

Francesca Palmiotto

# Preserving Procedural Fairness in The AI Era

The Role of Courts Before and After the AI Act

doi: 10.17176/20230105-121527-0



In the past years, scholars and civil society organisations have raised concerns regarding the use of automated systems in public decision-making. The [child benefit scandal](#), which led the Dutch government to resign in 2021, is just an example of poor human decision-making aided by flawed automated systems. In the same year, the European Commission proposed a [Regulation for AI systems](#), the so-called “AI Act”, to address the challenges and concerns raised by the increasing use of AI while encouraging businesses to develop them in the EU single market. While the proposal is still under [discussion in the European Parliament](#), AI systems have been used and challenged by individuals affected by their output. In the absence of a regulatory framework, national courts in Europe have been called upon to address claimants’ demands for fairness and legal protection. This post investigates the role of courts in preserving procedural fairness in the era of AI. I focus on six cases where automated systems were used to inform public decision-making to detect tax and social welfare fraud ([eKasa case](#) and [Syri case](#)), to grant permission for agricultural businesses ([AERIUS case](#)), and to recruit and transfer high school teachers ([Altomare](#) and [C.P.](#) cases) in Slovakia, Italy and in the Netherlands.<sup>1</sup> I show how national courts have been activists in preserving individuals’ procedural rights by setting requirements for AI systems. Their role is, however, doomed to change when the AI Act enters into force.

## Automated decisions in the public sector: what is at stake for procedural fairness?

The use of AI systems to replace, support and aid human decision-makers raises several concerns, especially in terms of non-discrimination, data protection and compliance with fundamental rights. When focusing on the

relationship between AI systems and procedural rights, three key legal issues emerge from the selected cases. Firstly, the lack of awareness of individuals about the use of an automated system in decision-making hinders their possibility of seeking an effective remedy. Even if access to information and knowledge about automated processing are cornerstone principles of the [Regulation 679/2016](#) (see Articles 5, 12, 13, 14 and 15 GDPR), particularly when a decision is “solely based on automated processing” (see Articles 22 and related access rights in Articles 15(1)(h), 14(2)(g) and 13(2)(f) GDPR), in some specific contexts, such as law enforcement and migration control, opacity is the rule rather than the exception. It is not a coincidence that the [Directive 2016/680](#) (hereafter LED) - which applies to data processing by law enforcement authorities - contains broader restrictions for the data subjects’ rights to information compared to the twin GDPR (see, for instance, Article 15 LED). Interestingly, some EU Member States demand opacity of their fraud detection systems by law to prevent “gaming” by individuals and preserve the State’s interests in the effective prosecution and investigation of crimes ([Hadwick 2021](#)). The lack of awareness and transparency about the use of automated systems explains why, except for cases concerning platform workers, the vast majority have been brought before Courts by civil society organisations, activists, or political representatives, rather than individual citizens affected by automated decision-making.

The second legal issue emerging from case law is the protection of design information as trade secrets, hampering the claimant’s possibility to challenge the accuracy of the system. Design information, such as algorithms, source code, and training data, are generally trade secrets, which, if disclosed, could harm the competitive advantage of the system developer. Therefore, disclosure of design information requires a careful balancing be-

<sup>1</sup>The cases have been selected from the caselaw collection that my colleagues and I are creating for the [AFAR Project](#). This collection is planned to be published as an online resource, the Newtech Caselaw Database.

tween public and commercial interests, individual rights, and companies' intellectual property entitlements.

US Courts anticipated this debate years ago in “driving-under-influence” cases, where defendants attempted to compel the disclosure of breath analysers' source codes used to bring evidence against them at trial. The main argument in these cases was that, notwithstanding the protection of the source code as a trade secret, courts should have compelled its disclosure to satisfy their right to confrontation. A similar argument was advanced in the widely known *State v Loomis*, where the Wisconsin Supreme Court held that the use of an algorithmic risk assessment in sentencing did not violate the defendant's due process rights, even though the methodology used to produce the assessment was disclosed neither to the court nor to the defendant. In recent years, courts in Europe are starting to approach similar legal questions due to the increasing litigation in the field of automated decision-making (see [FPF Report](#)).

Finally, the third legal issue relates to the opacity of AI systems. Not only do AI systems not explain *how* they reached a conclusion, but neither do they justify *why* they have reached it. In *Altomare* and *C.P.*, two cases where an AI system was used to transfer teachers across Italy, the claimants complained that the system was taking decisions without justifying why it did not consider their listed preferences. When decisions are (fully or partly) automated, the opacity of AI challenges the right to have a reasoned decision and effective judicial review.

### Filling a regulatory gap: the activist role of national courts

While AI systems increasingly inform public decision-making, the opacity and secrecy surrounding their use adversely impact the protection of procedural rights. If individuals are not aware that an AI system has been used in their case, they cannot challenge its use. If individuals do not know how the system works, they cannot identify errors and obtain redress. How have national courts addressed these legal issues?

