Artificial Intelligence Must Be Used According to the Law, or Not at All

Paul Nemitz 2022-03-28T11:36:19

Democracy requires to strengthen the Rule of Law wherever public or private actors use algorithmic systems. The law must set out the requirements on AI necessary in a democratic society and organize appropriate accountability and oversight. To this end, the European Commission made several legislative proposals. In addition to the discussion on how to use algorithmic systems lawfully, the question when it is beneficial to use them deserves more attention.

Nobody should hide their responsibilities behind automation

In August 2020, when hundreds of students grouped together and shouted "f**k the algorithm" in front of the UK's Department for Education, they did not rage against the machine. Their rage was directed against the government that decided to use a tool they perceived as unjust. Even though media headlines and articles sometimes claim that "algorithms already rule our lives", the students were not confused about who was responsible. Even if certain decision-making processes are automated, a "rule of the algorithm" shall and does not exist. There must always be someone, either a legal or natural person, who uses the algorithm and can be held responsible. In some cases, this use can be a challenge for the respect and enforcement of applicable legislation, where a system is used without adequate safeguards and quality controls to automate or support decision-making processes or for activities such as surveillance, this may violate the rights of individuals. Such violations can occur at great scale, depending on how broadly a system is used, and they can be difficult to prevent or detect when the system is not sufficiently transparent, or people remain unaware of its use. For example, the automated inference of information about people can affect their privacy and data protection rights. Another example is that bias in algorithms or training data of AI systems can lead to unjust and discriminatory outcomes.

The use of automated systems can also affect many other rights laid down in the European Charter of Fundamental rights, such as those to human dignity, good administration, consumer protection, social security and assistance, freedom of expression, freedom of assembly, education, asylum, collective bargaining and action, fair and just working conditions, access to preventive care, or cultural and linguistic diversity. If those systems are used in the context of law enforcement or the judiciary, they can also affect the presumption of innocence and the right to fair trial and defense.

The inaccessibility or non-existence of relevant information on automated systems impedes effective enforcement of fundamental rights obligations, secondary law and access to legal remedies. In addition, we sometimes see a tendency to design for purposes of deception and for evading responsibility. For example, certain car makers designed an algorithm that recognized when a car was being tested for exhaust fumes, to produce false test results which would not correspond to the real emissions in normal traffic. And in the *Right to be Forgotten/Google Spain* Case before the European Court of Justice, Google tried to dissociate its responsibility from the performance of its search algorithm, with the argument that it was fully automated, and that Google would not be responsible for the search results as a company or as a controller under the General Data Protection Regulation (GDPR). Thankfully, the European Court of Justice did not accept this early effort to create a new “irresponsibility defense”.

A coordinated European approach to ensure that people rule the algorithms[1)]This section is an adapted reproduction of passages from the 2021 annual report on the application of the Charter of fundamental rights

To address the challenges identified in the previous section, in April 2021, the European Commission presented a proposal for a Regulation on AI (AIA). Key objectives of the proposed AIA are the protection of fundamental rights and safety. The proposal aims to ensure that high-risk AI systems are designed and used in compliance with fundamental rights and that competent national authorities and courts can more effectively investigate and address possible breaches of fundamental rights obligations.

The proposal follows a risk-based approach. Certain AI systems are prohibited outright, such as the use of remote biometric identification systems in publicly accessible spaces for law enforcement purposes, unless clearly defined exceptions and safeguards apply (Art. 5.1.d and 5.2).

High-risk AI systems will need to comply with a set of requirements (Art. 8-15). Those requirements ensure appropriate documentation and testing of high-risk AI systems, as well as adequate data quality, traceability, human oversight, robustness, accuracy and cybersecurity. They will apply where AI systems are used in critical areas, such as biometric identification, education, employment, essential public and private services, such as credits, or public assistance benefits, law enforcement, migration and border control, and the judiciary (Annex III).

The proposal ensures that the users of AI systems, such as companies interacting with clients, or public authorities taking decisions, are provided with adequate information from the developers of the systems to ensure suitable use of their applications and to enable them to fulfil their obligations under fundamental rights law (Art. 13).

Should infringements of fundamental rights occur through the use of AI systems, effective redress for affected persons will be facilitated by means of transparency and traceability of AI systems, coupled with strong ex post controls by competent authorities. Supervisory authorities in charge of enforcing fundamental rights, such as data protection authorities, equality bodies or consumer bodies, will have access to all documentation on high-risk AI systems that fall within their mandate and they will be able to cooperate with market surveillance authorities to test the respective AI systems where needed (Art. 64).

For specific AI systems, transparency obligations (Art. 52) towards affected people will minimize the risk of manipulation, in particular, in the case of chat bots (computer programs that can answer questions in an online chat) or 'deep fakes' (artificially generated or manipulated image, audio or video content that resembles existing people, objects, places or other entities or events and which falsely appear to be authentic or truthful).

The AIA proposal is currently under negotiation with the co-legislators. It will work jointly with other existing and proposed legislation laying down substantive rules for the use of AI systems in clearly targeted contexts, and it will work jointly with other legislation that is applicable to automated systems without having specific rules on the technology or its use. It is important to look at the AIA proposal together with these other elements, because the different initiatives and laws are designed to complement and strengthen each other. When the Commission receives criticism about lacking provisions in a particular proposal, the explanation for this lack is sometimes that the matter is addressed elsewhere. Given the increasing importance of automation in different areas of daily life, the corpus of relevant laws and proposals is growing.

For example, when automated systems are used to process personal data, the GDPR is fully applicable. Many of the rights and obligations set out in the GDPR will thus have to be respected in the design and use of AI systems, such as the information rights, including notably in case of automated processing that affects rights of individuals, as set out in Articles 13-15 and 22 of the GDPR.

