3. 6. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Umělá inteligence ve světle pandemie COVID-19 a potřeba jejího urychleného legislativního rámce

Současná krize zapříčiněná pandemií COVID-19 vyvolala řadu otázek a přinutila se zamyslet nad řadou témat, která byla do dnešní chvíle opomíjena, resp. odkládána na později. Jedním z takových témat je i rozvoj digitální technologie, zejména pak rozvoj umělé inteligence (dále jen "AI"), která má všechny předpoklady stát se hlavní technologií budoucnosti a do které se bohužel pořád ještě zejména v EU neinvestuje tolik peněz a úsilí, kolik by bylo potřeba.

Technologie AI

Co je to vlastně to AI, o kterém tu hovoříme? Většina lidí tento pojem slyšela, ale málokdo dokáže definovat, o co se přesně jedná. Jisté světlo k pochopení tohoto pojmu přináší nová a zároveň první definice AI v legislativních textech EU. Definice AI byla původně vytvořená Evropskou komisí, ale následně byla upřesněna speciálně vytvořenou skupinou odborníků na úrovní EU pro potřeby AI, tzv. "*High-Level Expert Group on Artificial Intelligence*". Samotná definice zní (laicky přeloženo) nějak takto:

„Systémy umělé inteligence (AI) jsou softwarové (pravděpodobně i hardwarové) systémy navržené lidmi, jež dosahují stanoveného komplexního cíle, jednají v hmotném nebo digitálním rozměru tak, že vnímají své okolí skrze sběr dat, interpretují nashromážděná strukturovaná nebo nestrukturovaná data, uvažují nad vědomostmi, nebo zpracovávají informace odvozené z těchto dat a rozhodují o nejlepších postupech k dosažení daného cíle. Systémy AI mohou použít buď symbolická pravidla, nebo se naučit numerický model, mohou také upravit své chování analýzou změn v okolí zapříčiněných jejich předchozím chováním.” [1]

Dle výše uvedené definice lze tedy AI vnímat jak ve formě hmotné (např. AI robot, AI auta, AI drony, apod. – skládající z hardwarové i softwarové složky), tak i digitální (počítačový program – software). Společné pro obě formy AI je to, že na rozdíl od jejích technologických předchůdců budou nejen naprogramovány pro určitý úkol, ale budou se moci na základě přijatých dat učit a vyvíjet, ostatně tak to dělají v průběhu svého života i samotní lidé (i když ne všichni se ze svých chyb dokáží poučit tak jako AI). Tam, kde se v definici (poslední věta) hovoří o "*úpravě změny chování analýzou svého okolí*" se má na mysli nejvyspělejší druh AI. Pod tím si můžeme představovat zejména roboty (ale nejenom je) založené na AI, kteří již dokáží porozumět myšlenkám a emocím člověka a na základě toho přizpůsobit své následující chování. Jeden příklad za všechny je příklad robota ze známého filmu "*Terminátor 2 – Den zúčtování*", v hlavní roli s Arnoldem Schwarzeneggerem, ve kterém sice robot byl naprogramován na určitý úkol (ochranu osoby), ale již sám uvažoval a časem dokázal pochopit city člověka a na základě toho adekvátně reagovat

Pokud jde o AI v digitální formě, tak to se již široce používá k personalizaci reklamních e-mailů a vytváření personalizovaných speciálních nabídek. Je rovněž integrováno do tzv. CRM (řízení vztahů se zákazníky) a marketingových automatizovaných platforem - strojové učení totiž dokáže lépe analyzovat zpětnou vazbu od zákazníků, v důsledku čehož dochází k lepším výsledkům v rámci

jednotlivých kampaní. [2] Bez toho, abychom se nad tím jakýmkoliv způsobem zamýšleli, používáme AI na denní bázi již nyní, např. platformy na překlad jazyků, generování titulků ve filmech nebo blokování spamu v e-mailech. [3]

AI má množství výhod - dokáže snadno a rychle plnit rutinní úkoly, pracovat neomezeně dlouho, minimalizuje chyby zapříčiněné lidským faktorem, může být používáno kýmkoliv, pomoci nám vylepšit naše dovednosti, učinit nás produktivnějšími a dokonce i pomoci žít zdravěji a déle (algoritmy nahradí výživové poradce, kouče, apod.).