Firstly, while the importance of the GDPR for the regulation of automated assessments was acknowledged, courts considered that additional safeguards were needed to ensure that the constitutional guarantees were met. For this purpose, they set specific requirements for automated systems, including the reliability and non-

discriminatory nature of the criteria, data and models used (especially in *eKasa*) and the principles of transparency and interpretability of algorithms (in particular in *CP* and *Altomare*). Even in the more sensitive field of tax enforcement, transparency must be guaranteed, according to the Slovak Constitutional Court, which held that the individual concerned must have knowledge about the *existence, scope and impact* of the assessment by automated means, whether through public registers, specific instructions or otherwise. In the Court's view, this requirement is crucial for the right to “effectively defend himself or herself against possible errors” (§133 *eKasa judgment*). The Hague Court adopted a similar approach in the *Syri* case, which concerned a system used to prevent and combat fraud in social security and income-related schemes, tax and social insurance contributions, which they found to be insufficiently “transparent and verifiable” and, therefore, incompatible with Article 8 ECHR. Moreover, according to the Higher Administrative Court of Italy, automated systems must also be interpretable, which requires information to be comprehensible both for citizens and for the judge. For this purpose, the algorithm should be accompanied by explanations which clarify how the legal rule was translated into the technical formula.

Additionally, national courts also established obligations for public authorities using automated systems, such as the duty to publish and provide information about the systems used (in *AERIUS*) and to carry out a human rights impact assessment (in *eKasa*). More specifically, in *AERIUS*, the Dutch Council of State decided that public authorities must publish the choices made, the data and the assumptions at the basis of the system in a complete, timely and accessible manner ([Jurgen & Goossens, 2019](#)). In the Court's view, this duty for public authorities enables effective legal protection against decisions based on automated systems and allows courts to review the legality of these decisions.

Finally, courts recognised the link between transparency and the effective exercise of procedural rights, ruling against the protection of intellectual property when conflicts arose. In the *eKasa* judgment, the Court strongly supported the prevalence of fundamental rights over trade secrets. In the words of the Court: “Intellectual property rights cannot be a reason for denying effective access to the necessary information” (§ 135 *eKasa judgment*). In the Court's view, the State must comply

with the same conditions of transparency even when a third party provides the technology. For this purpose, public authorities should act from the procurement stage to ensure adequate access to information. Access to design information and algorithms was also a key conclusion of the Italian Higher Administrative Court in two cases where they assessed, for the first time, the legitimacy of the adoption of an algorithm for the performance of an administrative activity (Altomare and C.P.). In the twin judgments, the Court held that the principle of “full upstream knowability” of the algorithm used and the criteria applied must be respected.

Conclusively, in the absence of a regulatory framework for AI, courts have played an activist role in preserving procedural fairness in the era of AI by setting requirements for automated systems, establishing obligations for users, and granting transparency to individuals. However, their role is doomed to change in the future when the regulatory gap is filled by the AI Act.

### **The day after the AI Act: from activist to referring courts?**

Courts have done in the past what the AI Act will do in the future: setting requirements for high-risk AI systems, obligations for users (including public authorities) and granting transparency and access to (some) information. The differences between the proposed AI Act and the courts’ rulings are, however, stark. Just to mention a few, the AI Act provides limited transparency to the individual affected by the system (apart from some general information in Article 52 AIA); it does not require

the system to be interpretable to the end-user but only to the trained user (Article 13 AIA); it demands data be relevant and free of errors, but does not mention non-discrimination (Article 10 AIA); it requires registration in a public database, but excludes systems used in law enforcement and migration control (Article 51 AIA). Finally, the AI Act does care about trade secrets (Explanatory Memorandum point 3.5). The lack of rights for individuals affected by the use of AI systems in the AI Act in the current proposal has been criticised by scholars and civil society organisations (see, for instance, the [report by Lilian Edwards for the Ada Lovelace Institute](#)). Looking at the future, it is therefore important to ask what role will remain for Courts in preserving fundamental rights in the AI era.

While national courts have been activists in the past, the same approach will be problematic once the AI Act enters into force. The AI Act aims to ensure the proper functioning of the internal market by setting harmonised rules on essential elements regarding the requirements for AI products and services, their marketing, their use and liability regime. In light of the primacy of EU law, national courts will have to abide by these rules or refer to the CJEU for a preliminary ruling on the validity and interpretation of the AI Act ([Article 267 TFEU](#)). In the “day after the AI Act”, the protection of fundamental rights will be addressed through judicial dialogue between national courts and the CJEU, offering the Luxembourg Court the opportunity to safeguard individual rights for the entire EU and develop common values of digital constitutionalism in Europe.