When automated systems are used on platforms like social networks, this will have to be done in compliance with the proposal for a Digital Services Act, adopted by the Commission in December 2020, which is currently under discussion by the co-legislators. It frames the responsibilities of online intermediaries. Without prejudice to sector-specific EU rules such as those on copyright or terrorist content online, it provides a single horizontal set of rules in the EU for a balanced governance of online content moderation.

This would apply jointly with the proposed Regulation on transparency and targeting of political advertising, adopted by the European Commission in November 2021, as part of measures aimed at protecting election integrity and open democratic debate. These proposed rules would require any political advertisement to be clearly labelled as such and include information such as who paid for it and how much. Political targeting and amplification techniques would need to be explained publicly in unprecedented detail and would be banned when using sensitive personal data without the explicit consent of the individual.

In addition, in June 2021, the European Commission adopted a new proposal for a Directive on consumer credits repealing and replacing the current Consumer Credit Directive. It proposes rules in relation to granting credits to consumers according to which Member States will have to ensure documentation of procedures and information used in creditworthiness assessments (Art. 18.3). Furthermore, the assessments will have to be based on relevant and accurate information on financial and economic circumstances (e.g. income and expenses) and should not be based on data such as social media data (Art 18.2 and recital 47). Consumers will also have the right to an explanation (Art 18.6) on how a decision on their creditworthiness was reached, to express their point of view and to obtain human intervention, mirroring the principles of the GDPR concerning automated decision-making. The proposal is currently under negotiation with the co-legislators.

In December 2021, the European Commission has proposed a Directive to improve working conditions for platform workers at the EU level by ensuring correct determination of their employment status, by promoting transparency, fairness and accountability in algorithmic management in platform work and by improving transparency in platform work. This proposal is also under negotiation with the co-legislators.

There is much more work ahead

To enforce the abovementioned laws and other rules, states, rights holders and civil society will face an increasing need for technological capacities. Those who need to comply with these rules will have similar demands. We are not at the advent of any “rule of the algorithm”. However, in the face of increasingly complex automated systems used in ways that are relevant for the functioning of our societies, it will take great efforts to rule over the algorithms used already today. The law will have to be further developed, alongside new technologies to support its application and enforcement.

The law is a noble expression of democracy and we must ensure its enforcement. At the same time, democracy and the principle that the way things are done in a society must be open for change also has implications for the use of AI and other forms of automation.

In the light of these challenges, it seems useful to examine in each particular situation whether the use of a specific automated system is actually an improvement. As Julia Powles observed, when it comes to artificial intelligence, there is often a lot of discussion on how to use it, but very little on whether using it would be appropriate: “The endgame is always to “fix” A.I. systems, never to use a different system or no system at all.”

There is so much rhetoric about the declared benefits of AI tools, notably about efficiency, it sometimes seems as if there was a common belief that any AI system would always amount to an efficient solution, notwithstanding needs for adaptation and maintenance, the bureaucracy to ensure an appropriate data management, or challenges to ensure a lawful and reliable use. This enthusiasm deserves more scrutiny. Not every task is best fulfilled by means of automation. Especially in contexts that require genuine understanding of the objectives and the situation at hand, automation might be less efficient and reliable.

While public entities usually have to ensure good administration to the extent possible, private parties are free to use flawed tools as long as they do not break the law. In hiring, for instance, a number of automated tools are marketed with promises about the information these tools supposedly generate about applicants when analyzing data about them, and about the efficiency gains this would bring for potential employers. Often enough, there is little evidence to back these claims. At the same time, there is a growing realization in academia and among companies that employers are missing out on good candidates when they use certain software to scan CVs. If a tool is already implemented and does not work as intended, it can be challenging to fix it, especially when it is provided by a third party.

Another way to avoid the “rule of the algorithm” is therefore not to use one where it does not work properly or even causes a loss of control over the way tasks are carried out. Thoroughly examining its suitability before deploying an automated system is good advice also beyond legal compliance.

Automation in the public sector in countries such as Germany usually requires a specific legal basis. So far, these only exist where the law is very “numerical”, thus for example in the area of taxation and social support, when it comes to the calculation of obligations or benefits. However, the law excludes the use of automated systems for administrative acts wherever these require the use of discretion. Only a human can exercise discretion. This principle of binding the introduction of automation to the need for an explicit legal basis is a key safeguard of democracy, through the rule of law, against technological automation that could otherwise risk undermining democratic accountability.

It will be key for democracies to assess any use of automated systems in the exercise of public authority, as to the affordances of the system to accommodate democratic political change, at which costs and with which speed. Democracy in the smart city, for example, cannot be locked into technological systems that are too expensive to adapt once a new political majority takes over. Before deploying AI systems in any sector that is subject to political choices, from education via health through to mobility or law enforcement, we must ask the question whether the system will be as efficient and open to incorporating and operationalizing a democratic change of direction in these policies as humans are. We must also ask the question whether the automated system affords criticism, interrogation, and the drive for change born out of frustration with the present, which are key to innovative and progressive societies. So far, it is judges who dissent, teachers and students who protest, or doctors who try new methods outside the traditional path, to give some examples, which are at the core of creativity, innovation and progress. So far, we have not seen such capacities in any technological system. We must avoid technological conservatism that results in a lock-in situation when moving tasks from humans who have those capabilities to machines, which do not. The way must be open for change, also in the digital age.

The authors express their personal opinion and not necessarily that of the European Commission.

References

- This section is an adapted reproduction of passages from the 2021 annual report on the application of the Charter of fundamental rights