thus far two such proposals were published, each given a different legal status as one was presented as a draft regulation (Draft Regulation)[1] and the other one was planned to be enacted in the form of respective directive (Draft Directive)[2]. None of these proposals expressly and directly relates to liability for damage caused by AI as a result of violation of the legal rules on processing of personal data. The preambles to the drafts also lack mentions of the issue clear enough to allow to ascertain whether including liability for losses consequent upon data infringement was the intention of the law maker proposing AI liability rules at hand.

The goal of this paper is to shed light on the neglected topic of liability in damages for data breach by AI. Particularly it purports to establish the reason for limited application of the article 82 of the GDPR (compensatory remedy offered therein) by data subjects who currently make such a rare use thereof. On top of it, it proposes predictions of how the fate of the article at scrutiny may change due to the development of AI technology and the increase of automated data processing and consequential proliferation of instances of data breach by AI. Looked at from this angle the problem tackled in this article appears to lie at the crossroads of the two sets of legal rules governing both personal data processing (like the GDPR) and

[1] Civil liability regime for artificial intelligence European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) (2021/C 404/05).
[2] 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.

liability for AI-inflicted losses yet to be enacted (i.e. draft legal rules proposed in the legislative proposals mentioned above). This paper offers insight into how the two sets of rules may interplay in the likely event of the above-mentioned or similar special rules on liability for AI becoming a binding law in the future. The juxtaposition of these sets of rules leads to questions of twofold nature. First, which of these legal rules are to be applied where damage is caused as a consequence to data breach by AI system. This is a question which lawyers would be forced to face if the above-mentioned legislative plans of introducing special regime of liability for AI came true. This is a rather technical question that the lawmaker could easily avoid by expressly deciding the relation of the above-mentioned legislative proposals on liability for AI and the article 82 of the GDPR. What is way more complex are the policy reasons underlying any such decision. One may even speculate that no decision as to the relation of the two sets of legal rules was expressly made, for no policy choices have been made thus far in the field. The ultimate goal of this paper is to try and formulate policy directions that should determine future decisions of the law maker. As it was underlined, the liability scheme provided for in the article 82 of the GDPR draws so far little attention in the legal writing. Thus, some preliminary observations about its legal nature and preconditions to liability should be made. Let it be the starting point of the further analysis.

2. Legal Nature of Liability Under the Article 82 of the GDPR, the Preconditions to Liability

According to the article 82 of the GDPR any person who has suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the controller or processor for the damage suffered. When talking about preconditions to liability in damages traditionally three are pointed out, namely: a loss or damage (be it monetary, non-monetary or both kinds of losses), an event defined in the piece of legislation imposing liability (the event that may trigger liability if it constitutes a cause of loss) and the causal link between this event and the items of loss incurred by the victim seeking compensation. The liability provided for in the article 82 of the GDPR is usually viewed as tortious liability (non-contractual liability)[3]. This follows that for this liability to arise all above-mentioned preconditions need to be met. This view is approved of by the CJEU in a judgement referred to as *Österreichische Post* case. The CJEU underlined that

> it is clear from the wording of that provision that the existence of 'damage' which has been 'suffered' constitutes one of the conditions for the right to

[3] See E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffré, Milano, 2019, p. 49.

> compensation laid down in that provision, as does the existence of an infringement of the GDPR and of a causal link between that damage and that infringement, those three conditions being cumulative[4].

3. GDPR Violations in the Course of Personal Data Processing by AI

As in the case of "traditional", non-automated personal data processing, data breach may well occur in the course of data processing by AI. The legal protection provided for in the GDPR is technologically neutral[5]. The way it imposes duties on controllers and processors follows the rights-based approach[6]. It means that the infringement of the GDPR can be ascribed to controllers or processors regardless of whether data processing contrary to the GDPR provisions was the performance of their own hands (where controllers or processors collected, recorded, organized, structured, stored, reviewed, used or disclosed personal data in an "analog" manner) or the result of the use of an AI system (working for the controller or processor). At the same time, the use of AI systems seems to bring about the hazard of new risks of the GDPR infringements that are inherent to this type of technology. A simple use of common Chatbots (which undoubtedly bear the hallmarks of AI), while interacting with data subjects (customers) may lead to instances of such data breach. For example, a GDPR violation could occur in the case of a Chatbot processing given personal data by using them as "training data" with the purpose of deep learning. A situation that should definitely be viewed as GDPR infringement is a likely scenario where the controller who makes use of a Chatbot obtains consent and provides the information clause only in respect to the main purpose of data processing, which is the possibility of establishing commercial contact and conducting communication, including answering questions addressed to the

[4] Judgment (Third Chamber) of 04/05/2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), case C-300/21.

