CO TO JE REGULATORNÍ SANDBOXING PRO AI?

Na žádost Knowledge Centre Data & Society se pro toto vydání brAInfood vyjádřila Katerina Yordanova, výzkumnice na CiTiP (KU Leuven), která přiblížila pojem regulatorní sandboxing pro AI.

„Regulatorní sandbox je popisován jako „bezpečné místo", prostředí, kde mohou podniky testovat nové inovativní produkty a služby (obchodní modely nebo doručovací mechanismy) se zmírněnými riziky v souvislosti s případným uvalením sankcí a v úzké spolupráci a za asistence národních regulačních orgánů."
– Katerina Yordanova

Navzdory vnímaným výhodám regulatorního sandboxingu se jeho koncepty významně liší mezi jednotlivými zeměmi a jurisdikcemi napříč EU.

Tento díl brAInfood zodpovídá některé z nejnaléhavějších otázek týkající se regulatorního sandboxingu pro AI.

Katerina Yordanova, výzkumnice na CiTiP, se specializuje na oblast lidských práv v digitálním prostředí, na podnikání a lidská práva. Realizuje výzkum v oblasti AI a jejích implikacích na lidská práva, inteligentní výrobu a podnikání a lidská práva v kontextu digitálních dodavatelských řetězců.

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

Kdo chce testovat AI systémy v regulatorních sandboxech?

„Subjekty, které mají obvykle prospěch z regulatorních sandboxů, jsou **start-upy a další podniky,** ale také veřejný sektor. Pokud jsou dodrženy všechny ostatní požadavky stanovené veřejnými orgány, které umožňují sandboxing, neměly by existovat překážky v tom, kdo může otestovat své produkty nebo služby."

Které regulatorní požadavky musí testovaná AI aplikace dodržet?

„Rozsah **záleží na veřejném orgánu, který bude sandboxing umožňovat** a na volnosti, kterou má v souvislosti se svým mandátem. Jisté ale je to, že národní autorita nebude moci zrušit nebo změnit požadavky během procesu sandboxingu, pokud budou tyto požadavky stanoveny právním předpisem EU. Objevují se proto určité názory, které říkají, že by regulaci měl vykonávat centrální orgán EU místo národních autorit, ale je sporné, zda smlouvy EU pro to poskytují právní základ."

[1] Nezávislý orgán ve Velké Británii, který má za úkol ve veřejném zájmu hájit práva na informovanost, podporuje otevřenost veřejných subjektů a ochranu dat jednotlivců.

Kde by k regulatornímu sandboxingu docházelo?

„Obvykle se experimenty vykonávají **v reálném tržním prostředí pod dohledem odpovědné autority**. Nicméně za účelem zaručení práv třetích stran, může být test proveden na omezené škále (například služba bude poskytnuta omezenému počtu osob) a třetí strany musí vědět, že se účastní tohoto testu a musí k němu dát souhlas."

Čí (osobní) data budou použita, a bude možné od účasti odstoupit?

„Produkty nebo služby, které jsou testovány v sandboxu jsou ve stádiu, kdy jsou připravené k uvedení na trh. Obvykle byla **data již použita na vytrénování potenciálního AI systému**. Užití osobních dat je v sandboxu vždy možné. To je také důvodem, proč autority jako ICO[1] mají své vlastní sandboxy, kde se snaží testovat, jak by technologie ovlivnily **práva na ochranu dat a/nebo právo na soukromí**.

Jedním z požadavků na takové testy je **transparentnost** pro účastníky testů a pro ty, jejichž data budou použita. Dalším požadavkem je odpovídající **ochranný mechanismus**, který by co možná nejvíce zmírňoval rizika.

Samozřejmě, pokud se ukáže, že produkt nebo služba ovlivňují osobní data způsobem, který se neslučuje se zákony na ochranu osobních údajů a neexistuje způsob, kterým by to bylo možné vyřešit, produkt nebo služba se nedostane na trh."

Jaké AI systémy je nejzajímavější testovat prostřednictvím regulatorních sandboxů?

„Bezesporu **AI systémy, které ovlivňují více než jednu oblast, budou nejzajímavější a pravděpodobně i obtížnější na testování**. Příkladem takového systému by byl systém finančních technologií, který nabízí a poskytuje množství finančních služeb a produktů ale zároveň také zpracovává osobní data, jako je například biometrická identifikace. Čím komplexnější produkt nebo služba je, tím více je zapotřebí ho testovat v různorodých scénářích."

Co se stane v případě, že se experiment v rámci sandboxingu nepovede a je způsobena škoda?

„Účast v sandboxu neznamená soudní imunitu. Ve skutečnosti to, co evropské autority během procesu sandboxingu nabízejí, jsou **dopisy o negativním ujištění a ochrana před vymáháním** (např. náhodné porušení právních předpisů nemusí vést k okamžitému donucovacímu opatření). I když regulátor může prominout některá porušení pravidel, takové privilegium může být regulátorem kdykoliv opět odebráno (např. pokud je dáno, že přínosy převáží rizika nebo v případě opakovaného nedodržování předpisů). Pokud to řekneme laicky, v případě porušení pravidel regulátor zpravidla **ponechá nějaký čas na vyřešení chyby, ale každá škoda musí být odškodněna**."

CLAIRE CZECH INSTITUTE OF INFORMATICS ROBOTICS AND CYBERNETICS CTU IN PRAGUE