I přesto, že AI může v hodně věcech pomoci, může také napáchat hodně škody. Škoda může být buď podstatná (bezpečnost a zdraví jednotlivců, včetně ztráty na životech, škody na majetku), či méně podstatná (ztráta soukromí, omezení práv na svobodu projevu, ztráta lidské důstojnosti, diskriminace - například při přístupu k zaměstnání). Tak či onak s ní může být spojená celá řada rizik.[4]

Tato rizika mohou vyplývat z nedostatků v celkové konstrukci systémů AI (včetně dohledu ze strany člověka) nebo používání dat bez úprav potenciálních zkreslení (např. systém je školen použitím údajů pouze nebo zejména od mužů, což může vést ke zkreslujícím výsledkům ve vztahu k ženám).

Výše uvedené škody, které může AI napáchat, pramení ze současného nedostatečného legislativního rámce, kdy současná legislativa není připravena na použití podobných systémů v praxi, resp. jejich definování, stanovení právních mantinelů působnosti, určení odpovědnosti za případnou škodu apod. Většina zákonů při svém vzniku totiž s podobným druhem technologie nepočítala.

Jako příklad lze uvést odpovědnost za škodu způsobenou vadou výrobku dle §2939 a násl. NOZ [5]. Budeme-li systém AI považovat za výrobek (což je diskuse sama o sobě), tak v případě škody způsobené jeho vadou je legislativa poněkud nejasná. Za normálních okolností totiž lze považovat výrobek za vadný (§2941 odst. 1 NOZ) v případě, kdy není "*tak bezpečný, jak to od něho lze rozumně očekávat se zřetelem ke všem okolnostem, zejména ke způsobu, jakým je výrobek na trh uveden nebo nabízen, k předpokládanému účelu, jemuž má výrobek sloužit, jakož i s přihlédnutím k době, kdy byl výrobek uveden na trh.*" Při vadě systému AI (např. při nějaké chybě v jeho programování) by se tedy poškozený mohl domáhat náhrady škody právě podle tohoto ustanovení zákona (ve spojení s §2939 NOZ a případně dalšími) a to na základě objektivní odpovědnosti. Problém ale nastává tehdy, kdy se systém AI samostatně učí, resp. na základě přijetí více dat dělá postupně autonomní rozhodnutí. V daném případě by se odpovědná osoba mohla své odpovědnosti zprostit v souladu s § 2942 odst. 2 písm. b) NOZ, stanovujícího, že "*Povinnosti k náhradě škody se tato osoba rovněž zprostí, prokáže-li, že lze důvodně předpokládat s přihlédnutím ke všem okolnostem, že vada neexistovala v době, kdy byl výrobek na trh uveden, nebo že nastala později.*" To právě sedí na případ, kdy byl systém AI uveden na trh bez jakýchkoliv vad, ale v průběhu času a na základě svého učení a autonomního chování dojde k nějaké chybě, která zapříčiní újmu poškozenému, resp. škodu k náhradě které se ale odpovědná osoba může zprostit dle výše uvedeného ustanovení NOZ.

Nepřipravenost legislativy na možnost efektivního použití této technologie pak byla patrna při současné krizi zapříčiněné pandemií COVID-19, což se pokusím rozebrat na několika řádcích níže.

ČR v době pandemie COVID-19 a důsledky chybějící technologie AI

Aktuálnost tohoto tématu v České republice, EU i celém světě se ukázala zejména v době koronavirové krize. Ta totiž poukázala na slabiny zejména v oblasti zdravotnictví, kde nedostatek rozvoje AI (jak legislativního, tak i technického rázu) mohl, ale bohudík neměl, vážnější dopady na životy lidí.

Prvním vážnějším nedostatkem byla chybějící legislativa, která by umožnila využít umělou

inteligence v praxi. Mám na mysli efektivní způsob zabránění šíření COVID-19 prostřednictvím zejména speciálních aplikací v telefonu sledujících pohyb lidí, sdělujících informaci ohledně jejich zdravotního stavu a umožňující na základě těchto dat efektivnější vystopování potenciálních nakažených. Aplikace vytvořené za tímto účelem většinou fungují skrze bezdrátový systém Bluetooth, kdy jsou všechna čísla mobilních telefonů v dosahu cca 1,5 metru od infikované osoby ukládána ve speciální databázi (buď v telefonu, nebo externě) pro jednodušší vystopování potenciálních nakažených. Jednotlivé státy pak přistupují k získávání a zpracování těchto dat rozdílně [6]:

- Čína – používá QR kódy pro monitorování zdravotního stavu a pohybu svých občanů. Tyto QR kódy musí být skenovány před nástupem do jakýchkoliv dopravních prostředků či jakýchkoliv bytových komplexů;

- Itálie – používá aplikaci pro sledování pohybu svých občanů pro vystopování těch, kteří se dostali do kontaktu s nakaženým;

- Jižní Korea - používá aplikaci na pozadí procesu telefonu pro sledování pohybu svých občanů, resp. pro vystopování těch z nich, kteří se dostali do kontaktu s nakaženým. Rovněž zavedli použití elektronických náramků pro ty z nich, kteří ignorují domácí karanténu. Někteří jedinci totiž obcházeli pravidla stanovená vládou, resp. nechávali telefony s monitorovacími aplikacemi doma a vycházeli ven, i když to měli zakázáno. Odmítnutí náramku pak znamená umístění osoby na izolační oddělení, náklady na takový pobyt musí osoba hradit ze svého; [7]

- ČR – funguje aplikace eRouška, jenž je součásti tzv. chytré karantény. Hygienici mají s pomocí eRoušky snadněji získávat kontakty na lidi, kteří byli v kontaktu s pacientem nakaženým COVID-19. Jak popisuje jeden z autorů této aplikace: *„Aplikace slouží jako automatický notýsek, do kterého se zapisují anonymní ID zařízení, se kterými jste přišli do styku. Tento notýsek je uložen jen ve vašem telefonu a o odeslání hygieně rozhodnete jen vy sami, pokud vás o to pracovník hygieny požádá.“* [8]

Zásadní rozdíl mezi používáním aplikací v jednotlivých zemích je jejich povinnost či naopak dobrovolnost. Zatímco v Číně jsou tyto aplikace povinné, v Evropě (tedy i v ČR), kde je ochrana soukromí základním právem každého občana, dbají státy a výrobci aplikaci na větší ohleduplnost k ochraně soukromí. Zde je tudíž používání těchto aplikací dobrovolné a pro sběr dat a jejich následné odeslání potřebují souhlas vlastníka. [9]

Evropské státy se tímto způsobem snaží chránit soukromí svých občanů, což je sice pochopitelné, na druhou stranu ale vznikají otázky ohledně efektivity těchto kroků. Zejména v době rozšíření podobných nemocí jako je COVID-19, tedy v době nedostatků jakéhokoliv efektivního způsobu léčby (resp. vakcíny), je potřeba brát ohled na další lidská práva, jakými jsou zejména práva na ochranu zdraví (čl. 31 LZPS) a právo na život (čl. 6 LZPS).

Ochrana soukromí (čl. 7 LZPS) by pak v takto výjimečně době, jako je tato, neměla být nadřazena zdraví a životu lidí. Pokud lze totiž za současné situace omezit svobodu pohybu (čl. 14 LZPS), shromažďování (čl. 19 ZMPS) a dalších základních práv, měla by být možnost (za splnění určitých předpokladů – nezbytná doba, proporcionalita a další) omezit i právo na soukromí, které se od výše uvedených práv zásadním způsobem neliší.

Nedostatkem postupu evropských států je i způsob zpracování dat. Např. v ČR to mají za úkol prověření hygienici, jen ti mají přístup k zabezpečenému rozhraní pro zpracování přijatých dat.[10] Takový systém může dobře fungovat jen v případě, kdy ho využívá menší skupina uživatelů a kdy je

počet nakažených nízký. Pokud by bylo nemocných daleko více, resp. tyto aplikace by používalo více osob, např. alespoň 10% populace, osoby (v daném případě pověření hygienici) obhospodařující tuto aplikaci by byly neúměrně přetíženy, což by v důsledku mohlo stát život velkého počtu lidí. Zde vidím velký prostor pro využití AI, které by bylo schopno zpracovat ve velké rychlosti i větší množství dat a určit diagnózu jednotlivých pacientů (a jeho nejbližšího okolí) v poměrně krátkém čase.

