UNIVERZITA KARLOVA

Právnická fakulta

Viktor Záruba

Umělá inteligence v trestním právu

(se zaměřením na použití při vyšetřování trestných činů)

Diplomová práce

Vedoucí diplomové práce: JUDr. Mgr. Marek Dvořák, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 12. 6. 2024

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 182 842 znaků včetně mezer.

Viktor Záruba

V Praze dne 10. 6. 2024

Poděkování

Poděkování patří především doktoru Marku Dvořákovi za jeho vřelý přístup při konzultacích a za to, že mi byl nápomocen ve všech ohledech při psaní diplomové práce, které mě i díky němu po celou dobu naplňovalo.

Obsah

Úvod

Fenomén umělé inteligence (dále jako „UI“) v posledních několika málo letech postupně vstupuje do našeho života v nejrůznějších podobách, ať už se jedná o samostatné uklízecí roboty v domácnosti, nebo třeba zavedení autonomních vozidel do veřejné dopravy. Technologie UI se čím dál tím víc začleňuje i do virtuálního prostředí, zejména k personalizaci nakupování na internetu a digitálního marketingu.[1] S UI se tedy v dnešní době setkáváme téměř denně, a to i na místech, kde bychom to úplně nečekali. Spolu s využitím v běžném životě se nezbytně pojí vliv této technologie na práva a svobody každého jednotlivce, který s ní přijde do styku. Pro právo jako takové to přináší nespočet nových výzev. Světové právní řády budou muset v nejbližší době reagovat zakotvením efektivních pravidel schopných odrážet neustávající technologický vývoj v této oblasti. Využití systémů, které fungují na bázi UI se s největší pravděpodobností významně promítne do většiny právních odvětví. Na té nejzákladnější úrovni může jít o automatizaci rutinních a administrativních úkolů například v rámci soudních a správních řízení, nebo také zjednodušení tvorby a přizpůsobování soukromoprávních smluv. V korporátním právu se jistě zužitkuje efektivní a rychlé zpracování velkého množství dokumentů během fúzí. Velký rozruch UI způsobí v právu autorském, a to v souvislosti s umělým generováním zvukových nahrávek a video obsahu.[2]

Zásah systémů UI do oblasti trestního práva je jeden z těch závažnějších a vyvolává mnoho právních a etických otázek i v těch nejzazších koutech trestněprávní nauky: Co vlastně považujeme za UI? Jak vypadá trestněprávní úprava UI? Jak se UI projevuje v trestní odpovědnosti? Jak UI mění podobu trestné činnosti pachatelů? Jaký má UI vliv na rozhodování v trestním řízení? Jak se UI používá při vyšetřování trestných činů? Co můžeme v kontextu trestního práva od UI očekávat do budoucna a jak s ní správně pracovat? Cílem této práce bude odpovědět na vybrané otázky v jednotlivých kapitolách a poskytnout tak ucelený přehled o propojení UI s instituty trestního práva. Bude tak dosaženo převážně metodou komparace právních systémů různých zemí se zaměřením na využití UI policejními (donucovacími) orgány při vyšetřování trestné činnosti.

---

[1] *What is artificial intelligence and how is it used?* European Parliament, 2023. Dostupné z: https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used [cit. 2024-05-24].

[2] Viz například https://www.reuters.com/legal/litigation/how-copyright-law-could-threaten-ai-industry-2024-2024-01-02/ [cit. 2024-05-24] a https://www.epravo.cz/top/clanky/mestsky-soud-v-praze-o-umele-inteligenci-a-autorskem-pravu-117318.html [cit. 2024-05-24].

Téma práce není v českém trestněprávním kontextu příliš známé a natolik probádané jako tomu je v zahraničí. Hlavními zdroji proto bude především zahraniční odborná literatura, soudní rozhodnutí a cizí internetové zdroje. Práce však poskytne i úhel pohledu z perspektivy českého práva.

