ODR AND ONLINE COURTS: WHAT IS THEIR FUTURE AFTER THE AI ACT

Andrej Krištofík / Pavel Loutocký

Andrej Krištofík, Ph.D. student, Masaryk University, Faculty of Law, Institute of Law and Technology, Žerotínovo nám. 617/9, 601 77 Brno, CZ, kristofik@law.muni.cz

Pavel Loutocký, Ph.D., postdoc researcher, Masaryk University, Faculty of Law, Institute of Law and Technology, Faculty of Informatics, Žerotínovo nám. 617/9, 601 77 Brno, CZ; loutocky@muni.cz

Keywords: ***Onilne Dispute Resolution; online courts; eJustice; AI Act; Judicial Decision Making Support systems; Artificial intelligence***

Abstract: *Online Dispute Resolution (ODR) is characterized by the use of technological means, which makes ODR platforms beneficial compared to standard courts and dispute resolution methods. Any regulation of technical means has an impact on the use and possibilities of ODR, especially when such regulation directly references usage in judicial settings. The proposed AI Act aims to regulate any use of specified AI technologies in situations that could potentially impact fundamental rights, with specific emphasis on the right to a fair trial. The article analyzes the implications of the AI Act on the usage of such technologies in ODR processes, whether and to what capacity they are permissible, based on the categories proposed by the AI Act. The article also analyzes other aspects of ODR processes that could have implications for fundamental rights but are either out of scope of the AI Act or are overlooked by it.*

1. Introduction[1, 2]

This article sets out to evaluate the impact of the European Union legislation that aims to regulate artificial intelligence in cases where online dispute resolution ("ODR") approach is used for deciding disputes. ODR involves the use of modern technologies at different stages of the process with different technological penetration, and as the matter of fact, such reliance on the use of technology constitutes one of the defining elements of ODR.

The current version of the AI Act[3] is presented as the legislation leading to regulate the use and development of artificial intelligence and to establish rules for providers of such systems. It generally sets out three basic levels of systems with varying degree of regulatory duties: (i) prohibited use of artificial intelligence systems, (ii) high-risk systems, and (iii) other systems ("low or minimal risk"). In its last version, there are special obligations for other specific uses of Artificial Intelligence, such as manipulation and generation of content, that are stand-alone categories.

The first category,[4] established in Title II, lists AI systems that are prohibited from being developed and/or placed on the market. The second category[5] represents the broadest category regulated by the AI Act, which

[1] This article has been written at Masaryk University as a part of the project MUNI/A/1293/2022 „Právo a technologie XI" with financial support of specific research of the Ministry of Education of the Czech Republic for the year 2023.

[2] Pavel Loutocký has written first and second section of this article.

[3] *European Pairlament.* 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 last accessed 10.10.2023 (further stated as „the AI Act").

[4] Title II or Article 5.2 of the AI Act.

[5] The AI Act is primarily focused on these systems and sets up particular rules which are further elaborated by the proposal and selected will be dealt with later in this article.

includes high-risk systems listed in more detail in Annex III and comprises the most interesting category from the standpoint of this article, since most of the regulation of AI Act is placed on this category. The third category includes systems that do not fall within the definitions set out in Annex III, yet the AI Act provides either obligations or recommendations for them, related to transparency and compliance. Lastly, there are some specific uses, with regulation outside of this categorisation, that is established not based on the impact, as is the case of the three-level categorisation, but more on the technology as such – for example deepfakes.

The article focuses primarily on the second level of risk categorisation of the current AI Act, which encompasses high-risk systems, mostly listed in the Annex III. The definition of the usage of AI systems in the context of administration of justice "*AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts*".[6] The AI Act's general requirement to preserve fair trial and respect fundamental rights is another important principle for further assessment and is essential to this analysis. Another, more general, principle that must be respected in further assessment is the AI Act's general requirement to preserve fair trial and respect fundamental rights. Thus, the primary requirements stated by the AI Act are transparency of the AI system,[7] the possibility of effective overseeing of the process „*by natural persons during the period in which the AI system is in use*",[8] and, for example, reporting obligations.[9]

ODR can be generally viewed as a contemporary method and an approach to resolving disputes, whether in its binding or non-binding form, and notably, by making use modern technologies. We contend that ODR should primarily be perceived as a flexible alternative employing contemporary tools and diverse methodologies for conflict resolution.[10] Given its fundamental objective of resolving disputes, the implications of the AI Act on the nuanced aspects, both technical (use of AI based technology) as well as legal (possible interaction with fundamental rights) of decision-making within distinct ODR approaches necessitate careful examination, as previously outlined in this discourse.