[5] See recital 15 of the GDPR preamble, according to which "in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation". See also the article 4 (2) of the GDPR, which expressly provides that "processing [of personal data] means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[6] See L. Edwards, M. Veale, "Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for", in *Duke Law and Technology Review*, 16 (2019), pp. 16-84; O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015; R. Gellert, "On Risk, Balancing, and Data Protection: A Response to van der Sloot", in *European Data Protection Law Review*, 2 (2017), p. 185.

controller regarding the goods or services offered. According to one possible interpretation of the GDPR provisions, the use of collected personal data as a training data set does not require separate consent of the data subject, for the legal basis for this type of processing is constituted by the Article 6(1)(f) of the GDPR, which means that personal data processing is deemed necessary for the purposes of the legitimate interests pursued by the data controller. This approach was followed in a widely discussed case of a temporal ban on the processing of Italian users' personal data by OpenAI (i.e. the company launching ChatGPT) imposed by *Garante per la Protezione dei Dati Personali* (Italian national supervisory authority within the meaning of the GDPR). *Il Garante* rightly considered OpenAI to be data controller of personal data collected through websites or social media in order to be used for machine learning by ChatGPT. Initially, *il Garante* accused OpenAI of not having provided the users of ChatGPT (and therefore data subjects) with appropriate information about the processing of their data, and of having processed personal data without an appropriate legal basis. However, as a final chord of the dispute between *il Garante* and OpenAI, the former, after formulating guidelines regarding the company's information policy, allowed OpenAI to process personal data of Italian users pursuant to Art. 6(1) 1 letter f GDPR.

Even if we accept the reasoning of the Italian supervisory authority, the mere recognition of the data processing with aim to train the system within the framework of machine learning being the legitimate interest of the data controller (the Article 6(1)(f) of the GDPR), does not mean that the controller is exempt from the information duties. It is still the controller's duty under the GDPR to provide the data subject with information (information clause) on the legal basis of data processing and on "additional" purpose of the processing as training data (see Article 13(1)(c) of the GDPR[7]). In my view, some of the controllers, used to "traditional information clause content" and sometimes even not aware of the fact that the Chatbot used by them may collect personal data and use it as training data, will be prone to fail to fully comply with these information duties. Another possible case of GDPR violation in connection with the use of a Chatbot that can easily be thought of, is a scenario in which an entrepreneur makes use of a Chatbot or similar AI system to entrust the system with automated individual decision-making regarding their current or potential client, which would clearly be in violation of the Article 22 of the GDPR, as well as the Article 5 of the Artificial Intelligence Act.

[7] According to which, the controller shall provide the data subject with information about purposes of the processing as well as the legal basis for the processing. However, if specific personal data are collected for several different purposes, the controller is obliged to indicate all these purposes, and if data processing is carried out pursuant to Art. 6 section 1 letter f GDPR, the controller should also provide the data subject with information about the legitimate interest they pursue when processing data (see P. Barta, M. Kawecki, P. Litwiński, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 in 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). Commentary*, C.H. Beck 2021, pp. 226 ss.

To conclude, one can notice that automated personal data processing by AI not only does not mitigate the risk of GDPR infringement but can even broaden the potential areas of data breach. At first sight, it could lead to a conclusion that the increased number of cases of data processing by AI may render the article 82 of the GDPR more practical as more data subjects could decide to seek compensation under this provision for losses incurred in the process of AI processing their personal data. Whether this is an apt observation needs to be verified taking into account other preconditions to liability provided in the article 82 of the GDPR and the potential to meet them in case of personal data processing by AI.