Samozřejmě, že mnohem efektivnější by tato technologie byla, v případě splnění určitých okolností, kdyby byla povinná celoplošně, tedy povinně nainstalovaná na všech zařízeních. Tato možnost by ale za současné ochrany lidských práv připadala v úvahu jen při velmi vysoké hrozbě (daleko přesahující hrozbu, která byla nyní), a navíc při splnění dalších požadavků jako je sběr jen nejnutnějších údajů, jejích šifrování apod. Na tomto místě totiž musíme neustále myslet na vyvažování dvou protipólů - ochrany zdraví (příp. života) a ochrany soukromí. Legislativa by se pak de lege ferenda měla takovým možným situacím přizpůsobit.

Současná krize poukázala i na další problém, a to ohrožení zdraví občanů ČR zapříčiněné útoky hackerů na české nemocnice a další strategická cíle. Šlo zejména o nemocnice v Olomouci, Ostravě a Pardubickém kraji, útoků čelilo rovněž ministerstvo zdravotnictví a Letiště Václava Havla.[11] Většinou jde o útoky skrze vyděračské programy nacházející se v příloze e-mailu, které se snaží být co nejvíce důvěryhodné, a donutit tak zaměstnance těchto zařízení je otevřít. Následkem toho může dojít dokonce k ochromení zařízení (např. nemocnice) na několik dní, což by, zejména v době krize COVID-19, představovalo obrovské riziko s nedozírnými dopady na zdraví občanů ČR. [12]

Tomu by mohlo zabránit AI, které má velký potenciál změnit pohled na kybernetickou bezpečnost. Systém založený na AI funguje obecně řečeno tak, že zakládá kritérium „normálního“ chování. Kdykoli pak nějaká událost nebo krok nebude odpovídat „normálnímu“ chování, software o tom informuje podporu IT, tedy fyzické osoby odpovědné za kybernetickou bezpečnost, a označí ohrožená zařízení, účty, soubory nebo sítě. AI se postupně učí na základě vlastních zkušeností a časem se stává přesnější v detekci potenciálního nebezpečí. Algoritmus v pozdějším stádiu pak dle předpokladu nebude vyžadovat ani lidský dohled. Velkou výhodou tohoto systému je, že data a bezpečnostní postupy, které AI pro ochranu instituce nashromáždí, bude pravděpodobně ve stejném rozsahu možné použít i pro ochrany dalších institucí. [13] Může tudíž vzniknout centrální státní systém pro ochranu všech nemocnic a dalších strategických cílů, kdy již nebude potřeba kontrolovat oddělené sektory samostatně.

V této oblasti může tedy AI velmi pomoci, ale taky velmi uškodit. Nelze totiž zapomínat na to, že podobný systém mohou časem využívati samotní hackeři. Pokud by se jim podařilo využít tuto technologii pro útoky na civilní cíle, mohl by se z velkého pomocníka stát nebezpečný nepřítel – AI dokáže kreslit obrázky, upravovat fotografie lidí dle jejich předpokládaného stáří, psát na takové úrovni, aby dokázalo zaměstnance přesvědčit o pravdivosti svých tvrzení, dokáže najít chyby v bezpečnostním systému a rovněž se každým útokem enormní rychlosti zlepšuje. [14]

Dokonce již existuje případ použití takového systému AI v praxi. Před necelým rokem došlo k jednomu pozoruhodnému případu deepfake [15], kdy zločinci vygenerovali software založený na AI, aby replikovali hlas generálního ředitele jedné nejmenované energetické společnosti ve Velké Británii. V tomto případě si podřízený myslel, že telefonuje se svým nadřízeným, generálním ředitelem německé mateřské společnosti, který mu nařídil poslat 220 000 EUR jednomu maďarskému dodavateli, to vše pod podmínkou urgentnosti a požadavku, aby platba proběhla do hodiny. [16]

Výše uvedený útok byl sice výjimečný, ale přesto důležitým varovným signálem pro státy, že v blízké budoucnosti můžeme očekávat více útoků s podporou AI. S pomocí AI lze totiž vytvořit efektivního útočníka, který bude trpělivý, inteligentní, nezávislý a neúnavný, který jen bude čekat na svojí

příležitost. Proti AI útočníkovi bude velmi těžká obrana, může útočit na více místech najednou a současný způsob kybernetické obrany by jen stěží stíhal čelit všem útokům naráz.