2. What is ODR and how the disputes can be decided

In discussing online dispute resolution (ODR), it is important to consider the aspects that are essential for such an approach to dispute settlement. Previous research[11] has identified three important aspects of ODR: (i) dispute settlement, (ii) using modern communication technologies to exchange information, and (iii) more complex software assistance and using tools to optimize (automatize) the decision-making processes.[12] In this article, the focus is on the implications of the proposed AI Act on the usage of such technologies in ODR processes.

1. Dispute settlement, as the initial facet of ODR, encompasses the diverse options available to resolve disputes, either extrajudicially or through the judicial system. An exemplary approach to dispute resolution is demonstrated by online courts, amalgamating both non-binding and binding (judicial) stages in the pro-

[6] High-risk systems in the present context are also to be generally considered as relevant in the case of adjudication of disputes under point 6 of the Annex III (Law Enforcement); here, however, the focus of the legislation is primarily on criminal offences, which do not fall primarily within the scope of this article.

[7] Article 13 of the AI Act.

[8] Article 14 of the AI Act.

[9] Article 62 of the AI Act.

[10] More on this below or for example here: Loutocký, Pavel, Possible Approaches towards the Architecture of Online Courts and their Potential in the Decision-making Process. Jusletter IT, vol. 2022, 1-12 (2020).

[11] This is the research within the project on the basis of which we present some of the considerations in this paper.

[12] Carver, Todd/Vondra, Albert A, Alternative Dispute Resolution: Why It Doesn't Work and Why It Does. Harvard Business Review, vol. 1994, no. May-June. https://hbr.org/1994/05/alternative-dispute-resolution-why-it-doesnt-work-and-why-it-does accessed 10.10.2023 last accessed 10.10.2023 (1994).

cess, resulting in an optimized transformation of the decision-making process architecture.[13] Additionally, within the realm of private dispute resolution, e-commerce platforms offer another illustrative instance.

2. Leveraging modern communication technologies for information exchange stands as another significant facet of ODR and constitutes its integral and defining component. This extends beyond mere synchronous or asynchronous data transfer among pertinent parties, encompassing the utilization of video conferencing capabilities. While this aspect holds significance within ODR, it‘s notable that the technologies employed, though crucial, are neither novel nor uncharted. Furthermore, their relevance in the context of the AI Act is relatively marginal.
3. Within the latest legislative framework, a particularly intriguing aspect, to be expounded upon in subsequent sections of this article, pertains to the potential application of assistive systems. These systems extend beyond conventional software platforms for data management in the decision-making context, embracing advanced prospects for optimizing and automating the entire process. Notably, these advancements are progressively manifesting within the structures of private providers as well as certain systems designed for binding decision-making.

In connection to this final point, we further present the diverse requisites envisioned by the AI Act.

3. What is covered by AI Act

In this section of the article, our initial focus will be an examination of the AI Act‘s scope and its broader relevance to ODR. Subsequently, we will present specific instances showcasing the utilization of AI technology within ODR processes.

Initially, one could raise an objection suggesting that the AI Act explicitly advocates for application within the judicial domain. One might as well contend that ODR processes do not fall within this scope, possibly citing the European Court of Human Rights‘ interpretation of “judicial” in the application of Article 6, which encompasses bodies established based on a legal act.[14] However, it is important to acknowledge a diverse range of counterarguments to this conclusion.

On one end of the spectrum, an argument supporting an extensive interpretation of the term “ODR” asserts that any dispute resolution that relies on technological means to resolve said dispute, qualifies as an ODR process. Consequently, even an online court, utilizing ODR tools, falls within this subset of ODR processes, thereby making the AI Act applicable in those cases as a judicial use. This line of reasoning closely aligns with a second perspective, suggesting that while ODR and judicial processes retain distinctions, the ongoing digitization of justice is gradually blurring these boundaries. This evolution renders such a differentiation increasingly irrelevant. Though ODR and judicial processes are not yet fully synonymous, a future-proof approach would involve regulating them accordingly.