4. AI and Damage

Damage or loss constitutes the inherent, necessary precondition to any type of liability in damages, be it tortious liability or liability for breach of contract. The same is true for the liability scheme as provided in the Article 82 of the GDPR. The provision at hand expressly renders liability dependent on the damage caused as a result of a violation of the GDPR provisions[8]. The wording of the Article 82 of the GDPR leaves no doubt that the liability may be triggered by the occurrence of both material or (and) non-material damage. Reported cases of article 82 application in disputes pending before national civil courts in the EU member states, even if not numerous, demonstrate that data subjects invoke the article 82 of the GDPR to seek compensation of non-monetary damage. Hardly ever it appears as legal basis in the context of monetary loss. This is probably due to the fact that personal data processing not in line with the GDPR has low potential to directly cause any material damage[9]. Contrary conclusion seems to be legitimate when it comes to non-monetary damage. In contrast to monetary damage, which is understood similarly in the majority of legal systems, the notion of non-monetary damage is given manifold meaning across EU Member States. The question of whether GDPR violation by AI may actually lead to non-monetary damage subject to compensation under the Article 82 depends, thus, on the way the concept of non-monetary damage is to be understood in this very provision. Ever since the GDPR got into force, there could be no doubt that the term "non-monetary damage" in the article 82 thereof should be interpreted autonomously, independently of the content of equivalent concepts in national laws of the Member States. It was thus rather clear, at least in Academia, that when interpreting the term no resort must be made to "national" non-monetary damage, e.g. within the meaning of the article 448 of the Polish Civil

[8] See Judgment (Third Chamber) of 04/05/2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), case C-300/21.

[9] However, such damage may certainly be caused indirectly – e.g. as a result of the leak of personal data originally collected by AI without the consent of the data subject, which is then used by a third party to obtain a loan.

Code, article 2059 of the Italian Civil Code or section 253 of BGB[10]. Quite recently this conclusion was clearly confirmed by the CJEU[11]. Regardless of the certainty as to the method by which the term "non-monetary damage" in the article 82 of the GDPR should be interpreted, the result of this interpretation remained highly uncertain for a very long time. This uncertainty seems to be one of the main reasons why the article 82 of the GDPR was so rarely invoked by data subjects.

Both in case law of national civil courts and in legal writing, three competing approaches to the interpretation of the term "non-monetary damage" in the article 82 of the GDPR could be distinguished. The most liberal of them assumed that non-monetary damage within the meaning of the Article 82 of the GDPR is constituted by the mere fact of the GDPR provisions being violated. Thus, according to this interpretation, each data breach vis-a-vis data subject equals their non-monetary damage by definition[12]. According to the alternative, dominant view (represented by the case law of German and Austrian courts), non-material damage giving rise to a claim for compensation under the Article 82 of the GDPR is a phenomenon separate from the GDPR infringement itself. This perspective holds, in a nutshell, that the non-material damage takes the form of negative feelings of the injured data subject. It is restrictive, however, as it limits the scope of the notion of non-monetary damage only to serious detrimental emotional effects of the GDPR violation. Mere stress, discomfort, or anxiety (because of the loss of control over one's own data) do not stand for non-material damage according to the interpretation referred to. For the non-material damage to occur, it requires that detrimental emotional effects of the GDPR violation be a consequence of social exclusion or humiliation, which constitutes "the minimis rule" or "a minimum

[10] R. Strugała, "RODO a odpowiedzialność odszkodowawcza, Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych", in *Monitor Prawniczy* 17 (2018), p. 915; A. Pązik, "Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy", in *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, 3 (2020), p. 133.

[11] See the Judgment (Third Chamber) of 04 May 2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), case C-300/21, which expressly undrelines that "the GDPR makes no reference to the law of the Member States as regards the meaning and scope of the terms set out in Article 82 of that regulation, in particular as regards the concepts of 'material or non-material damage' and of 'compensation for the damage suffered'. It follows that those terms must be regarded, for the purposes of the application of that regulation, as constituting autonomous concepts of EU law which must be interpreted in a uniform manner in all of the Member States".

