Sandboxes for Responsible Artificial Intelligence

Florina Pop and Lukas Adomavicius

Introduction

Keeping up with the pace of technological developments and innovation is a challenge for lawmakers in Europe. As a result, new approaches are being explored in order to address the perception that law-making lags behind technological innovation, or even obstructs its development.[1]

One of the most disruptive and promising technologies is artificial intelligence (AI). The possibilities to use AI to improve various processes in health, businesses or the public sector seem unlimited, but AI also raises concerns with respect to data protection and fundamental rights.

As AI technologies became more and more prominent, the European Commission developed an AI Strategy, published in 2018. The centrepiece is the proposal for an AI Regulation (Artificial Intelligence Act Proposal) submitted in April 2021.

One of the novelties introduced by this proposal is the creation of AI 'regulatory sandboxes'. This Briefing will explain what regulatory sandboxes are, and how they fit within the concept of 'legally disruptive experimentation'. It also asks whether the regulatory sandboxes may themselves pose challenges regarding personal data protection in the context of the AI Act Proposal and its possible loopholes.

Regulatory sandboxes

What are regulatory sandboxes?

The term 'regulatory sandbox' can be traced back to the financial technology, where regulatory sandboxes have existed since 2014, mainly in the UK. The term can be generally defined as a testbed for a selected number of projects where certain laws or regulations are set aside, and the project receives guidance and monitoring from a competent authority.[2]

The proposal does not provide a definition, but Article 54 states that AI regulatory sandboxes: 'shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time'. In order to understand the concept of AI regulatory sandboxes, one has to explore how it fits within the broader notion of experimental law-making.

What is legally disruptive experimentation?

An experimental legal regime (or experimental approach to legislation) encourages actors to test new technologies or services in a real-life environment. Three main features characterise an experimental legal regime: temporary nature, trial-and-error approach to regulation, and collaborative involvement of stakeholders or competent authorities in the process. In practice, an experimental legal regime, or an AI regulatory sandbox, requires the actor to present a proposal that would explain the objectives, process, and expected results to the competent authority, as well as details such as sample size and experimental period length.

Legal experimentation can be divided into two key types: experimenting by derogation and experimentation by devolution.[3] Experimenting by derogation implies that certain rules or regulations are put aside to complete the experiment. It requires the legislator to include an experimental clause in a legislative basis to enable the experiment to derogate from a

[1] Thomas Wischmeyer and Timo Rademacher, *Regulating Artificial Intelligence* (Springer 2020) <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2320666>.

[2] Sofia Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3839744> accessed 27 July 2021.

[3] Michiel A Heldeweg, 'Experimental Legislation Concerning Technological & Governance Innovation - an Analytical Approach' (2015) 3 The Theory and Practice of Legislation 169.

specific law. Experimentation by devolution requires a national or supranational government to empower the local government to establish a regulation or law in a particular area relevant to the experiment. It allows policy differentiation between government levels, so that decisions can be taken at a local level taking into account local preferences and needs. Thus, devolution potentially creates a policy laboratory and stimulates innovation.

What are the benefits and shortcomings of regulatory sandboxes?

Regulatory sandboxes make it possible to test new technologies transparently and contribute to evidence-based lawmaking. From a market actor perspective, one of the main benefits is the additional flexibility in terms of regulatory burden. In addition, the controlled environment of regulatory sandboxes is particularly accommodating to products and services that do not easily fit the traditional regulatory framework.[4]

However, they also present several shortcomings. For instance, the crucial design phase raises concerns with regard to proper methodological assessment. Moreover, if the project is applied to a very small sample, it may not represent the possible impact on the larger part of society.

Personal data protection and AI regulatory sandboxes

Are there risks from derogation?

Concerns are also expressed as to whether the Commission has envisaged a derogatory instrument that would allow the private entities to test their new AI systems, under the supervision of the competent national authorities, in a de-regulated space. Such an instrument could lower regulatory barriers in the sense that private entities processing personal data will not be obliged to comply with all the applicable data protection requirements when testing their AI systems.[5]

The AI Regulation specifically clarifies that the purpose of the regulatory sandboxes is 'to ensure compliance of the innovative artificial intelligence system with the Regulation and other relevant Union and Member States legislation' including data protection legislation. Moreover, for the AI systems that involve the processing of personal data, the national data protection authorities (DPAs) are appointed as the gatekeepers of the AI regulatory sandboxes.

