Article 5 of the AI Act can benefit from a better integration of law and code (an architectural standpoint)

Memorandum

Ilona Masiuk

July 24 2023, Amsterdam

1 Objectives

This memorandum dissects Article 5 of the Artificial Intelligence Act with the purpose of identifying key legal-technological opportunities for establishing a stable and minimally restrictive legal environment around the use of AI systems. At the moment, Article 5 adopts a unilateral focus on the mitigation of social risks through complete prohibition of the use of AI in a number of application scenarios [1]. By contrast, the adoption of an integrative Law + Technology approach would allow to combine harm prevention with value generation while supporting existing regulatory objectives [2]. The goal of this memorandum is to briefly survey Article 5 in terms of aspects that either support or fall short of incorporating the principles of Law + Technology and to discuss prospective integration pathways for law and code.

2 Context

The Law + Technology regulatory framework consists of two complementary paradigms aimed at integrating law into technology and vice versa. These paradigms are titled Code as Law and Law as Code respectively. Under Code as Law, the code is engineered to directly reflect legal boundaries [2]. In other words, the scope of the user's legal behaviour is defined through the architecture of the technology. Law as Code in turn presupposes the treatment of legal texts as machine-readable code, opening new horizons for the way the law can be enabled or enforced [2]. Through this integration, both approaches offer regulators new instruments for devising legal environments that are preventive of the harms and inclusive of the benefits technology gives rise to.

3 Discussion

Paramount to appraising the extent to which the original Article warrants modification is not only the identification of prospective stumbling blocks but also the Article's existing fortes. In assessing the impact of rapid technological and economic transformations the world has witnessed in the beginning of the 20th century, [3] makes an argument that the technology should not be directly equated with the detriment caused by its use, for it is always a means to economic ends. In the same line of thinking, it is reasonable to assert that the risk borne by AI systems ought to be evaluated through the purposes that they serve. [2] also cautions against not drawing the distinction between technologies whose architecture leads to harm and those whose use causes it. Both these perspectives are latently present in Article 5: the Article opts for prohibiting specific use cases and avoids drawing the limits of the ban based on architectural specifics of AI systems. In placing the emphasis on unfavourable application scenarios rather than types of architecture differentiating one technology from another, the current version of the Article acts to preserve all existing types of AI. This

approach successfully bypasses the 'technology extinction' pitfall highlighted in [2], adding no negative impact to technological innovation per se.

Despite indirectly protecting innovation and technological diversity, the Article features no propositions on leveraging architecture to assist its objectives, in spite of it being a major regulatory factor[4]. Moreover, clause d of the Article introducing the prohibition on the use of AI systems considered 'real-time' appears to be in potential violation of the 'fair warning' principle [5]. The idea of 'fair warning' mandates that legal notions have a sufficient degree of precision so as to accurately inform the citizens of the scope of (il)legal activities [5]. The current text of the legislation contains no information on discriminating between 'real-time' and non-'real-time' systems, creating ambiguity for the subjects of the regulation. This absence of a clear definition is detrimental to the law's enforceability in a number of ways. Namely, the uncertainty associated with whether a system can be considered real-time threatens compliance among the subjects by making liability questionable and lays the ground for selective enforcement by relevant authorities. One of the ways to address this uncertainty is to jointly adopt the Code as Law and the Law as Code approaches. In other words, the legal definition of 'real-time' currently absent from the article may be built around computational estimates produced by the systems at hand and then integrated directly back into their architecture. For instance, for the task of subject detection and and identification, a system given a 'real-time' input would take some minimal amount of time to produce its output. Such an interval could then be considered the bottomline definition of 'real-time'. Such benchmarks could then be augmented with a legal interpretation to achieve better generalisability. Elaborating what 'real-time' entails by superimposing computational and regulatory definitions would allow to strike a balance between case-by-case variability and general proscriptions. Most importantly, introducing a clear definition of 'real-time' systems would aid in reducing legal uncertainty and help the subjects effectively differentiate between real-time and non-real-time systems. Furthermore, increasing the precision of the law to the point of making it machine-readable would present the opportunity to capitalise on the Law as Code approach. In particular, converting legal definitions into clear temporal constraints could enable compliance by design. Compliance by design solutions could in turn maximise the benefits of using the most task-appropriate technology while still meeting the legal requirements for its use. For instance, for a given non-compliant system operating in 'real-time' measures as simple as delays could be implemented to render it in line with the legislation. The architectural integration of law and code with respect to the definition of 'real-time' AI would therefore address the triple challenge posed by the original text of the legislation: it would better satisfy the 'fair warning' principle, improve compliance and support technological innovation.

4 Conclusion

The amendments to Article 5 of the AI Act proposed in this document are aimed at capitalising on the integrative capabilities of the Law as Code and Code as Law paradigms [2]. In particular, this memorandum offers a detailed argument for a more precise definition of 'real-time' systems, which coupled with a deeper architectural integration of law and code could simplify compliance, better align with the principle of 'fair warning' [5] and support minimally restricted software design. This serves to show that the adoption of a broader regulatory perspective allowing for complementary support between law and technology yields the power to not only better achieve the preventive objectives of the current legislation but to help further devise benefit-maximising methods of AI governance.

5 References

[1] European Commission, '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', 2021. Accessed: July. 20, 2023. [Online]. Available: `https://artificialintelligenceact.eu/the-act/`

[2] T. Schrepel, "Law + technology," SSRN Electronic Journal, 2022. `doi:10.2139/ssrn.4115666`

[3] S. Zuboff, The Age of Surveillance Capitalism: The Fight for the Human Future at the New Frontier of Power. London: Profile Books, 2019.

[4] L. Lessig, Code: Version 2.0. New York, USA: Basic Books , 2006.

[5] G. K. Hadfield, "Weighing the value of vagueness: An economic perspective on precision in the law," California Law Review, vol. 82, no. 3, p. 541, 1994. `doi:10.2307/3480972`