[12] For example, the Court of Appeal for England and Wales in its judgment of 2 October 2019 (in the case of Lloyd v. Google, LLC [2019] EWCA Civ 1599). Although the decision was made before the so-called Brexit, on the basis of the "legal predecessor of the GDPR", i.e. Directive 95/46, it was later recognized in the scholarship as valid under the article 82 GDPR (see e.g. B. Van Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 3 (2016), p. 284).

threshold of seriousness"[13]. "The minimum threshold of seriousness" set by German courts resulted in a very limited scope of detriments that could be viewed as non-material damage under the article 82 – in fact it would amount to the effects of disclosing the injured party's sensitive data, if the interpretation at hand was accepted. The third, most balanced position as to the meaning of non-material damage, links this notion to negative feelings of the injured data subject, it does not require, however, any "minimum threshold of seriousness" to be met. This allows for the mere stress or discomfort due to the loss of control combined with the fear of their unauthorized use by a third party to be recognized as non-material damage, as referred to in Article 82 of the GDPR[14].

The interpretation of the concept of non-damage has only just begun to be clarified in the case law of the CJEU. In *Österreichische Post* case (in response to a question referred for a preliminary ruling by the Austrian Supreme Court), the CJEU expressed a position closest to the third approach mentioned above. It explained that the occurrence of non-monetary damage within the meaning of Article 82 of the GDPR must not be confused with the violation of the GDPR provisions, as the two elements stand for two separate preconditions to liability both being necessary to meet for the liability to arise. The CJEU underlined that in a compensation case the plaintiff is required to demonstrate the existence of negative (non-material) effects of a given GDPR infringement as a separate (from the GDPR violation itself) liability prerequisite. At the same time, it refused the view that for the liability to arise given effects need to be particularly significant – as significant as to reach the "minimum threshold of seriousness". The facts of the *Österreichische Post* case were strikingly similar to the circumstances of the very famous "Cambridge Analytica scandal" that exploded a few years ago in the US. The plaintiff was seeking compensation under the Article 82 of the GDPR against the Österreichische Post as an entity that, in violation of the GDPR, processed the personal data of its clients using specific algorithms in order to "profile" them for political purposes – with aim to get precise information on the political preferences of the clients and to direct to them selected campaign advertising materials of specific political parties matching the "profile" of the addressee. The plaintiff held that non-monetary damage that he allegedly incurred stemmed from the fact that political beliefs or sympathies were attributed to him that were inconsistent with his actual political affiliation. The plaintiff felt offended by the mere attribution of such political beliefs to him, and was also outraged by the fact that the company kept the information about his alleged preferences. He identified these feelings with non-monetary damage within the meaning of the Article 82 GDPR. The interpretation

[13] See e.g. the judgment of the regional court in Karlsruhe of 2 August 2019, O 26/19; the judgment of the District Court in Hamburg of 4 September 2020, 324 S 9/19; judgment of the District Court in Frankfurt am Main of 10 July 2020, 385 C 155/19.

[14] This interpretation was presented to the CJEU by the Supreme Administrative Court (Varhoven Administrativen Sad) of Bulgaria within the preliminary question procedure in the case C 340/21.

of this provision employed by the CJEU *Österreichische Post* case enables to conclude that such an identification may turn out legitimate.

The interpretative approach accepting non-monetary damage as separate precondition to liability, but rejecting the "minimum threshold of seriousness" was confirmed by the CJEU in the next judgment of December 14, 2023, in which the CJEU – referring to the content of recital 85 of the GDPR preamble – emphasized that a real fear of possible future misuse of personal data may amount to non-monetary damage. The Court noted that the existence of such a real fear should be decided in relation to the specific plaintiff and specific circumstances in which the GDPR violation occurred[15].

Despite such a reservation, it seems that the developing case law of the CJEU could constitute a breakthrough, encouraging potential plaintiffs to seek compensation protection under the article 82 of the GDPR more often. Irrespective of the way the CJEU approached the notion of the non-monetary damage, which is rather liberal, the very fact that the CJEU dwelled on it and expressed firm interpretative direction as to the notion will definitely reduce the uncertainty as to the actual content of the article 82 of the GDPR, and therefore also the degree of legal risk that has so far been associated with bringing actions based on this provision. It seems reasonable to ask whether the possible entry into force of further EU regulations, this time relating to liability for AI, would not mitigate this effect by introducing new legal uncertainty for data subjects to face whose data is processed in an automated manner – with an aid of AI (by AI).

