Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement
Working Paper Series

AI and EU law enforcement [(*)]

Luis Arroyo Jiménez [(**)]

Abstract

Technological disruption is dramatically transforming the production and implementation of law from various perspectives. The challenge of incorporating automated decision-making (and specifically artificial intelligence) systems into EU law enforcement is to enjoy the promise of optimization of EU policies, while evading at least their most notable risks connected with the rule of law. Copying with this challenge requires different trade-offs to be achieved by EU courts and the EU legislator. Those trade-offs will plausibly depend on criteria such as: (i) the technological approach of the system – semi or fully automated systems, machine learning, deep learning, and so on, (ii) the functions it performs – red-flagging, allocation of scarce resources, provision of public services, and so on, and (iii) the area where it operates – the internal market, the area of freedom, security and justice, and so on. This paper explores these claims in terms of different building blocks of the rule of law.

Keywords:

Automated Decision-Making; Artificial Intelligence; EU Law; Enforcement; Rule of Law

[(*)] This paper is a summary of the talk given at the EULEN Conference that was held at the University of Heidelberg on the 23rd of June 2023. I have not included any footnotes, preferring to keep the original text, which was drafted as a lecture.

[(**)] Professor of EU and Administrative Law. University of Castilla-La Mancha, Spain [luis.arroyo@uclm.es].

1. Introduction

1. Technological disruption is dramatically transforming the production and implementation of law from various perspectives. In the framework of the EULEN network, we have focused on a group of these changes, namely those brought about by the expansion of automated decision-making (ADM), and in particular of artificial intelligence (AI) systems, in the activity of public authorities carried out to enforce EU law. The output of the network's action in this area has been threefold: a conference on the topic "AI Systems and EU Law Enforcement - Between Effectiveness and the Rule of Law", the on-line publication of a series of 12 working papers on the impact of AI systems on different areas of European Union (EU) law, and a special issue consisting of 7 articles that has recently been accepted for publication in an European academic journal.

2. Our approach has been both deductive and inductive. On the one hand, the implications of ADM and AI systems in terms of general principles of EU law have been explored – effectiveness of EU law, non-delegation, transparency, due process, good administration, and so on. These and other principles comprise legal requirements that can be put at risk when public authorities enforce EU law through ADM and AI systems. On the other hand, those issues have been analyzed as they arise in the various policy-areas covered by the EULEN network – banking supervision, competition, fraud, immigration, asylum, and border control.

3. Two preliminary conceptual observations should be made. On the one hand, the operation of ADM systems is based on two elements: the first is software that assists, supplements, or replaces human decision-making processes, leading (as far as this topic is concerned) to the adoption of acts or the promulgation of rules for the implementation of EU law, and which produces outputs in the form of contents, predictions, recommendations or decisions; the second element is the data that operates as input and which can be used for various purposes. On the other hand, AI systems can be conceived of as a subcategory of systems that seek to emulate human intelligence using a series of scientific approaches and technologies that we are very fast getting used to hear about (logic-based approaches, statistical approaches, machine learning, deep learning, and so on).

4. The challenge of incorporating ADM (and specifically AI) systems into EU law enforcement is to enjoy the promise of optimization of EU policies, while evading at least their most notable risks. Copying with this challenge requires different trade-offs to be achieved by EU courts and the EU legislator. Those trade-offs will plausibly depend on criteria such as: (i) the technological approach of the system – semi or fully automated systems, machine learning, deep learning, and so on, (ii) the functions it performs – red-flagging, allocation of scarce resources, provision of public services, and so on, and (iii) the area where it operates – the internal market, the area of freedom, security and justice, and so on.

5. These claims can be tested from the perspective of both effectiveness of EU law and the rule of law, and as far as the latter is concerned, in view of various of the building blocks of this EU value (Art. 2 TEU). Next, I will focus on some of the most significant of them, in terms of (mostly administrative) enforcement of EU law: the principle of legality (2), the principle of transparency (3), the duty to give reasons (4), the duty of care (5), and the principle of effective judicial protection (6). Since the aim of this paper is to offer an introductory framework for further discussion, both the analysis of these issues and the conclusions that it draws (6) are inevitably general.

2. Legality

6. ADM systems consist of software that often shapes the content of administrative action by means of abstract rules, and in this respect, they resemble administrative rule-making. Although formally they are not, in substance they fulfil a similar function, namely, to steer administrative action through abstract, general rules. This feature brings ADM systems closer to internal administrative rules and soft law instruments: they are not executive rules, but they can be used for the same purpose. For this reason, the question arises as to the role of the principle of legality in the regulation of the specific ADM systems used by European and national authorities in the implementation of EU law; and, in particular, whether or not the definition of these systems should be subject to some kind of legal programming, either by means of EU legislative acts or by legal rules of domestic law.