On the opposite end of the spectrum, an argument contends that ODR and judicial processes are inherently distinct, yet this distinction may not be pertinent. Despite the AI Act‘s repeated reference to „judicial“ settings, it isn‘t the sole criterion for its applicability. The Act‘s overarching mission, reiterated consistently, revolves around safeguarding fundamental rights, preventing discrimination, and establishing a secure environment for the integration of AI systems into society and commerce. ODR processes, being capable of delineating, modifying, or nullifying rights and obligations of participants across diverse domains (ranging from customer disputes to rental contracts), are inherently connected to fundamental rights. It is imperative that

[13] One of the best examples can be provided by the Civil Resolution Tribunal in Canada: https://civilresolutionbc.ca/ last accessed 10.10.2023 and was theoretically described by Susskind, Richard, Online Courts and the Future of Justice. Oxford University Press, Oxford. p. 62 et seq. (2019).

[14] See for example: Registry, Guide on Article 6 of the European Convention of Human Rights. Council of Europe, Brussels. pp. 20 – 21. https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf last accessed 10.10.2023 (2022).

such processes adhere to the prerequisites outlined by the AI Act, including non-discrimination, protection of weaker parties, transparency, accurate datasets, and human oversight where feasible. Prioritizing the protection of users‘ fundamental rights fosters a stable business environment for the development and utilization of AI-based systems, thereby aligning with the second goal of the AI Act.

The subsequent question then is how the AI Act should be applied to the ODR processes and what ramifications does that carry. As previously elucidated, a fundamental characteristic of ODR lies in its substantial reliance on technology, effectively constituting the „third“ party in dispute resolution.[15] Consequently, the technology involved must be substantive; merely employing email during proceedings does not elevate the process to ODR status. However, not all substantive technology falls within the AI Act‘s purview, as the Act explicitly encompasses technologies employing artificial intelligence. Not all of this substantive technology then is in the scope of the AI Act, since it obviously covers only such technologies that use artificial intelligence. The definition of relevant technology is itself rather problematic, as in its (reasonable) attempt to remain technologically neutral,[16] the definition encompasses any such technology that follows human-defined objectives and outputs decisions, interacting with its environment.[17] This, rather broad and less-than-ideal definition s complemented by a list of specific approaches constituting AI use, akin to the main text‘s breadth, to the extent that even calculators technically fit within this framework.[18] Given this extensive scope of technology defined in the Act, a thorough analysis of its impact on ODR becomes increasingly essential.

An illustrative instance of AI technology application in ODR is DoNotPay[19], characterized as a “legal chatbot”. This tool effectively resolves uncomplicated disputes, such as parking tickets, or offers simplified legal assistance, like canceling subscriptions. While the intricacies of the technology remain undisclosed to the public, it is evident that the chatbot employs Natural Language Processing (NLP) for inputs. Given that the outputs mainly manifest as forms for submission, automated technology is utilized to generate outputs that interact with the environment, thus aligning with the AI Act‘s definition. Plausibly, this positions the technology somewhere between Level 1 and Level 2 of legal system autonomy on the Eliots‘ scale.[20]

Another notable example is the AssetDivider technology, predominantly applied in various family law or divorce cases concerning property disputes.[21] This system employs a proprietary algorithm to equitably distribute assets between the involved parties, considering not only their objective value but also their subjective value to each party. This approach leads to more agreeable settlements and aligns with the definition provided by the AI Act, regardless of whether conventional artificial intelligence methods are used.

4. The regulatory duties

Having established the possibilities of applying the AI Act to ODR processes and acknowledging that these processes fall within the AI Act‘s technological scope, the ensuing question revolves around the responsibilities engendered by this observation. As outlined in the introductory section, the AI Act delineates three categories based on the perceived potential to infringe upon fundamental rights. Through this categorization, we can ascertain the permissibility of such usage and, if permitted, discern whether it entails specific obligations or mere recommendations. Despite inherent uncertainties, the definition of “prohibited usage” is relatively

15 Katsh, Ethan/Rifkin, Janet, Online Dispute Resolution: Resolving Conflicts in Cyberspace. Jossey-Bass, Hoboken. (2011).

16 Point 5.2.1 of the AI Act.

17 AI Act point 6 of the preamble.

18 Annex I of the AI Act.

19 *DoNotPay website.* www.donotpay.com last accessed 10.10.2023.

20 Eliot, Lance, Antitrust and Artificial Intelligence (AAI): Antitrust Vigilance Lifecycle and AI Legal Reasoning Autonomy. arXiv. http://arxiv.org/abs/2012.13016 last accessed 10.10.2023 (2020).