Dobrou zprávou je, že vytvoření automatického programu je velmi komplikované. Algoritmus AI není tzv. *„user friendly"* (uživatelsky přívětivý) a hackerský nástroj vyžaduje vyšší odbornost AI. Dovednosti jsou v současné chvíli v tomto oboru nedostatečné a to i na odborné úrovni, nemluvě již o hackerském prostředí. Je tedy velká pravděpodobnost, že první pokroky v podobných útocích budou učiněny na úrovni států a v zájmu jejích cílů.

Zde je na místě ukázat jeden příklad (pravděpodobně státem řízeného) útoku a fatálních důsledků, který takový útok může mít pro napadené státy. Před nějakou dobu čelili úspěšným útokům hackerů největší poskytovatelé zdravotní péče v USA. Jednalo se o následující poskytovatele – Primera, Care First a Anthem. Útoky byly závažné zejména kvůli tomu, že pacienty těchto poskytovatelů bylo mnoho federálních zaměstnanců. Ihned poté následovalo hacknutí americké společnosti Lockheed Martin (jde o vojensko-průmyslovou společnost) a nezávislé agentury federální vlády USA – oddělení lidských zdrojů (Office of Personnel Management), která má ve Spojených státech na starosti bezpečnostní prověrku 5. úrovně. Důsledkem útoků byla ztráta otisků prstů a osobních údajů tisíce lidí. Předpokládalo se, že data byla ukradena některým ze států. Tato domněnka se zakládala na skutečnosti, že se ukradená data neobjevila na *„dark webu"* [17], kde je útočníci většinou prodávají třetím osobám. Držitelé těchto dat májí nyní přístup k rozsáhlé databázi záznamů o zdravotní péči, záznamům HR, federálních bezpečnostních kontrol a jejích pozadí a mimo jiné i údajů o dodavatelích výše uvedených společností a organizací.

Zpracování dat do určitých výstupů k přímému praktickému použití by bez AI zabralo velmi mnoho času. Program na bázi AI by však mohl propojit jednotlivá data tak, aby z toho vznikl přehledný výstup údajů o jednotlivých osobách, resp. cílů na které by byl možný další útok. Zpracováním dat lze propojit informace o rodinách osob, jejich zdravotních problémech, přezdívkách, federálních projektech, na kterých se podílely nebo podílejí. Rozsah škod při využití těchto informací je nedozírný. [18]

Výše uvedené praktické hrozby, kterým pravděpodobně budou čelit všechny státy, podporuje myšlenku nutnosti urychleného pokroku ve vývoji této technologie a jejího legislativního rámce a že již včera bylo pozdě. Schopnost použití AI pro obranu je totiž věc, kterou budou týmy zabývající kybernetickou bezpečností v nejbližší době velmi potřebovat.

Současný stav legislativy AI v EU

Technologický rozvoj je nezastavitelný a kdo se v tomto sektoru AI prosadí jako první, bude mít ohromný náskok. Toto si uvědomila i Evropská unie, která se oficiálně začala zaměřovat na tento sektor technologie v roce 2017, kdy Evropská rada vyzvala Evropskou komisi k položení základu společné legislativy EU týkající se AI. Zaujala přitom stanovisko, že v dané otázce musí být postupováno společně, výsledkem by tedy mělo být vypracování jednotné legislativy pro všechny státy EU. [19]

Komise reagovala na výzvu Rady 25. dubna 2018 zveřejněním strategie IA, což zapříčinilo exponenciální narůst zdrojů EU vyčleněných na rozvoj projektů IA (téměř 1,5 miliardy EUR mezi lety 2018 a 2020) s cílem do budoucna zpřístupnit tyto technologie v rámci EU široké veřejnosti. [20] Tímto krokem EU započala soupeření se zeměmi jako USA, Čína, Japonsko a dalšími, které již nějakou dobu upírají svůj pohled k této technologii. Problém však spočívá v tom, že EU ještě pořád neinvestuje tolik, kolik by bylo třeba. Vezmeme-li například počáteční investice do této technologie v EU (cca 3,2 miliardy EUR v roce 2016) a srovnáváme-li jí s investicí za stejné období v Severní Americe (12,1 miliard EUR) a v Asii (6,5 miliard EUR), nejsou investice EU ještě na takové hodnotě,

abychom mohli říci, že stojíme u pomyslného kormidla jejího rozvoje. [21]