7. The answer is undoubtedly in the affirmative in cases where the ADM system controls or leads to the restriction of fundamental rights, since in this case the restriction must be provided for by law (Art. 52(1) CFR). This is the case on the one hand of systems used to support decisions whose content directly leads to a restriction of a fundamental right, such as personal freedom (Art. 6 CFR) or the right to asylum (Art. 18 CFR). It also applies to systems that operate in areas of law that are not in themselves fundamental rights sensitive, but whose very operation involves a restriction of a fundamental right, for example because they use personal data (Art. 8 CFR).

8. The CJEU has specified that the regulation of the processing of such data through an ADM system must be contained in legal norms, and that they must lay down "clear and precise rules governing the scope and application" of the restrictive measure (Opinion 1/15, 141). The CJEU has further specified that “scope” refers here to the "pre-established models and criteria" on which the ADM system is based, which must be specific and reliable, as well as to the databases used to obtain the system's input information, which must be up-to-date and fit for purpose (Opinion 1/15, 172). Beyond the substantive requirements, which are also developed in this CJEU case law, as well as in the case law of other courts (such as BVerfG, Judgment of the First Senate of 16 February 2023 - 1 BvR 1547/19), what is relevant here is that these issues regarding the design of the specific system have to be defined in legal rules.

9. Interestingly, this requirement is not generally established in the proposal for an AI Act (AIA), probably because it regulates the use of AI systems by both public and private subjects. The only requirement of previous legal regulation of an AI system established in the AIA is the one related to the use of real-time remote biometric identification AI systems in public spaces for law enforcement purposes, in cases where they are not exceptionally prohibited: the use of these systems must be authorised by the Member States in accordance with detailed domestic legislation (Art. 5 AIA). It should also be noted that the AIA does not provide for a similar requirement for the use of these systems by EU agencies (Europol and Frontex). However, Article 52(1) CFR and the case law of the ECJ continue to apply whenever a fundamental right is restricted.

10. However, ADM systems are not always used in the procedure for the adoption of measures restricting fundamental rights, nor do they always use personal data. The question then arises as to whether, apart from the cases in which the system triggers this requirement under Art. 52(1) CFR, its content must be regulated beforehand by law. A positive answer to this question has been sought on the basis of the application of the non-delegation doctrine, which has two main bases in EU law: the venerable *Meroni* case-law (C-9/56), which limits the possibility of delegating the exercise of the regulatory discretion conferred by the Treaty on the Commission, and Art. 290 TFEU, which prevents legislative acts from delegating the regulation of essential aspects of the subject matter to the Commission.

11. Yet for the non-delegation doctrine to be applicable, it must be understood that the decision to use an ADM system confers power on a different actor. According to proponents of this approach, this is what happens when the outcome of the ADM system, instead of supplementing the process, or assisting the decision-making authority, completely replaces it. In this case, it is argued, the system ceases to be a tool and becomes an agent. This is the cyber-delegation hypothesis, that has been defended in the USA and in the EU alike. However, whatever appeal cyber-delegation may have as a metaphor, an ADM system is not really a subject, an agent; it remains a procedure, a way of conducting an action. The fact that it may completely determine the content of the decision in a particular case does not change this, and therefore does not transform the nature of ADM systems. The same is true of those internal administrative rules or soft law instruments which regulate with absolute precision the content of the administrative decision taken in a specific case. This does not create a new actor other than the authority responsible for the final decision or the authority to which the final decision is legally attributed.

12. Moreover, the cyber-delegation hypothesis and the fundamental rights reservation of law operate differently: the latter triggers the mandate for prior legal regulation whenever fundamental rights are restricted and regardless of whether the system is fully autonomous or not, whereas cyber-delegation also requires prior legal regulation of ADM systems that do not affect fundamental rights (where it may not be indispensable), but only in cases where the system is truly autonomous (thus excluding cases where legal programming of the system would be advisable). In conclusion, the hypothesis of cyber-delegation is not only based on dubious assumptions, but also leads to less satisfactory results.

3. Transparency

13. The requirement for ADM systems to be transparent and to be known and understood by those affected by their operation is one of the generally recognised ethical principles of AI. However, when ADM systems are used by public authorities in the implementation of EU law, transparency becomes a constitutional requirement that rests on several foundations: (i) the principle of legality, which requires that the actions of public authorities can reasonably be foreseen by their addressees; (ii) the principle of accountability of public authorities, both through judicial control of their actions and through political accountability to citizens and their representatives; and finally (iii) the principle of good administration, which includes the right of access to administrative information, the right to be heard, and the right to a reasoned decision. There are, however, different options for the specific configuration of the transparency of ADM systems, and I will mention two of them below. I will next focus on the duty to give reasons.