The European Data Protection Supervisor (EDPS) will also play an essential role, giving detailed guidance through its established AI regulatory sandboxes, but also supervising compliance and applying fines to EU institutions, agencies and bodies when they fall within the scope of the AI Regulation.

At the time of writing (September 2021), it seems premature to conclude that the instrument providing a legal basis for the AI regulatory sandboxes will have a derogatory nature. Moreover, with DPAs having gatekeeper functions in the AI regulatory sandboxes, it is improbable that we will see overall or broad exemptions from the data protection legislation. The mere consultative and 'regulatory comfort' type of sandboxes seem to be the position of the national data protection supervising authorities, that have established AI regulatory sandboxes even before the publication of the AI Proposal.

Possible loopholes endangering personal data protection

Another point of concern is the proposed Article 54 on the further processing of personal data provisions for developing certain AI systems in the public interest in the AI regulatory sandbox. Are these provisions intended to apply as *lex specialis* (and thus override the General Data Protection Regulation (GDPR)) or merely to complement the existing provisions in the data protection legislation?

The purpose limitation principle (Article 5(1)b) of GDPR, and its provisions related to the lawfulness of processing (Article 6(4)), clearly set up the criteria to be considered when a controller intends to further process personal data for a purpose other than that for which the personal data have been collected.

[4] Deirdre Ahern, 'Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon' [2021] European Business Organization Law Review 1.

[5] Ranchordas (n 2).

The main criteria is for the new purpose not to be incompatible with the initial envisaged purpose that was communicated to the data subject. The proposed Article 54 of the AI Regulation seems to exempt controllers from their obligation to conduct this compatibility test when they use the personal data to test AI systems developed for safeguarding substantial public interests.

So even though those personal data have been collected initially for another purpose, and processing those data could be lawfully performed only after balancing between the controller's interests and the data subject's interests, the AI Regulation seeks to derogate from Article 6(4) of the GDPR. The EDPS has already stated that it is important to clearly avoid in the AI Regulation any inconsistency and possible conflict with the GDPR (EDPS/EDPB, Joint Opinion on AI Regulation).

Clarifying the application of such provisions in the final version of the Regulation that is adopted will be essential before any implementing acts are adopted so that it leaves no discretion in the further use of personal data.

Conclusions

The challenges posed by the AI disruption most certainly pressured the European Commission to opt for more flexibility when drafting the AI legal framework. The obvious objective of this approach is to support innovation and small-scale providers and, in the background, to move away from the criticism that EU regulatory cautiousness hamstrings innovation.

Whether the AI regulatory sandboxes will prove to be innovation-friendly even without compromising on personal data processing requirements is yet to be seen. The GDPR is a recent piece of legislation and its application to certain AI systems has not been tested yet. A provision initially construed as a show-stopper for the processing of personal data when training, developing and testing of certain AI systems could, under the interpretation and guidance of the data protection supervisory and monitoring bodies, lead to different outcomes or, if not, permissible solutions.

Even so, without a data protection derogatory instrument, the advantages that can result from the use of regulatory sandboxes to test AI are manifold. First, the mutual and continuous learning and exchange of information processes offers the private stakeholders a real-world environment in which to test their novel AI systems, while also giving the regulatory body - in this case the DPAs and EDPS - a better understanding of the benefits and risks related to a certain AI system deployed in different industries or public sector. Secondly, all the actors involved in the regulatory sandboxes will work together to identify how data protection by design is to be integrated within these new disruptive technologies. And thirdly, on a larger scale, the exchange of best practices, lessons learned, and recommendations among the Member States will address the existing fragmentation on the AI systems market.

www.eipa.eu

Postal address
P.O. Box 1229
6201 BE, Maastricht
The Netherlands

Visiting address
Onze Lieve Vrouweplein 22
6211 HE, Maastricht
The Netherlands

Contact
+31 43 32 96 222
info@eipa.eu