Na druhou stranu ale nelze EU upřít snahu s tímto stavem něco dělat. V souladu s výše uvedenou strategií AI přijala Komise koordinovaný plán na podporu rozvoje a využívaní AI v Evropě. [22] Komise také navrhla od příštího programového období 2021–2027 investovat do AI nejméně 1 miliardu EUR ročně z programů Horizont Europe a Digital Europe. Nařízení o ochraně osobních údajů (GDPR) by se pak mělo stát důležitým prvkem zajištění důvěry široké veřejnosti v AI. Důvěra veřejnosti je dle Komise obzvláště potřebná, pokud jde o zpracování zdravotnických dat pro aplikace řízené AI. AI totiž funguje na principu - čím více dat obdrží, tím lepší je funkcionalita jejího systému. Vše je založené na tom, že AI vytvoří vzory chování na základě dostupných dat, a pak tyto vzory používá na nově přijatá data, a tím se postupně vylepšuje. Po nějakém čase tyto algoritmy mohou klasifikovat subjekty (např. pacienty v nemocnicích), které nikdy neviděly, s přesností přesahující znalosti lidských odborníků. Přístup k datům je tedy zásadní pro vývoj AI. [23]

Přijetí společné legislativy AI nabralo další směr publikací tzv. *„White Paper o AI“*, dne 19. února 2020 (dále jen "White Paper"). Veřejná konzultace zahájená Komisí skončila 19. května 2020, kdy byly Komisi předloženy návrhy a připomínky, jak dále podpořit výzkum a vývoj AI, vylepšit povědomí o AI mezi evropskými malými a středními podniky a poskytnout základní prvky legislativního rámce týkajícího se AI. Podle názoru Komise mohou systémy AI pomoci EU při řešení současných sociálních problémů jako je boj proti změně klimatu, ochraně demokracie a boj proti zločinu. To vše bez zanedbávání dodržování základních lidských práv jako je lidská důstojnost a ochrana soukromí jednotlivců – zejména pak v oblasti představující vysoké riziko. Systémy AI by měly dle Komise být obecně považovány za vysoce rizikové na základě toho, co je v sázce, resp. zda odvětví jeho použití i způsob provedení představují ve svém souhrnu významné riziko, zejména z pohledu ochrany bezpečnosti, práv spotřebitele a základních lidských práv.[24]

Pokud bychom se zaměřili na odvětví zdravotnictví, o kterém jsme hovořili výše, White Paper se přímo vyjadřuje o tomto odvětví jako o vysoce rizikovém. To by samozřejmě mělo být zohledněno při jakékoli budoucí regulaci. Následně upřesňuje, že při využití AI v rizikových oblastech musí být splněny body specifikované níže:

- dodržování požadavků na sběr a využití dat;
- dodržování obsahu uchovávaných údajů a záznamů;
- poskytování informací o použití AI;
- dodržení technické robustnosti a přesnosti systému;
- lidský dohled;
- dodržování zvláštních požadavků na určité konkrétní aplikace AI, jako jsou například ty, které se používají pro účely vzdálené biometrické identifikace.

Zejména v části *sběru a využití dat* ke školení AI se Komise vyjadřuje tak, že je důležitější než kdy jindy propagovat, posilovat a hájit hodnoty a pravidla EU a zejména pak práva občanů vyplývající z práva EU. Mimo jiné se tím má na mysli zaměření na zajištění přiměřené ochrany soukromí a osobních údajů při používání produktů a služeb podporujících AI.

V době před pandemií COVID-19 by se nad výše uvedeným asi nikdo nepozastavoval, ale současná krize ukázala, že ve výjimečné době je potřeba balancovat mezi ochranou soukromí a právem na ochranu zdraví, resp. právem na život. Pozoruhodné je též to, že Komise před samotnou publikací

White Paper nevzala v úvahu současnou situaci ve světě (resp. zejména výše uvedené vybalancování práv). V době vydání dokumentu se již COVID-19 šířil a na základě jednání jednotlivých státu bylo možné učinit alespoň nějaké závěry pro futuro.

V důsledku nekoordinovaného postupu EU dochází k individuálnímu a někdy chaotickému postupu jednotlivých států, které sice prozatím více či méně dodržovaly právo na soukromí při vytváření jednotlivých opatření při sledování svých občanů, ale to se může rychle změnit s případnou druhou vlnou nákazy, která by mohla přijít na konci léta. Právo na soukromí totiž bude dodržováno jen do té doby, dokud nebude ohrožen větší počet lidí (zejména jejích zdraví a životy). Pokud by byla případná druhá vlna silnější než předchozí, nelze vyloučit masivnější zkoušení technologie AI v dané oblasti, bohužel ale již bez jakéhokoliv harmonizovaného postupu a s rozdílným přístupem k právům na dodržování kterých jsou založeny hodnoty EU.