14. The first and most ambitious strategy is the obligation to publish the code by which the system is programmed. If the ADM system functions as a set of rules determining the content of the decisions of public authorities, that is, as if it was an administrative rule, then, it is argued, it should be subject to the same requirements of publicity that apply to legal rules, requirements that guarantee the possibility for citizens to access them and to know their content. The argument is similar to that which calls for the obligation to publish, at least on the Internet, soft law instruments used by public authorities in the decision-making process.

15. The second strategy also involves ex ante publicity of the ADM system but restricts its scope to certain information and documents. The degree of transparency varies according to two factors. The first one is the content of the information to be disclosed, which may be related to the data sources that feed the system, the criteria used to weigh the input information, the basic decisions regarding the configuration of the system, or the way in which its output is integrated into the decision-making process. Transparency can also be extended to the documentation produced as part of the subsequent processes for controlling the operation of the ADM system. The second factor concerns the way in which the transparency of these documents is ensured, which may be limited to the requirement that they be made available to the competent authorities on request, that they be systematically made available to them in the context of control procedures carried out by public authorities or by specialised private bodies, that they be entered in a register to which third parties may have access, or even that private subjects may exercise their right of access to public information vis-à-vis the public authorities that develop or, more often, use it.

16. The proposal for an AIA does not include an obligation to publish the code of AI systems, even if they are high-risk systems intended for use by public authorities. Rather, it explores this second strategy by, on the one hand, imposing on providers of high-risk systems the obligation to produce technical documentation (Art. 11 AIA), to provide for a quality management system (Art. 17 AIA) and to record events during the operation of the AI system (Art. 12 AIA); on the other hand, it establishes a conformity assessment procedure (Art. 43 AIA) as well as a common European database of AI systems that will be accessible to the public (Art. 60 AIA); and finally, it gives market surveillance authorities the power to request information about the system, including data sets and source code (Art. 64 AIA).

4. Reasons

17. An alternative way of increasing transparency of ADM systems is to improve the explainability of the decisions taken in the processes in which these systems are used. Here the perspective changes: instead of constructing the transparency of ADM systems as if they were rules, i.e. ensuring that individuals and firms have prior knowledge of their content so that they can adapt their behaviour accordingly, ADM systems are treated here as a set of rules that order the exercise of discretion, and transparency is articulated according to the model of the motivation of legal acts taken by public authorities. Again, the possible concretisations of this strategy can be many and varied, ranging from the requirement that the addressee of the decision be provided with an understandable explanation in natural language, to being informed that an ADM system has been used to arrive at the decision, where appropriate with an indication of the data sources used, the characteristics of the system, its margin of error, or the way in which the output information is incorporated into the decision-making process. The AIA does not generally impose this type of obligation, except for minimum transparency requirements for certain AI systems (Art. 52 AIA).

18. In any case, the possibility for an ADM system to provide a complete motivation of the content of the output information depends very much on its complexity, and in particular on the amount and diversity of the data used, as well as on the specific technology on which the system is implemented: AI systems based on rules of the type "if A, then B" may allow an ex post reconstruction of the procedure that led to the production of a given output information; machine learning systems, on the other hand, may not be based on such rules, but on other scientific approaches, such as statistical and probabilistic models that identify patterns in massive data and make predictions. This second type of AI system is capable of automatically adjusting itself to improve its performance according to the number of hits and misses produced in a training process, with the consequence that it may not be possible to reconstruct the reasons why the output information has been arrived at from these data. This is the famous black box effect of some AI technologies.

19. This reveals some of the limitations of the project of building transparency of ADM systems, and in particular of AI, on the model of ex post motivation, and highlights the need to design effective control mechanisms of the operation of ADM systems used by public authorities. One possible way to compensate for the lack of publication of the ADM system and the difficulties of explainability is the creation of public bodies specialised in the control of AI systems used by public authorities, with full access to the software and data used by them. Another alternative is to make the system available to citizens and associations so that they can use it to identify problems. However, it is not clear that this will make the systems more transparent, but rather compensate for the lack of transparency with other mechanisms to rationalise the exercise of power.

5. Due care

20. From the perspective of the right to good administration (Art. 41 CFR), the use of ADM systems brings both benefits and risks, in particular with regard to one of its building blocks, the duty of care or due diligence. According to the latter, administrative authorities must take decisions after a fair assessment of all the relevant factual and legal circumstances of the case (positive side), leaving aside those considerations that are not relevant under the applicable regulatory program (negative side).