21 Belluci, Emilia, AssetDivider: a new mediation tool in Australian family law. In: Hindriks, Koen V./Brinkman, Willem-Paul, HuCom ‚08: Proceedings of the 1st International Working Conference on Human Factors and Computational Models in Negotiation. Association for Computing Machinery, New York, pp. 11-18 (2008).

clear-cut, explicitly forbidding applications such as social scoring of citizens, subliminal manipulation, or the manipulation of vulnerable individuals, notably the elderly. Alternatively, this specific usage might fall under the regulated high-risk category.[22]

The other possibility is that this specific usage might fall under the regulated high-risk category. High-risk usage encompasses any application that jeopardizes health, security, and, significantly, fundamental rights. Section 3.5 of the AI Act, within its introductory segment, concentrates on interpreting the term "fundamental rights", drawing from the European Charter of Human Rights. This section explicitly references rights related to data protection and non-discrimination—both pertinent in (automated) ODR processes. Crucially, it emphasizes safeguarding the right to a fair trial and the right to an effective remedy.[23] Furthermore, the AI Act explicitly designates judiciary application as one of the high-risk applications. Given the described scope of application in the preceding section, an argument can be made that judiciary application should be construed broadly, encompassing any situation involving decisions that can alter or nullify individuals‘ rights and obligations. Even if one refrains from ex-tending the term "judiciary application" to ODR processes, the potential adverse impact on the aforementioned fundamental rights could still warrant categorization within this domain. The pivotal keyword here is "risk", underscoring that mere alignment with the category is insufficient; the usage must also pose a discernible risk to the rights. The AI Act proposes a risk-based framework, relying extensively on past performance for an ex-post evaluation conducted on a regular basis. This approach is akin to risk assessments observed in various AI regulatory endeavors concerning decision-making, exemplified by the Canadian Directive on Automated Decision Making.[24] Additionally, factors such as the extent of usage and opt-out alternatives constitute significant considerations within this framework. Additionally, factors such as the extent of usage and opt-out alternatives constitute significant considerations within this framework.

Although the precise categorization of AI systems in ODR processes may be shaped by subsequent observed impacts, considering the points discussed earlier, we can infer that it is likely to be categorized as high-risk usage, at least in most cases of the use of advanced, AI based technologies in the process of resolving the disputes. The remaining question revolves around the regulatory obligations associated with this classification. While scattered throughout the AI Act, the primary body of regulation, particularly addressing high-risk usages, is predominantly concentrated within Title III of the proposed AI Act.

Chapter II of this Title firstly, even though a bit redundantly, sets out the obligation to follow all of the following obligations. However, following Article, Article 9, already provides us with a more substantive duty and that is to put in place a Risk management system.[25] This process or functionality is detailed comprehensively; however, its core concept can be succinctly summarized as a system that continually identifies potential threats to the mentioned (fundamental) values, assesses them, and proposes potential remedies if any of the threats become pertinent. Essentially, this could manifest as an internal audit process. When a potential threat to a relevant value is detected, it does not automatically prohibit further use, a restriction reserved for the third category of AI system use, which follows a distinct methodology. Instead, it imposes the obligation to a) mitigate the risk, and if not feasible, then b) alleviate the impact on the protected values. In the event that neither is achievable, the minimal duty is to c) provide appropriate information (and relevant training) regarding the potential risk. Intriguingly, in the pursuit of ascertaining potential risks before introducing the system to the market, even risks stemming from improper usage must be taken into account.

---

[22] AI Act point 5.2.2. Lastly it also mentions a distant real-time biometric identification by police enforcement, however the Act mentions that as much as it is banned, it is permissible in unspecified situations, and it also classifies it as (permissible) high-risk in the Annexes.

[23] AI Act point 3.5.

[24] *The Government of Canada,* Directive on Automated Decision-Making. Quebec. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 last accessed 10.10.2023 (2019).

[25] These duties are mostly imposed on the subject that is placing the system on the market, even though it is sometimes unclear and could be debated whether that is the right choice.

