WHAT IS REGULATORY SANDBOXING FOR AI?

For this brAInfood, the Knowledge Centre Data & Society asked Katerina Yordanova, researcher at CiTiP (KU Leuven), to demystify regulatory sandboxing for AI.

"Regulatory sandbox is described as a "safe space", an environment where a business can test new innovative products and services (business models or delivery mechanisms) with mitigated risk of imposed sanctions and in close collaboration with and assistance of national regulators."

- Katerina Yordanova

Despite the perceived benefits of regulatory sandboxing, the concept significantly varies between countries and jurisdictions accross the EU.

This brAInfood answers some of the most pressing questions on regulatory sandboxing for AI.

Katerina Yordanova, researcher at CiTiP, specializing in the area of human rights law in the digital environment and business and human rights. She is carrying out research in the area of AI and its implications on human rights, smart manufacturing, and business and human rights in the context of digital supply chains.

Knowledge Centre Data & Society (2020). What is regulatory sandboxing for AI? brAInfood of the Knowledge Centre Data & Society. Brussels: Knowledge Centre Data & Society.

brAInfood of the Knowledge Centre Data & Society

Who will want to test AI systems in regulatory sandboxes?

"The entities that usually benefit from a regulatory sandbox are **start-ups and other businesses**, but also **the public sector**. There should be no barrier regarding who can test their products or services, as long as they meet the other requirements that are set by the authority that conducts the sandbox."

To which regulation does the tested AI application need to adhere to?

"The scope **depends on the authority that is going to conduct the sandbox** and the leeway it has according to its mandate. What is certain, however, is that a national authority would not be able to lift or amend requirements during the sandbox process, when those requirements are established by EU law. There are certain views that a central EU body would be allowed to do this instead of the national authorities, but it is debatable if the EU treaties provide such legal ground."

[1] UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Where would a regulatory sandbox take place?

"Usually the experiment takes place **in a real market environment under the supervision of the respective authority**. In order to guarantee the rights of third persons, however, the test could be conducted on a limited scale (for example the service would be provided for a limited number of people) and the third parties need to understand they participate in this test and agree to it."

Whose (personal) data will be used, and will it be possible for them to opt out?

"The products or services that are tested in a sandbox are in a state ready to market. Typically, **data has already been used to train a potential AI system**. Use of personal data is always possible in a sandbox. This is the reason why authorities such as ICO[1] have their own sandboxes where they try to test how the technologies would affect **the right to data protection and/or the right to privacy**.

One of the requirements for such tests is **transparency** for the individuals who are going to participate in the test and whose data will be used. Another requirement are adequate **protection mechanisms** that would mitigate any risk as much as possible.

Of course, if a product or service turns out to affect personal data in a manner that is incompatible with data protection legislation, and there is no way to fix this, the product or service won't get to market."

Which AI systems are most interesting to test within regulatory sandboxes?

"Undoubtedly **AI systems that affect more than one domain would be the most interesting and allegedly difficult to be tested**. An example of such system would be a financial technology system that offers and grants a variety of financial services and products, but at the same time processes personal data, such as biometric identification. The more complex a product or service is, the more it needs to be tested in diverse scenarios."

What happens if the sandboxing experiment goes wrong and harm is done?

"Participating in a sandbox does not mean immunity from jurisdiction. In fact, what most of the European authorities offer during the sandbox process is **letters of negative assurance and comfort from enforcement** (i.e. an accidental breach of legislation may not lead to immediate enforcement action). Even if the waiver of some rules is allowed by the regulator, such 'privilege' can be lifted at any moment by the regulator (e.g. if it is established that 'the benefits outweigh the risk' or consistent non-compliance). To put it in layman's terms, if some rights are breached, the regulator will usually **allow some time so the mistake could be fixed, but any damages need to be indemnified**."

With the support of KU LEUVEN CiTiP CENTRE FOR IT & IP LAW