Závěrem lze konstatovat, že současná koronavirová krize nám v této oblasti otevřela oči. Již teď je zřejmé, že urychlení vývoje legislativy a rozvoje AI v EU by mělo být pro EU prioritou číslo jedna. EU by měla v této otázce postupovat rychle, koordinovaně a soudržně. Jednotlivé státy totiž nemohou dosáhnout potřebného pokroku a konkurovat světu bez společného postupu v rámci celé EU. Jen společným postupem lze totiž dosáhnout vývoje technologie a legislativního rámce na takové úrovní, aby se v ní EU stala světovým lidrem. Následkem neřízeného postupu v rámci EU může dojít k předem prohrané bitvě s třetími mocnostmi (resp. státy i hackery), které tuto technologii použijí dříve. To může vyústit v masivní únik dat z jednotlivých států EU, úspěšné napadání jejich důležitých civilních cílů, ochromení v určitých oblastech, v nejhorším možném scénáři, obětech na civilistech v době pandemie, ochromení jejích ekonomické infastruktury, zhoršení ekonomického stavu společnosti, nepokojům a celkové špatné životní úrovni. Abychom zabránili tomuto, možná pro některé, poněkud přehnanému a katastrofickému scénáři, musí jednotlivé státy EU pochopit, že tato technologie je technologií budoucnosti. Nesmí opomíjet její závažnost a musí pracovat společně a urychleně na jejím legislativním rámci a celkovém vývoji tak, aby zajistily bezpečnost nejen svých občanů ale i celé EU.

Mgr. Ruslan Popov,
advokátní koncipient

P / R / K

ADVOKÁTNÍ KANCELÁŘ

PRK Partners s.r.o. advokátní kancelář

Jáchymova 2

110 00 Praha 1

Tel.: +420 221 430 111
Fax: +420 224 235 450
e-mail: prague@prkpartners.com

---

[1] *WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust*. In: Brussels, 2020, COM(2020) 65 final. K dispozici >>> zde.

[2] ZHIDKOV, Roman. The Future Impact of AI on Cyber Crime. *Becoming Human: Exploring Artificial Intelligence & What it Means to be Human* [online]. 2020 [cit. 2020-05-15]. K dispozici >>> zde.

[3] *ANNEX to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions: Coordinated Plan on Artificial Intelligence*. In: Brussels, 2018, COM(2018) 795 final. K dispozici >>> zde.

[4] *WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust*. In: Brussels, 2020, COM(2020) 65 final. K dispozici >>> zde.

[5] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

[6] CHABBA, Seerat. Coronavirus tracking apps: How are countries monitoring infections? *DW.com: Made for minds* [online]. 2020 [cit. 2020-05-21]. K dispozici >>> zde.

[7] BOSTOCK, Bill. South Korea launched wristbands for those breaking quarantine because people were leaving their phones at home to trick government tracking apps. *Businessinsider.com* [online]. 2020 [cit. 2020-05-21]. K dispozici >>> zde.

[8] SLÍŽEK, David. Je tady eRouška. Aplikace od COVID19CZ sleduje přes Bluetooth kontakty s lidmi. *Lupa.cz: Server o českém internetu* [online]. 2020 [cit. 2020-05-14]. K dispozici >>> zde.

[9] How do COVID-19 tracing apps work and what kind of data do they use? *Bbva.com* [online]. 2020 [cit. 2020-05-21]. K dispozici >>> zde.

[10] SLÍŽEK, David. Je tady eRouška. Aplikace od COVID19CZ sleduje přes Bluetooth kontakty s lidmi. *Lupa.cz: Server o českém internetu* [online]. 2020 [cit. 2020-05-14]. K dispozici >>> zde.

[11] ČTK. Několik nemocnic a pražské letiště se staly terčem hackerů. Zdržte se útoků na české cíle, vyzval šéf americké diplomacie. *Ihned.cz/* [online]. 2020 [cit. 2020-05-19]. K dispozici >>> zde.

[12] ČTK. Kyberútoky na nemocnice mohou stát desítky milionů korun. *Novinky.cz* [online]. 2020 [cit. 2020-05-19]. K dispozici >>> zde.