We now turn our attention to the somewhat inadequately formulated regulations, which, despite their initial appearance of reasonableness, indicate a certain degree of misunderstanding of the subject matter being regulated by the governing body. The first point, perhaps the least problematic, pertains to the data utilized during the developmental phases. These regulations broadly address issues concerning other protected values that could be relevant when considering AI applications in ODR processes – specifically, data protection and non-discrimination.[26] However, complexities arise with the requirement to maintain logs. On one hand, this requirement is reasonable due to the necessity for iterative risk assessment and auditing. On the other hand, the insistence on logs is questionable, particularly considering the current technology landscape, where what is typically regarded as AI, such as various forms of deep learning, challenges the applicability of this requirement. This discrepancy is not aligned with the AI Act's intent of „future-proofing." While the AI Act does outline the specifics of how logs should be maintained and what information they should contain, it raises fundamental questions about the efficacy of this entire article. This, in turn, prompts us to question whether the primary focus should have been on iterative risk assessment, with the detailed aspect of record-keeping, especially within highly specialized technology, left to the discretion of the entity responsible for conducting the risk audit. Moreover, one of the stipulations for record-keeping pertains to the inclusion of the identification data of the natural person overseeing the process. This requirement seamlessly leads us to another challenging aspect of the AI Act – human oversight.[27]

This particular stipulation once again highlights a potential misunderstanding of the subject being regulated, as the specific requirements resemble those found in regulations governing heavy machinery. This article mandates operators of relevant systems to possess a complete understanding of the entire operational process and have the capability to conduct inspections at any given moment during its operation. Additionally, they must be able to make necessary adjustments to the process or outcome when required.

However, this requirement overlooks the challenges posed by algorithmic black boxes and the general nature of various machine learning techniques. These aspects render such oversight practically impossible and, at the very least, are in direct conflict with the efficiency of automated processes—a fundamental element in their creation. In light of this, it might be more rational to draw inspiration from the Canadian Directive on Automated Decision Making, which underscores the capacity to conduct ex-post controls. From a technical perspective, these controls are more robust, particularly due to methods like explainable AI (xAI), including backpropagation.[28]

The last Article lumps together several duties, such as the need for the proper cybersecurity of systems and ensuring its accuracy, which is again a requirement better suited to be part of the iterative testing in the lifecycle of the system.

Regarding the regulatory duties for ODR systems under the current AI Act, two conclusions can be drawn. Despite the significant reliance on technological means within ODR processes—so much so that it constitutes an integral part of ODR's definition—not all aspects are likely to fall within the scope of this regulation. For those that do, the primary duty revolves around establishing a comprehensive risk assessment system to be utilized throughout the system's lifecycle. The primary objective of this system is to detect potential threats to the protected values and subsequently address them, either by eliminating the identified risks if feasible, or by mitigating them. The majority of the remaining duties are in some way linked to this central duty, designed to facilitate or support its fulfillment, as we argue they should be perceived.

---

[26] This of course is correct regulatory move, since a lot of the critique towards any AI based decision making stems biased data or improper use of collected data. See Richardson, Rashida/Schultz, Jason/Crawford, Kate, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. NYU Law Review, vol. 94, no. 192, pp. 193 – 223 (2019).

[27] Article 14 of the AI Act.

[28] For an overview of posthoc evaluation method see: *Van der Velden, Bas H. M. et al.*, Explainable artificial intelligence (XAI) in deep learning-based medical image analysis. Medical Image Analysis, vol. 79. Pp. 1 – 21 (2022).

Lastly, there are several regulatory duties, that are imposed outside of the scope of this three-level risk assessment. Those are set out in Title IV and essentially encompass a transparency obligations. Those are however, unfortunately not imposed on ODR systems, as defined above, nor are they understood in the proper sense of the word and as such comprise a shortcoming of the AI Act, which will be addressed in the following section.

5. The shortcomings of the current AI Act

There is a substantial criticism that can be directed towards the AI Act. Some relatively minor, like the improper use of certain terms, like the unclear distinction, between „judiciary application" and „application in the administration of justice." On a more general level, there are broader criticisms directed at the AI, this includes notably expansive definitions in the Annexes and the imposition of duties that seem incongruous with technological specifics. Numerous rules, while not in direct contradiction, introduce significant uncertainty. For instance, the classification of any system encroaching on fundamental rights as prohibited under Title II, while an iterative control finding such violation in an already deployed system could be mitigated or addressed through the provision of information to maintain the system's classification as high-risk, thus allowing its continued usage. Furthermore, there are certain uncertainties and overlooked aspects within the AI Act that could be directly applicable to ODR.