V první části práce bude nejprve uveden vztah UI s trestním právem na několika praktických příkladech, na kterých se ukáže nejen to dobré, ale i to špatné, co může tato technologie nabídnout. Základním východiskem bude poté definování pojmu UI, ačkoliv bezpochyby nebude možné dosáhnout jediné perfektní definice, která by tento pojem po obsahové stránce kompletně vyčerpala. Pod obecně přijímaným pojmem UI se navíc skrývá mnoho dalších podpojmů, které budou pro úplnost rovněž stručně definovány. Dále se pak práce pokusí shrnout dosavadní snahy o trestněprávní úpravu UI na mezinárodní, evropské a státní úrovni. Zvlášť se zaměří na připravované nařízení Evropské unie, tzv. Akt o umělé inteligenci, který by měl být finálně schválen během roku 2024. Poté přijde na řadu jedna z nejsložitějších trestněprávních otázek v souvislosti s UI, a to její trestní odpovědnost, kterou odborná literatura dělí na tři teoretické modely, ze kterých bude tato práce vycházet. Každý z nich bude představen samostatně a také ve vzájemném provázání modelů mezi sebou. Na to naváže ukázka nových podob trestné činnosti, kterou pachatelé praktikují s využitím UI, se zvláštním zřetelem na technologii *deepfake* představující jedno z největších bezpečnostních rizik blízké budoucnosti. Dalším dílčím tématem bude zhodnocení potencionálního vlivu UI na rozhodování v trestním řízení. Zde budou odkryty zásadní problematické aspekty použití UI soudci a vězeňskou službou.

Druhá část této práce bude zkoumat využití UI policejními orgány při vyšetřování trestných činů. Detailněji se bude věnovat oblastem predikce trestné činnosti, shromažďování a analýzy důkazů, a biometrické identifikace, ve kterých se UI využívá nejvýrazněji. V rámci predikce trestné činnosti se práce zaměří na proces sestavování map kriminalit a na využití prediktivních modelů k předpovídání kriminality u konkrétních jedinců. V kontextu shromažďování a analýzy důkazů bude kladen důraz na použití UI k ulehčení přijímání trestních oznámení a vyvinutí nových forenzních metod ke zpracování velkého množství digitálních dat a rozboru důkazních materiálů otisků prstů a vzorků DNA. Téma biometrické identifikace bude zúženo na automatizované rozpoznávání obličeje a v těchto mezích bude prozkoumána legalita a legitimita jeho použití policií na veřejně dostupných místech v reálném čase. Taktéž budou řešeny otázky ochrany osobních údajů, transparentnosti a chybovosti systémů UI v těchto vybraných oblastech.

Ve třetí části práce bude zmíněn potenciál UI v oboru trestního práva, a zároveň budou předloženy navazující otázky k diskuzi, které mohou být relevantní pro další zkoumání této problematiky. S ohledem na velmi rychlý technologický vývoj lze očekávat, že tato práce zanedlouho nebude věrně odrážet aktuální stav využití UI v praxi. Toto úskalí je v práci zohledněno a z tohoto důvodu jsou součástí diskuze i návrhy na doporučení k dosažení efektivní aplikace technologie UI, která se budou opírat o nejdůležitější zjištění a poznatky ze současného trestněprávního prostředí.

1. Umělá inteligence v trestním právu

UI má potenciál stát se dlouhotrvající a nezbytnou součástí trestního práva. Do některých dílčích oblastí už zasahuje takovým způsobem, že je s ním neoddělitelně spjata. Jde především o technologie predikce trestné činnosti nebo biometrické identifikace. Systémy UI však pronikají i do procesů trestního řízení. Nicméně, k naplnění základních funkcí trestního práva v zásadě nepotřebujeme technologie žádné; trestní právo je takříkajíc soběstačné. K zahájení trestního řízení (shromáždění a analýzy důkazů, výslechy svědků atd.), následnému podání obžaloby, řízení před soudem a dosažení soudního rozhodnutí je třeba nanejvýš tužky a papíru. Posun díky využití nových technologií, které zrychlují a zefektivňují celý proces trestního řízení, lze bezesporu uvítat. Technologie UI tedy nebyla výjimkou a orgány činné v trestním řízení ji postupně začleňují do trestněprávní praxe. Aplikace UI se ale od jiných moderních technologií liší především ve složitosti jejího fungování a v potřebě zpracování neuvěřitelného množství dat k tomu, aby fungovala správně a efektivně. Na následujících příkladech využití UI ve světě je možné pozorovat, co dobrého může UI přinést v oblasti trestního práva, ale i jak velké nebezpečí představuje, když se dostane do špatných rukou.

