Český telekomunikační úřad

www.ctu.gov.cz

AI Act v ČR: Férové hřiště pro inovace a ochranu občanů

Umělá inteligence (AI) se stává běžnou součástí našich životů i byznysu.

Na evropské úrovni byl přijat AI Act, který má nastavit jasná, přiměřená a smysluplná pravidla pro její bezpečné využití v rámci evropského trhu. Tato pravidla jsou tedy přímo působící i pro nás.

Jen je potřeba adaptovat konkrétní úpravu i pro Česko národním zákonem. Ten je navržen minimalisticky. Absolutně žádný gold plating či zavádění další svazující byrokracie.

AI Act zajišťuje bezpečné prostředí, kde platí férové podmínky pro všechny.

Základní myšlenka: Ochrana, nikoliv šikana

Vnímáme silnou celospolečenskou i podnikatelskou averzi vůči novým regulacím. K realizaci AI Actu v Česku proto přistupujeme jinak:

- **Jsme průvodci, ne drábové:** Naší primární rolí je edukovat a vysvětlovat, co je možné a co už je „přes čáru“.
- **Pravidla jako garance férovosti:** Pokud firma hraje podle pravidel, AI Act ji chrání před nekalou konkurencí. Je to jistota, že na stejném trhu nebude někdo jiný beztrestně podvádět.
- **Udržení důvěry ve společnost:** Lidé se oprávněně bojí deepfakes a zneužití dat. Naším úkolem je zajistit, abychom jako společnost neztratili schopnost rozpoznat realitu od manipulace.

Co AI Act reálně přináší?

1. Pro české občany: Jistota a ochrana důstojnosti

- **Zákaz manipulace a neviditelného sledování:**
  Občané mají garanci, že AI systémy nebudou zneužívány k jejich podvědomé manipulaci, social scoringu anebo neoprávněné diskriminaci (např. při žádostech o úvěr či v zaměstnání).

- **Transparentnost:**
  Právo vědět, že komunikuji s umělou inteligencí nebo že konzumuji uměle vytvořený obsah (ochrana před deepfakes).

- **Ochrana dat:**
  Garance, že citlivé osobní údaje nebudou zneužity k trénování pochybných modelů bez jasných pravidel.

2. Pro české firmy a OSVČ: Bezpečný růst a export

- **Celoevropská unifikace místo 27 režimů:**
  Pravidla sjednocují podmínky na celém evropském trhu. České firmě vyvíjející AI stačí splnit jedny požadavky a získá přístup k 450 milionům zákazníků v EU. AI Act tak omezuje prostor pro odlišné národní úpravy.

- **Důvěra klientů:**
  Produkt, který splňuje parametry AI Actu, získává punc důvěryhodnosti a bezpečnosti.

- **Podpora inovací:**
  Zaměřujeme se na rozvoj AI pro firmy s důrazem na metodickou podporu (jak pravidla splnit co nejjednodušeji a bez zbytečných nákladů).

3. Pro stát a společnost: Bezpečné řešení velkých výzev

- AI má obrovský potenciál pro zdravotnictví, dopravu nebo energetiku. AI Act umožňuje státu a institucím tyto technologie adoptovat bez rizika selhání nebo narušení etických hodnot.

Role regulátora

AI Act není všespásný, ale je to racionální a nezbytný základ.
Náš přístup jako regulátora bude **maximálně vstřícný a efektivní**.
Budeme využívat konkrétní, srozumitelné příklady z každodenního života k vysvětlování toho, jak nás AI ovlivňuje a proč jsou dané mantinely důležité.

Hlavní cíl:

Být občanům i firmám spolehlivým partnerem, který garantuje bezpečnost a férovost v digitálním prostoru.

Český telekomunikační úřad

www.ctu.gov.cz

Příloha: Vybrané praktiky představující tzv. „nepřijatelná rizika“ pro základní lidská práva, soukromí a bezpečnost občanů, zakázané Aktem o umělé inteligenci.

1. Manipulace a zneužívání

- **Podprahová manipulace:** Systémy využívající skryté techniky (audio, video, rozhraní) k ovlivnění chování člověka bez jeho vědomí (např. vynucování nákupů změnou nálady).
- **Zneužívání zranitelnosti:** AI zneužívající věk, fyzické či mentální postižení nebo sociální a ekonomickou situaci k tomu, aby člověka přiměla k chování, které mu může uškodit.

2. Sledování a hodnocení chování

- **Sociální hodnocení (Social scoring):** Hodnocení a klasifikace občanů na základě jejich sociálního chování nebo osobních vlastností, což vede k diskriminaci (např. odepření služeb).
- **Prediktivní policie:** Vyhodnocování rizika, že jednotlivec spáchá trestný čin, čistě na základě profilování a osobních charakteristik (bez vazby na konkrétní probíhající vyšetřování).
- **Rozpoznávání emocí v citlivém prostředí:** Používání AI k odvozování emocí a záměrů lidí na pracovištích nebo ve vzdělávacích institucích (např. hodnocení pozornosti žáků nebo výkonu zaměstnanců).

3. Biometrie a narušování soukromí

- **Plošné vytěžování obličejů (Scraping):** Necílené stahování snímků obličejů z internetu nebo z průmyslových kamer za účelem vytváření rozsáhlých databází pro rozpoznávání tváří.
- **Biometrická kategorizace:** Rozřazování lidí na základě biometrických údajů s cílem odvodit citlivé informace, jako je rasa, politické názory, náboženské přesvědčení nebo sexuální orientace.
- **Biometrická identifikace v reálném čase:** Plošné sledování a rozpoznávání tváří na veřejně přístupných místech pomocí kamerových systémů (až na velmi úzké a přísně kontrolované výjimky při pátrání po závažných zločincích).