21. On the one hand, the greater volume of data that can be taken into account and the greater capacity for analysis of such data offered by ADM systems are reasons that in principle facilitate better compliance with the positive dimension of the principle of due care or due diligence. From this perspective, big data and ADM systems appear as allies of citizens' rights vis-à-vis EU and national authorities. On the other hand, however, some AI systems can also provide output information based on correlations they find in the data on which they have been trained, without there being a causal relationship between the elements that make up the correlation, and this can lead to the final decision being based precisely on objectively irrelevant considerations. From this other perspective, this type of ADM system may lead to a violation of the negative dimension of the principle of due diligence.

22. A related issue is the permissibility of the use of ADM systems in the exercise of discretionary powers. Germany, for example, prohibits the adoption of administrative acts by fully automated means if these acts involve the exercise of discretionary powers (Art. 35a VwVfG). One argument for excluding ADM systems from the area of administrative discretion is precisely the principle of due care, which involves the mandate to adequately weigh the circumstances of the case. The exercise of discretion requires consideration of the circumstances of the particular case and this, it is argued, cannot be done when the decision is taken by a fully automated system.

23. However, this argument does not seem convincing. It is well known that the exercise of administrative discretion can be anticipated by the adoption of internal administrative norms or soft law instruments, which establish a set of rules that associate different ways of exercising discretion to different groups of cases, to the point where discretion may progressively diminish and even disappear when the time comes to take the final decision in an individual case. In these situations, discretion is exhausted by the abstract programming of the way in which it is to be exercised (Ermessensreduzierung auf Null). But this phenomenon does not mean that the circumstances of the specific case are not taken into account, since they determine the way in which discretion is exercised. And this is precisely what happens in the case of the use of ADM systems, which suggest, for example, that if circumstances A and B are met in a particular case, the authority should grant or reject an application or open an investigation. To summarise, the prohibition of ADM systems in discretionary decisions does not seem to have a firm basis in the principle of good administration.

6. Judicial protection

24. The CJEU has explored the impact of AI systems on the fundamental right to an effective judicial protection in the *Ligue des droits humaines* ase (C-817/19). The CJEU recalls that Art. 6(3)(b) of Directive (EU) 2016/681 provides that passenger information units may process personal data (personal name records) against "pre-determined criteria" (para 194), and goes on to say that this requirement "precludes the use of artificial intelligence technology in self-learning systems ('machine learning')", that are "capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria" (para 195).

25. Moreover, the CJEU evaluates machine learning AI systems in terms of effective judicial protection: "given the opacity which characterises the way in which [they] wor[k], it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 [CFR]" (para 195). It is worth noting that the CJEU does not only censure this insofar as recital 28 of the Directive (EU) 2016/681 explicitly states that it seeks to ensure a high level of protection of the right to judicial redress, "in particular in order to challenge the non-discriminatory nature of the results obtained", but also as a matter of the fundamental right to an effective judicial remedy enshrined in Article 47 CFR, which would be violated if the court were not be able to know the "reason why a given program arrived at a positive match" (para 195).

26. This problem is exacerbated by the composite structure of the European administrative space. In the enforcement of EU law, AI systems are often used in a context of shared administration – be it within a network, in a composite procedure or using shared data. The problems this poses for the effectiveness of judicial effectiveness are well known and have begun to be addressed in the *Berlioz* saga by the CJEU, which requires some extent of transnational judicial review if some circumstances are met.

27. The expansion of big data and AI-based tools (especially machine learning correlations) will certainly aggravate these difficulties, as it will be more difficult to identify distinct acts within these administrative interactions, not only when compared to old-fashioned mutual administrative assistance requests, but also to more recent access to shared data bases by both EU and national authorities alike. Recent proposals suggest that this gap in judicial protection should be filled by more *ex ante* transparency and ongoing supervision, as well as by allowing transnational judicial review of data held by other Member States that have been used as input information. However, it is uncertain whether these and other developments will be able to meet a challenge for effective judicial protection of this magnitude.

7. Conclusion

28. Let me conclude by enumerating the main points I have made so far: (i) ADM systems used by public authorities must be subject to prior legal regulation as long as they control or determine the restriction of a fundamental right (but not in every case), and this depends very much on the functions that the system performs and the area in which it operates; (ii) the transparency of ADM systems used by public authorities must be dealt with according to a differentiated strategy that takes into account the functions that they perform and the area in which they are used; (iii) the scope and possibilities of AI systems explainability also depend on the scientific and technological approach on which they are based; (iv) the use of ADM systems by administrative authorities is ambivalent in terms of due care and either to be welcomed or strictly controlled, depending on the data sources used and the approach followed, without there being good reasons to exclude fully automated systems from the area of administrative discretion; and (v) the scientific and technological approach on which de AI system is based can pose a significant risk in terms of effective judicial protection that can be further exacerbated in areas of shared enforcement EU law.