One of the key concerns surrounding (automated) decision-making systems revolves around their transparency.[29] Although the AI Act incorporates provisions on transparency,[30] it confines them to a specific category of systems that falls outside the established three-level categorization. Furthermore, it interprets the transparency requirement differently. While entities like AI HLEG and OECD view transparency as an obligation for providers to construct systems transparently, encompassing proper data handling, traceability, and a suitable level of decision explainability, the AI Act construes this requirement as the need to disclose that the process is managed by an AI system.

Undoubtedly, there is merit in this disclosure requirement[31], extending even to ODR processes, although they are not explicitly mentioned in Title IV of the AI Act. Providing information about the extent to which such systems are utilized in ODR processes would be a reasonable step. However, the alternative interpretation of the transparency requirement holds significance and should not be dismissed. On the contrary, the AI Act should heed the recommendations of AI HLEG, as it acknowledges, and underscore the imperative for transparent processes and their traceability.

This interpretation of the transparency requirement holds particular significance in decision-making processes, especially within contexts such as ODR, where it directly impacts individuals' rights and responsibilities. This is especially pertinent concerning other aspects overlooked by the proposed AI Act, which are typically associated with (quasi)judicial proceedings, including proceedings in the second instance, such as appeals or reviews. This association ties back to the way the Act addresses the concept of fundamental rights. The possibility of appeal is, at least according to the ECtHR's interpretation, part of the right to a fair trial, or more broadly, an aspect of the effective remedy—both of which are highlighted as protected fundamental rights in the AI Act. However, this reference remains quite general, leaving uncertainty regarding how second instance proceedings should be handled in automated decision-making to ensure compliance. It raises questions on whether it is mandatory to always have the option to appeal to a human—a procedural requirement estab-

[29] See for example *OECD*, AI Principles. Transparency and explainability (Principle 1.3). https://oecd.ai/en/dashboards/ai-principles/P7 last accessed 10.10.2023 (2022) or even EU's own AI HLEG referenced in the AI Act and their guidelines for trustworthy AI *AI HLEG,* Guidelines for Trustworthy AI, April 2019, Brussels. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai last accessed 10.10.2023 (2019).

[30] Title IV of the AI Act.

[31] AI Act references them especially in connection to DeepFakes and „direct interaction" i.e. customer service VoiceBots.

lished in the GDPR[32] – or if obtaining a different „automated opinion“ is a viable alternative. Furthermore, the possibilities to object to the use of such AI systems when individuals‘ rights and obligations are at stake remain unclear.

A prevailing criticism of the AI Act revolves around its inherent uncertainty and what seems to be a discernible misunderstanding of the regulatory subject matter. This misunderstanding places an undue burden on providers to fulfil duties that are incompatible with their technology. Conversely, the act falls short in establishing requirements that are better aligned with safeguarding (specific) fundamental rights.

6. Conclusion

The conclusions are twofold. Firstly, it pertains to the matter of applicability, discussed in the third section, where we have advocated for a broader interpretation of the term “judiciary”. This broader interpretation is warranted not only because the term ODR inherently encompasses online courts but also due to the inherent nature of all ODR processes, which possess the potential to impact an individual‘s rights and obligations.

Furthermore, as we thoroughly examined the regulatory responsibilities of ODR providers, particularly if they fall within the high-risk AI use category as defined by the AI Act, we found these duties to be largely sensible. The primary motivations behind the creation of the AI Act were to ensure a) the protection of fundamental rights and b) the establishment of a secure environment for innovation and business. Therefore, it is highly advisable for ODR systems to embrace the safeguards outlined in the current wording of the AI Act. This approach would foster greater trust in these processes, encouraging their broader adoption and facilitating a smoother transformation into fully developed online courts.

The second conclusion arising from this article highlights several shortcomings in the proposed wording of the AI Act. Apart from its inherent uncertainty stemming from the desire for technological neutrality and other issues, it also lacks numerous essential safeguards necessary for the broader adoption of AI technologies in (quasi)judiciary settings. Specifically, critical matters such as the treatment of AI-driven decisions in a possible second instance and the provision for an opt-out option remain unanswered. Although a step in the right direction, the current wording of the AI Act overlooks crucial aspects that need to be addressed to comprehensively cover not only ODR technologies but also their responsible use.

[32] Article 22 of *European Parliament.* 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) -lex.europa.eu/eli/reg/2016/679/oj&usg=AOvVaw1XAG3mHMtSjUcR1oFXnGgW&opi=89978449 last accessed 10.10.2023 (2016).