5. Damage Consequent Upon Data Breach and Damage Caused by AI

As mentioned above, for some time now, analyses, studies, as well as specific legislative initiatives have been undertaken at the EU level regarding the liability for damage caused "by artificial intelligence". There are undoubtedly certain legal policy motives behind them, such as the desire to unify the legal rules governing this kind of liability throughout the EU, which could result in the EU's competitiveness in the field of artificial intelligence. There is no doubt that the way in which the legal rules governing liability for damage caused by AI are shaped may have an impact on the development of this technology. If they are excessively restrictive, their application will result in a chilling effect both in the area of innovation (when it comes to the responsibility of broadly understood technology producers) and the use of technology itself (when it comes to the rules of liability of the users).

However, the main reason behind taking up the problem of liability at hand at the EU level is that the liability rules currently in place in the majority of Member States may turn out to be ineffective in the event of the damage being "caused by

[15] See the CJEU Judgment of 14 December 2023, C340/21.

AI". This is the conclusion commonly drawn in the private law scholarship in relation to liability frameworks that are based on the principle of fault that would be applicable in the majority of Member States in the cases of AI causing damage. Legal systems providing for general strict liability of persons in control of things for damages caused by the use of these things are rather exceptional (see e.g. *la responsabilité du fait des choses* and *la responsabilità per cose in custodia* in the article 1242 of the French Civil Code and the article 2051 of the *Codice Civile*). Irrespective of whether as broad interpretation of such strict liability provisions is accepted as to include within the scope of their application losses caused by the operation of various types of new technologies (machines, robots or even the so called stand-alone AI software not embedded in any tangible hardware)[16], the strict liability would remain available for the injured persons in very limited number of Member States. In the major part of them for the injured party to seek compensation for losses caused by AI it would be necessary to identify the culpable behaviour of the AI user, owner or possessor and to establish a causal link between such behaviour and the damage caused by the specific functioning of AI.

In a world where human activity is replaced by the use of AI, tracing back the damage caused directly by the use of AI to any culpable human behaviour may be very challenging. The complexity of AI systems and limited knowledge into the way they operate from the perspective of the injured party (the so-called black box effect) gives rise to difficulties in linking specific action of AI that resulted in damage with the culpable behaviour of a person involved in the functioning of a given AI system. In the case of "intelligent machine" that caused damage as a result of a specific, unpredictable "behaviour" (e.g. in the case of a lawn mower that did not stop in time, injuring a toddler's hand), the injured party may meet enormous obstacle in determining whether the machine "behaved" in a harmful way because the software was defective from the beginning (e.g. the code was bugged, which presupposes an error, i.e. fault on the side of the system designer), because the device was fed with incorrect data in the process deep learning, either because it was not updated properly (which presupposes the user's fault) or because its physical elements (sensors, cameras, etc.) did not work properly (which would constitute the fault of the manufacturer of the device or its parts). Since in the majority of legal systems, in the fault liability schemes the burden of proving causality is placed on the injured party, in cases of AI-inflicted damage the victim is put under the risk of failing to meet the burden of proof and consequently of remaining not compensated for their damage.

This risk becomes even more significant when the proof of fault is taken into consideration. Regardless of how the concept of fault is defined in a given legal system, a common feature of fault liability is the need for the injured party (who

[16] As to this broad interpretation employed in the French law see European Parliamentary Research Service (ed. T. Evas), *Civil liability regime for Artificial Intelligence. European Added Value Assessmen*t, Brussels, 2020, p. 111; L. Archambault, L. Zimmermann, "Repairing damages caused by artificial intelligence: French law needs to evolve", in *Gaazette du Palais*, 9 (2018), p. 17.

bears the burden of proof in this respect) to demonstrate certain irregularity in the behaviour of the defendant (deviation of their behaviour from the standard model of due, careful behaviour of a reasonable person). The standard (model) of behaviour constituting a reference point for determining fault may pose a huge challenge to the application of provisions on fault-based liability for damage caused by AI. This state of affairs is natural for every new phenomenon of social life. Natural difficulties in determining the standard of caution (due care) that should characterise the actions of people who use AI is a consequence of the lack of "historical data" – the lack of knowledge about what behaviours may intensify the risk of damage and what may be considered a reasonable use of AI preventing it from inflicting damage.