Ve Velké Británii si tamní ministerstvo spravedlnosti vytrénovalo vlastní neuronovou síť k identifikaci faktorů, které ovlivňují vznik problémů ve věznicích.[3] Algoritmus propojuje nejčastěji zmiňované incidenty ze zpráv inspekcí věznic a umožňuje tak vězeňským pracovníkům rychle odhalit například příčiny konfliktů mezi vězni. Výstupy pak slouží ke zlepšování vězeňských politik napříč celou zemí.

Na hraničních přechodech Maďarska, Lotyšska a Řecka jsou pilotně spuštěny inteligentní systémy detekce lži (*iBorderCtrl*).[4] Systémy profilují cestující na základě automatizovaného pohovoru, uskutečněného přes webovou kameru, během kterého systém analyzuje 38 mikrogest v detailu obličeje vyslýchané osoby. Až při vyhodnocení odpovědí jako pravdivých umožní překročení hranice.

Nizozemská charita *Terre des Hommes*, v rámci svého projektu na ochranu dětí před sexuálním zneužíváním na internetu, vytvořila chatbota jménem *Sweetie*, který byl navržen tak,

[3] *How the Ministry of Justice used AI to compare prison reports*. Online. Ministry of Justice, 2019. Dostupné z: https://www.gov.uk/government/case-studies/how-the-ministry-of-justice-used-ai-to-compare-prison-reports--2 [cit. 2024-05-04].
[4] *Obrana práv uprchlíků a migrantů v digitálním věku*. Online. Amnesy International, 2024. Dostupné z: https://www.amnesty.cz/zprava/5889/obrana-prav-uprchliku-a-migrantu-v-digitalnim-veku [cit. 2024-05-04].

aby vypadal jako 10letá dívka a konverzoval s lidmi projevující sexuální zájem u dětí.[5] Cílem bylo tyto online predátory vystopovat a identifikovat, popř. zaslat jejich informace policejním orgánům. Vylepšená verze *Sweetie 2.0* dokázala zvládnout tisíce konverzací najednou a odesílat pachatelům varovné zprávy o tom, že se dopouštějí trestné činnosti.[6] Tuto technologii, tzv. kybernetického agenta (*cyber agent*) lze efektivně použít v případě, že projde tzv. Turingovým testem,[7] ve kterém si lidé neuvědomují, že komunikují s UI, což v tomto případě nebyl žádný problém, protože během prvních 8 týdnů provozu se na tohoto chatbota obrátilo více než 20 000 predátorů ze 71 zemí.[8] Později se však ukázalo, že v několika jurisdikcích je odsouzení těchto pachatelů značně obtížné, jelikož ke skutečnému zneužívání dětí v zásadě nedocházelo (není možné sexuálně zneužít software).[9, 10] Kromě toho se tato technologie zároveň sama nesmí dopouštět trestné činnosti a neměla by se učit a osvojovat si nezákonné chování. Splnění tohoto kritéria bylo podstatně složitější. V mnoha jurisdikcích byl totiž postup, jakým byla technologie použita, kvalifikován jako navádění, provokace nebo podněcování k trestnému činu (srov. § 365 trestního zákoníku). I přesto *Sweetie* poslala za mříže desítky pachatelů v Austrálii, Belgii a Velké Británii.

Modernizace vybavení bezpečnostních sborů s sebou přinesla i rozšíření bezpilotních vzdušných systémů (drony), které jsou úzce provázány s moderními poznatky z oblasti UI a stále častěji využívány v rámci činnosti policie. Drony se využívají k dohledu nad sportovními, kulturními, politickými a dalšími společenskými akcemi s výskytem většího počtu osob na jednom místě a také k obecné prevenci trestné činnosti. Stejně tak je lze zneužít k páchání těch nejzávažnějších (i teroristických) trestných činů. Zneužití dronů může spočívat i v profilování vybrané skupiny obyvatelstva jako v případě zastrašování pokojných demonstrantů Kambodžskou vládou pod rouškou zajištění veřejného pořádku a bezpečnosti v roce 2022.[11] V dnešní době hrají

