

## WAT IS

# 'REGULATORY SANDBOXING'

## VOOR AI?

Voor deze brAlnfood vroeg het Kenniscentrum Data & Maatschappij aan Katerina Yordanova, onderzoekster bij CiTIP (KU Leuven), om 'regulatory sandboxing' voor AI te verduidelijken.

"Een 'regulatory sandbox' wordt omschreven als een 'veilige ruimte', een omgeving waar een bedrijf nieuwe innovatieve producten en diensten (bedrijfsmodellen of leveringsmechanismen) kan testen met een beperkt risico op opgelegde sancties en in nauwe samenwerking met en met de hulp van nationale regelgevers".

– Katerina Yordanova

Ondanks de vele voordelen van 'regulatory sandboxes', kan het concept sterk verschillen tussen landen en jurisdicties in de EU.

Deze brAlnfood beantwoordt enkele prangende vragen over 'regulatory sandboxing' voor AI.

Disclaimer: De vragen en antwoorden werden vrij vertaald vanuit het Engels (zie [Engelstalige brAlnfood](#) rond 'regulatory sandboxing for AI').

Katerina Yordanova, onderzoekster aan CiTIP, is gespecialiseerd in wetgeving rond mensenrechten in digitale omgevingen en in het bedrijfsleven.

Kenniscentrum Data & Maatschappij (2020). Wat is 'regulatory sandboxing' voor AI? brAlnfood van het Kenniscentrum Data & Maatschappij, Brussel: Kenniscentrum Data & Maatschappij.

Dit document is beschikbaar onder een CC BY 4.0 licentie.

brAlnfood van het Kenniscentrum Data & Maatschappij



### Wie zal AI-systemen willen testen in 'regulatory sandboxes'?

"De entiteiten die gewoonlijk gebruik maken van een 'regulatory sandbox' zijn **start-ups** en **andere bedrijven**, maar ook de **publieke sector**. Er mag geen obstakel zijn inzake wiens producten of diensten kunnen getest worden, zolang zij voldoen aan de andere eisen die worden gesteld door de autoriteit die de 'sandbox' beheert."

### Aan welke regelgeving moet de geteste AI-toepassing voldoen?

"Dit **hangt af van de autoriteit die de 'sandbox' zal beheren** en de ruimte die deze heeft volgens haar mandaat. Alleszins, een nationale autoriteit zou niet in staat kunnen zijn om vereisten op te heffen of te wijzigen tijdens het 'sandbox'-proces, wanneer deze vereisten werden vastgesteld in de Europese wetgeving. Sommigen zijn van mening dat een centraal EU-orgaan hiervoor beter geschikt is, in plaats van de nationale autoriteiten. Maar het is betwistbaar of EU-verdragen hier wel een rechtsgrond voor bieden."

<sup>1</sup> Onafhankelijk orgaan van het Verenigd Koninkrijk dat werd opgericht om informatierechten in het publieke belang te handhaven, én om openheid bij overheidsorganen en gegevensbescherming bij personen te bevorderen.

### Waar zou een 'regulatory sandbox' plaatsvinden?

"Meestal vindt het experiment plaats in een **echte marktomgeving onder toezicht van de desbetreffende autoriteit**. Om de rechten van derden te waarborgen, kan de test op een kleinere schaal worden uitgevoerd (de dienst wordt bijvoorbeeld aan een beperkt aantal personen verleend) en de derden moeten begrijpen dat zij aan deze test deelnemen en hier ook mee instemmen."

### Wiens (persoons)gegevens worden gebruikt? Kunnen zij zich terugtrekken uit de 'sandbox'?

"De producten of diensten die in een 'sandbox' worden getest, zijn markt klaar. Meestal werden **al gegevens gebruikt om een potentieel AI systeem te trainen**. In een 'sandbox' is het gebruik van persoonsgegevens altijd mogelijk. Daarom hebben autoriteiten zoals ICO<sup>1</sup> hun eigen 'sandboxes' waar ze testen hoe technologieën het **recht op gegevensbescherming en/of privacyrecht** kunnen beïnvloeden.

Een van de vereisten voor dergelijke tests is **transparantie** voor diegenen die zullen deelnemen aan de test en wiens data zullen worden gebruikt. Een andere vereiste zijn adequate **beschermingsmechanismen** die de risico's zoveel mogelijk beperken.

Indien een product of dienst persoonsgegevens beïnvloedt, op een manier die onverenigbaar is met het recht op gegevensbescherming, en dit niet kan opgelost worden, zal het product of de dienst niet op de markt komen."

### Welke AI-systemen zijn het interessantst om te testen in 'regulatory sandboxes'?

"Ongetwijfeld zijn **AI-systemen die meer dan één domein beïnvloeden het interessantst en het moeilijkst om te testen**. Een voorbeeld van zo'n systeem is een financieel technologisch systeem dat een verscheidenheid aan financiële diensten en producten aanbiedt en toekent, maar tegelijkertijd persoonsgegevens verwerkt, zoals biometrische identificatie. Hoe complexer het product of de dienst, des te belangrijker het te testen in diverse scenario's."

### Wat gebeurt er als het 'sandbox'-experiment misloopt, en er schade is aangericht?

"Deelnemen aan een 'sandbox' betekent geen immuniteit van jurisdictie. De meeste Europese autoriteiten zullen tijdens een 'sandbox'-experiment milder zijn bij toezicht (d.w.z. een toevallige inbreuk op de wetgeving kan niet leiden tot onmiddellijke handhavingsacties). Zelfs als de toezichthouder sommige regels onthefte, kan dit 'privilege' op elk moment door de toezichthouder worden opgeheven (bv. als wordt vastgesteld dat 'de voordelen zwaarder wegen dan het risico' of wanneer er sprake is van consequente niet-naleving). Kortom, **bij schending van sommige rechten, geeft de regelgever enige tijd om de fouten recht te zetten, maar mogelijke schade moet worden vergoed.**"