[13] ZHIDKOV, Roman. The Future Impact of AI on Cyber Crime. *Becoming Human: Exploring Artificial Intelligence & What it Means to be Human* [online]. 2020 [cit. 2020-05-15]. K dispozici >>> zde.

[14] RAY, Terry. One of the eternal truisms about cybersecurity is that it’s a cat and mouse game – and cybersecurity often seems to be behind the ball. *Technative.io* [online]. [cit. 2020-05-22]. K

dispozici >>> zde.

[15] DEEPFAKE je technologie na bázi AI, která shromažďováním modelů lidského chování vytváří vlastní modely, které by měly být racionální a inteligentní – tedy simulují lidské chování. Počítač tedy na základě kombinací obrázků a videí dostupných na internetu dokáže předpovědět, jak se určitá osoba v dané chvíli může cítit. Tento nově vytvořený obraz i zvuk se potom často vkládá do už existujícího videa, které má navodit pocit originality. Díky této technologii sledující skutečně může uvěřit, že osoba na videu skutečně, řekla nebo udělala něco, co ve skutečnosti nikdy nedělala. Pro lepší pochopení, k dispozici >>> zde.

[16] STUPP, Catherine. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case: Scams using artificial intelligence are a new challenge for companies. *The Wall Street Journal: wsj.com* [online]. 2019 [cit. 2020-05-21]. K dispozici >>> zde.

[17] DARK WEB je část internetu, která není viditelná pro vyhledávače, a vyžaduje pro přístup anonymní prohlížeč zvaný Tor. Tato část internetu je ohniskem kriminální aktivity - ůžete si koupit čísla kreditních karet, různé druhy drog, zbraně, padělané peníze, odcizená přihlašovací údaje, hacknuté účty Netflix a software, který vám pomůže proniknout do počítačů jiných lidí; Můžete si najmout hackery, kteří za vás zaútočí na počítače; Můžete si koupit uživatelská jména a hesla. Podrobnější popis k dispozici >>> zde.

[18] RAY, Terry. One of the eternal truisms about cybersecurity is that it's a cat and mouse game – and cybersecurity often seems to be behind the ball. *Technative.io* [online]. [cit. 2020-05-22]. K dispozici >>> zde.

[19] *European Council meeting (19 October 2017) – Conclusions*. In: Brussels, EUCO 14/17, CO EUR 17 CONCL 5. K dispozici >>> zde.

[20] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions: Artificial Intelligence for Europe*. In: Brussels, 2018, {SWD(2018) 137 final}, COM(2018) 237 final. K dispozici >>> zde.

[21] *WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust*. In: Brussels, 2020, COM(2020) 65 final. K dispozici >>> zde.

[22] *ANNEX to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions: Coordinated Plan on Artificial Intelligence*. In: Brussels, 2018, COM(2018) 795 final. K dispozici >>> zde.

[23] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions:* Coordinated Plan on Artificial Intelligence. In: Brussels, 2018, COM(2018) 795 final. K dispozici >>> zde.

[24] *WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust*. In: Brussels, 2020, COM(2020) 65 final. K dispozici >>> zde.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- GLP-1 v potravinářství: čekají nás v EU „GLP-1 friendly potraviny“?
- Rozhodnutí Soudního dvora Evropské unie o předběžné otázce – C-386/23 ze dne 30. dubna 2025 – Prolomení zákazu uvádět zdravotní tvrzení týkající se rostlinných látek?
- Novinky z české a evropské regulace finančních institucí za měsíc září 2025
- Prověřování zahraničních investic v EU: současný rámec, česká praxe a očekávané změny
- Novinky z české a evropské regulace finančních institucí za měsíce červenec a srpen 2025
- Že je jednotný patent drahý? Záleží na úhlu pohledu. Celoevropskou patentovou ochranu ale zlevňuje
- Přezkum rozhodnutí CAS vnitrostátními soudy Evropské unie
- Právo na soukromí vs. transparentnost firem: Kontroverze kolem evidence skutečných majitelů
- GDPR 2.0: Jednodušší regulace pro odvážnou a konkurenceschopnou Evropu?
- Důkladnější přezkum rozhodnutí vydaných Rozhodčím soudem pro Sport
- Novinky z české a evropské regulace finančních institucí za měsíc červen 2025