WAS IST REGULATORISCHES SANDBOXING FÜR KI?

Für dieses brAInfood hat das Knowledge Centre Data & Society Katerina Yordanova, Forscherin am CiTiP (KU Leuven), gebeten, das Thema regulatorisches Sandboxing für KI zu erklären.

"Die regulatorische Sandbox wird als "sicherer Raum" beschrieben, eine Umgebung, in der ein Unternehmen neue innovative Produkte und Dienstleistungen (Geschäftsmodelle oder Bereitstellungsmechanismen) mit geringerem Risiko für verhängte Sanktionen und in enger Zusammenarbeit mit und Unterstützung von nationalen Regulierungsbehörden testen kann."
- Katerina Yordanova

Trotz der vermeintlichen Vorteile des regulatorischen Sandboxing unterscheidet sich das Konzept zwischen den einzelnen Ländern und Gerichtsbarkeiten in der EU erheblich. Dieses Brainfood beantwortet einige der wichtigsten Fragen zum regulatorischen Sandboxing für KI.

Katerina Yordanova, Wissenschaftlerin am CiTiP, ist spezialisiert auf die Bereiche Menschenrecht im digitalen Umfeld und Wirtschaft und Menschenrechte. Sie forscht im Bereich KI und deren Auswirkungen auf die Menschenrechte, Smart Manufacturing sowie Wirtschaft und Menschenrechte im Kontext digitaler Lieferketten.

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

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

Wer will KI-Systeme in regulatorischen Sandboxen testen?

"Die Einrichtungen, die in der Regel von einer regulatorischen Sandbox profitieren, sind **Start-ups und andere Unternehmen**, aber auch **der öffentliche Sektor**. Es sollte keine Barriere geben, wer seine Produkte oder Dienstleistungen testen darf, solange sie die anderen Anforderungen erfüllen, die von der Behörde, die für Sandbox verantwortlich ist, vorgegeben werden.

An welche Vorschriften muss sich die getestete KI-Anwendung halten?

"Der Umfang **hängt von der Behörde ab, die die Sandbox verantwortet** und dem Spielraum, den sie gemäß ihrem Mandat hat. Sicher ist jedoch, dass eine nationale Behörde nicht in der Lage wäre, Anforderungen während des Sandbox-Prozesses aufzuheben oder zu ändern, wenn diese Anforderungen durch EU-Recht festgelegt sind. Es gibt Stimmen, die die Meinung vertreten, dass ein zentrales EU-Gremium dies anstelle der nationalen Behörden tun dürfe, aber es ist fraglich, ob die EU-Verträge eine solche Rechtsgrundlage bieten."

[1] Die unabhängige britische Behörde zur Wahrung der Informationsrechte im öffentlichen Interesse, zur Förderung der Transparenz von öffentlichen Einrichtungen und des Datenschutzes für Einzelpersonen

Wo findet eine regulatorische Sandbox statt?

"Normalerweise findet das Experiment in einer realen Marktumgebung unter der Aufsicht der jeweiligen Behörde statt. Um die Rechte Dritter zu gewährleisten, könnte der Test jedoch auch in einem begrenzten Umfang durchgeführt werden (z. B. wenn der Dienst nur einer begrenzten Anzahl von Personen zur Verfügung gestellt wird) und sie müssten darüber informiert werden, dass sie an dem Test teilnehmen und diesem zustimmen."

Wessen (persönliche) Daten werden verwendet, und besteht die Möglichkeit, der Teilnahme zu widersprechen?

"Die Produkte oder Dienstleistungen, die in einer Sandbox getestet werden, befinden sich in einem marktreifen Zustand. Typischerweise **wurden bereits Daten verwendet, um ein potenzielles System zu trainieren**. Die Nutzung von personenbezogenen Daten ist in einer Sandbox immer möglich. Das ist der Grund, warum Behörden wie das ICO[1] ihre eigenen Sandboxen haben, in denen sie versuchen zu testen, wie sich die Technologien auf **das Recht auf Datenschutz und/oder das Recht auf Privatsphäre** auswirken würden.

Eine der Voraussetzungen für solche Tests ist die **Transparenz** für Personen, die an dem Test teilnehmen und deren Daten verwendet werden. Eine weitere Voraussetzung sind angemessene **Schutzmechanismen**, die jedes Risiko so weit wie möglich minimieren sollen. Wenn sich herausstellt, dass ein Produkt oder eine Dienstleistung personenbezogene Daten in einer Weise beeinflusst, die nicht mit den Datenschutzbestimmungen vereinbar sind und es keine Möglichkeit gibt, diese zu beheben, wird das Produkt oder die Dienstleistung natürlich nicht auf den Markt kommen."

Welche KI-Systeme sind am interessantesten für Tests in den regulatorischen Sandboxen?

"Zweifelsohne wären **KI-Systeme, die mehr als einen Bereich betreffen, am interessantesten und vermeintlich schwierig zu testen**. Ein Beispiel für ein solches System wäre ein finanztechnisches System, das eine Vielzahl von Finanzdienstleistungen und -produkten anbietet und gewährt, gleichzeitig aber auch personenbezogene Daten verarbeitet, wie z. B. die biometrische Identifikation. Je komplexer ein Produkt oder eine Dienstleistung ist, desto mehr muss es in verschiedenen Szenarien getestet werden."

Was passiert, wenn das Sandboxing-Experiment schiefgeht und Schaden verursacht wird?

"Die Teilnahme an einer Sandbox bedeutet keine Immunität vor Gericht. Tatsächlich ist das, was die meisten europäischen Behörden während des Sandbox-Prozesses anbieten, eine **negative Zusicherung und ein Schutz vor Vollstreckung** (d.h. ein versehentlicher Verstoß gegen die Vorschriften darf nicht zu sofortigen Vollstreckungsmaßnahmen führen). Selbst wenn der Verzicht auf einige Vorschriften von der Aufsichtsbehörde erlaubt wird, kann dieses "Privileg" jederzeit von der Aufsichtsbehörde widerrufen werden (z. B. wenn festgestellt wird, dass "die Vorteile das Risiko überwiegen" oder bei einer konsequenten Nichteinhaltung). Um es mit den Worten eines Laien auszudrücken: Wenn einige Rechte verletzt werden, **räumt die Regulierungsbehörde in der Regel eine gewisse Zeit ein, damit der Fehler behoben werden kann, eventuelle Schadensersatzansprüche müssen jedoch geltend gemacht werden**."