[5] *Sweetie*. Online. Terre des Hommes, 2022. Dostupné z: https://www.terredeshommes.nl/en/projects/sweetie [cit. 2024-05-04].
[6] *Sweetie: 'Girl' chatbot targets thousands of paedophiles*. Online. BBC, 2017. Dostupné z: https://www.bbc.com/news/av/technology-42461065 [cit. 2024-05-04].
[7] TURING, Alan. M. *I.-COMPUTING MACHINERY AND INTELLIGENCE*. Online. Mind, Vol. LIX, No. 236, 1950. s. 433-460. ISSN 1460-2113. Dostupné z: https://doi.org/10.1093/mind/LIX.236.433 [cit. 2024-02-19].
[8] SCHWEIZER, Kristen. *Avatar Sweetie exposes sex predators*. Online. The Age, 2014. Dostupné z: https://www.theage.com.au/world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html [cit. 2024-05-04].
[9] SCHERMER, Bart; GEORGIEVA, Ilina; VAN DER HOF, Simone a KOOPS, Bert-Jaap. *Legal Aspects of Sweetie 2.0*. Online. In: VAN DER HOF, Simone; GEORGIEVA, Ilina; SCHERMER, Bart a KOOPS, Bert-Jaap (ed.). Sweetie 2.0. Information Technology and Law Series. The Hague: T.M.C. Asser Press, 2019. s. 1-94. ISBN 9789462652873. Dostupné z: https://doi.org/10.1007/978-94-6265-288-0_1 [cit. 2024-05-04].
[10] V českém právním kontextu by se dalo uvažovat o naplnění znaků trestného činu navazování nedovolených kontaktů s dítětem podle § 193b trestního zákoníku.
[11] CHANDRAN, Rina. *Activists say China's new Silk Road equips autocrats with spy tech*. Online. Context, 2022. Dostupné z: https://www.context.news/surveillance/activists-say-chinas-new-silk-road-equips-autocrats-with-spy-tech [cit. 2024-05-04].

drony obrovskou roli i ve válečných konfliktech (např. při ruské invazi na Ukrajinu[12]), a to nejen jako monitorovací a průzkumnické systémy, ale i jako nosiče výbušnin, střelných zbraní, či smrtících chemikálií a biologického materiálu. Výhodou oproti tradičním letounům je především skutečnost, že se jedná o tiché stroje bez posádky. Jsou také dostupné v různých velikostech, takže je s nimi možné manévrovat i v malých prostorech, a nejsou tak finančně nákladné na provoz. Drony mohou být aktivně ovládány na dálku, předem naprogramovány pomocí letových GPS souřadnic, nebo právě ovládány dynamickými autonomními systémy UI.[13]

Největšího zneužití UI se dopouští Čína, která používá technologie biometrické identifikace a monitoringu na sociálních sítích, k plošnému sledování svého obyvatelstva.[14] Funguje tam jakýsi „systém sociálního kreditu“ pro bodování lidí na základě hodnocení jejich sociálních kontaktů a chování jako je třeba nezaplacení daní, ale i kouření ve vlaku nebo venčení psa bez vodítka. Všechny údaje se následně shromažďují v Centru pro posouzení pověsti (*Credit Reference Center of the People's Bank of China*). Cílem má být „hodnověrné“ chování čínských občanů založené na principu pokut a odměn. Lidé s vysokým kreditem tak mohou volně cestovat; pro ty s nízkým kreditem je cestování omezeno, či úplně zakázáno. Čínské úřady mohou na základě sociálního kreditu znemožnit obyvatelům nákup letenek a dalších jízdních dokladů, nebo vybraným společnostem zakázat účastnit se výběrových řízení, dražit nemovitosti nebo obchodovat s cennými papíry.[15]

Další úmyslné zneužití UI k perzekuci obyvatelstva čínskou vládou můžeme pozorovat na extrémním případu Ujgurů a dalších muslimských menšin v autonomní oblasti Sin-ťiang.[16] Tyto skupiny obyvatel jsou Čínou vnímány jako etnická hrozba, které se snaží zbavit nejrůznějšími prostředky – politickým stíháním, zadržováním v pracovních táborech, náboženským utlačováním, omezováním svobody pohybu apod. K získání úplné kontroly nad ujgurským obyvatelstvem se používá i mnoho systémů UI schopných zaměřit a sledovat vybrané jedince. Místní donucovací