The EU legislative proposals mentioned at the beginning of the paper are aimed at eliminating the risk that the victims relying on fault liability would be put under. They do this in two ways, which vary in detail depending on the specific legislative proposal. The first possible way is to impose strict liability on the users (operators) of AI systems for damage caused as a result of the operation of a given AI system. The second is to impose liability dependent on fault on the users. This fault liability is accompanied by the reversal of the burden of proof – the presumption of fault or presumption of causation meant to improve the injured parties' position. The first model was employed in the Draft Regulation from 2020. In this draft, strict liability is proposed to be imposed on broadly understood operators (the so-called front-end operators and back-end operators, i.e. end users of the system and entities "technologically managing" the AI system) for damage caused by the so-called "high risk AI systems"[17] which would be periodically included in the list of high-risk systems issued by the European Commission on the regular basis. As far as the other types of AI are concerned (non-high risk systems), the Article 8 of the draft provides for the fault liability of the operators. However, fault is presumed according to the provision at hand and it additionally provides for an exhaustive list of exculpatory circumstances. The fault-based liability model has also been employed in the Draft Directive on liability for artificial intelligence. Strictly speaking, this draft is of procedural character. Its aim is not to harmonise the substantive law of the Member States. It provides for a mechanism to facilitate evidentiary rules by providing the defendant with the presumption of a causal link between the "harmful behaviour of the AI system" and the fault of the plaintiff, where the latter was proven by the way of special evidentiary proceedings[18].

As mentioned above, the relationship of the drafts of legal rules on liability for AI to the article 82 of the GDPR would appear highly unclear. If the drafts become a binding law, a natural question will arise whether in the case of the liability of the user in the case of data breach by the AI system processing data, the

[17] That is AI systems that have a significant potential to cause "randomly occurring damage to one or more persons in such a way that is beyond what could reasonably be expected".
[18] See P. Machnikowski, *Prawo deliktowe wobec nowych technologii*, Wolters Kluwer, Warszawa, 2023, pp. 565 ss.

article 82 of the GDPR is to be applied (for the case regards the GDPR violation expressly dealt with by the GDPR) or the special liability rules at hand should be applicable (as the case involves damage caused by AI). At the first glance the question may seem farfetched. One can reckon that in the event of data breach in the course of data processing by AI, the damage is always caused by the use of AI (and thus by the controller or processor who uses the AI system) and not by AI directly and the question at stake is not legitimate.

However, one should bear in mind that these special rules on liability (the draft rules mentioned above), if they become a binding law, will in fact concern liability for damage caused by humans (by the users relying on a given system bearing the hallmarks of AI). Strictly speaking, they will not concern the liability for damage caused "by artificial intelligence" as such. To the extent that the draft liability rules at hand are based on the principle of fault, they ascribe liability for damage caused by the operation of AI to persons who, while using this technology, have committed a specific violation of applicable standards of care (violations of legal provisions or precautionary rules) regarding the use of this technology (e.g. by not making the required system updates, by making an incorrect decision on the use of a certain AI system that was inappropriate in given circumstances, which led to an increased risk of causing damage compared to an alternative scenario in which specific action resulting in damage would have been taken by a human instead or by another, more adequate, AI system, or by neglecting to take all necessary and reasonable measures to avoid that the system start operating outside the consent and control of the user). In essence, the liability at hand can be viewed as liability for specific human behaviour (faulty behaviour) of the AI user that is the "background of the system's behaviour" from which the damage resulted. Talking about liability for damage "caused by AI", at least in some cases, is only a metaphor.

Consequently, it would not be reasonable to assume *a priori* that the GDPR infringements always occur as a result of human activity (controller or processor) and that the fact that the infringement occurs "while using AI" (within the course of processing data in an automated manner) should be neglected as completely legally irrelevant as the need to resort to special rules on liability never materialises. The potential overlap of the article 82 of the GDPR and the special rules of liability for AI (if enacted) would still raise a valid question of how the two sets of legal rules relate. This kind of question should be posed and answered conclusively when deciding cases of "data breach by AI" as the choice of one (the GDPR) or another (special AI liability regime) could lead to overwhelmingly different results as to whether the liability arises at all and as to the scope of potential liability. To prove this point, a few examples can be made.

If we think of the violation of the GDPR by a high-risk AI system within the meaning of the above-mentioned draft regulation (e.g. in the case of collecting personal data by a drone which could potentially be qualified as high-risk), a question would arise whether the damage consequent upon the GDPR violation is subject to compensation under the Article 82 of the GDPR or under the rules contained in the to-be-regulation draft (due to the fact that the data processing rules

specified in the GDPR were violated by high-risk AI). If the latter is chosen, the data-subject could claim limited compensation because articles 4 and 5 of the draft regulation, contrary to the GDPR, provide for a cap that limits the sum of damages to be granted to the victims. Similar doubts could arise where data breaches occurred as a result of a cyberattack. Under the GDPR the controller may escape liability for damage consequent upon the acquisition of personal data by a third party as a result of a cyberattack if they demonstrate that proportionate organizational and technical measures have been taken to prevent such an attack (Article 24 and 32 GDPR)[19]. Meanwhile, the Article 8 section 3 of the draft regulation clearly provides that "where the harm or damage was caused by a third party that interfered with the AI-system by modifying its functioning or its effects, the operator shall nonetheless be liable for the payment of compensation if such third party is untraceable or impecunious". If a specific AI system begins to "transfer" personal data collected by the original controller to a third party as a result of a cyber-attack, the answer to the question of whether the liability of the original controller arises would thus depend on whether the article 82 of the GDPR or the regulation (if enacted) is applicable.

The above described or similar doubts stem from legal discrepancies between the GDPR and special liability regime for AI accompanied by the lack of clarity as to the relation of the two sets of legal rules. Such obstacles could easily be avoided by the EU law maker at the final stage of the legislative process. If the decision is made to enact the special liability regime for AI, the EU legislative institutions could amend the drafts by expressly deciding their relation vis-a-vis article 82 of the GDPR. Potentially there are three options to choose from. The first is to give priority to article 82 of the GDPR and to decide that it is solely applicable even where damage consequential upon data breach was "caused by AI" (in the course of processing personal data by AI). The second is to decide that article 82 of the GDPR is not applicable in such cases, as it is overridden by the special liability regime because the damage was "caused by AI". The third possible choice is to decide that neither set of legal rules prevails and to leave for the victim (data subject) to freely decide whether they intend to rely on the GDPR or special liability regime. By choosing any of these three possible paths, the EU law maker would mitigate the risk of legal uncertainty linked to the future enactment of the special liability regime. Any clear cut by the law maker would be welcome from this perspective as it would remove the legal uncertainty potentially preventing the data subjects from seeking compensation of damage resulting from data breach by AI.

It would not be advisable, however, if the EU law maker limited themselves to this kind of minimum, technical problem solving. The puzzle of priority of the legal rules at hand is to be decided upon cautious consideration of reasons underpinning the special liability regime for AI.

[19] See the CJEU Judgement of 14 May 2021, C 340/21.

6. Concluding Remarks: Policy Choices

As mentioned above, the draft rules on liability for AI serve the purpose of easing the access to fair compensation for the victims of AI-inflicted losses by removing evidentiary obstacles they would face when relying on fault liability schemes. However, in the event of AI-inflicted damage caused by data breach these obstacles do not appear under the GDPR. The legal position of the victims would not change (would not be improved), if they followed within the scope of special liability regime of AI. From the victim's (data subject's) perspective it does not matter at all whether a given AI system collected their personal data without consent because this was the intent of the controller or because of the back-end operator's or programist's mistake that resulted in unintended data collection by AI system. In the light of rights-based approach employed in the GDPR, in any case the violation of the regulation can be said to have occurred. The GDPR makes it possible for the controller or processor to escape liability by proving if they prove not to be "in any way responsible for the event giving rise to the damage". According to the CJEU's view expressed in *Krankenversicherung Nordrhein* case[20], such a wording means that the liability provided in the article 82 of the GDPR is based on the principle of presumed fault. Thus the existence of fault as the precondition to liability is presumed, unless controllers prove otherwise (as the controller-defendant bears the burden of proving that the damage was caused as a result of circumstances for which he is not responsible). Thus under the GDPR, a scenario is impossible in which the data-subject would remain without compensation because of not being able to prove the preconditions of liability that substantially were met in the case. Therefore under the GDPR no risks appear that the special liability regime for AI oat to prevent. In my view the article 82 of the GDPR shall thus be given priority and remain a sole legal basis for liability for damage consequential upon data breach was "caused by AI" even if the special liability regime for AI is enacted.

[20] The CJEU Judgement of 21 December 2023, C-667/21, EU:C:2023:1022.