[12] *Drony Nemesis*. Online. Skupina D z.s., 2024. Dostupné z: https://www.dronynemesis.cz/ [cit. 2024-05-04].
[13] DVOŘÁK, Marek. Bezpilotní letadla (drony) a oprávnění policistů k zamezení jejich provozu. In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 280-293. ISBN 9788087284957.
[14] ALLEN-EBRAHIMIAN, Bethany. *Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm*. Online. International Consortium of Investigative Journalists, 2019. Dostupné z: https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/ [cit. 2024-05-04].
[15] KUO, Lily. *China bans 23m from buying travel tickets as part of 'social credit' system*. Online. The Guardian, 2019. Dostupné z: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system [cit. 2024-05-04].
[16] *"Break Their Lineage, Break Their Roots". China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims*. Online. Human Rights Watch, 2021. Dostupné z: https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting [cit. 2024-05-04].

orgány uplatňují obzvláště algoritmy k automatizovanému rozpoznávání obličejů na místech po celé ujgurské autonomní oblasti jako jsou školy, nákupní centra, mešity, nemocnice a obytné zóny. Dokonce každý kuchyňský nůž, který se prodá v Sin-ťiangu, je vybaven QR kódem obsahujícím osobní údaje jeho uživatele (číslo průkazu totožnosti, fotografie, etnická příslušnost, adresa atd.). Kromě toho musí být všechna vozidla povinně vybavena lokalizačním zařízením. Čína také masivně shromažďuje informace z elektronických zařízeních, včetně chytrých telefonů a Wi-Fi routerů, které pak využívá k profilování a trasování ujgurské menšiny.

1.1 Definice, související pojmy a dělení

Pro mnohé představuje UI velmi široký a nejednoznačný pojem. Z pohledu práva je důležité si definovat, co se pod tímto pojmem skrývá, aby bylo možné jej efektivně regulovat. Pro odvětví trestního práva je definice neméně významná. Systémy UI mohou do trestněprávních vztahů vstupovat v různých podobách, a to především v souvislosti s trestní odpovědností a jejím využitím v rámci činnosti orgánů činných v trestním řízení.

Ještě před úplně prvním zformulováním konkrétní definice se za UI považoval systém splňující tzv. Turingův test,[17] ve kterém se posuzuje, zda je člověk schopen rozlišit od sebe odpověď vygenerovanou strojem a odpověď poskytnutou skutečnou osobou. Stroj je pak považován za „inteligentní“, pokud tento člověk odpovědi od sebe spolehlivě rozlišit nedokáže.

Za jednu z nejstarších a nejzdařilejších je považována definice, která říká, že UI *„představuje vytvoření stroje chovajícího se způsobem, který bychom v případě člověka označili za inteligentní, a který zvládne provádět úkoly obvykle vyžadující lidskou inteligenci jako jsou řešení problémů, učení, vnímání, uvažování, porozumění jazyku a rozhodování.“*[18] Další autoři označovali za UI program, který bude v nahodilém světě fungovat alespoň stejně dobře jako člověk, s tím, že k tomu, aby byl program inteligentní, nemusí nutně disponovat znalostmi.[19] Při definování UI se někteří autoři[20] soustředili na vědecky měřitelné hodnoty inteligence, spíše než

[17] TURING, Alan. M. *I.-COMPUTING MACHINERY AND INTELLIGENCE*. Online. Mind, Vol. LIX, No. 236, 1950. s. 433-460. ISSN 1460-2113. Dostupné z: https://doi.org/10.1093/mind/LIX.236.433 [cit. 2024-02-19].
[18] MCCARTHY, John; MINSKY, Marvin; ROCHESTER, Nathaniel a SHANNON, Claude. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Online. AI Magazine, 1955. s. 11. Dostupné z: https://doi.org/10.1609/aimag.v27i4.1904 [cit. 2024-02-19]
[19] DOBREV, Dimiter. *A Definition of Artificial Intelligence*. Online. Mathematica Balkanica, New Series, Vol. 19, 2005. s. 2. Dostupné z: https://doi.org/10.48550/arXiv.1210.1568 [cit. 2024-02-19]
[20] HOFFMANN, Christian Hugo. *Is AI intelligent? An assessment of artificial intelligence, 70 years after Turing*. Online. Technology in Society, 2022. s 2. Dostupné z: https://doi.org/10.1016/j.techsoc.2022.101893 [cit. 2024-02-19]

na jednoduché pojmenování toho, co UI je a co není. Srovnání UI s člověkem bylo postupně opuštěno, jelikož i ty nejlepší systémy nedosahovaly sofistikovanosti a komplexnosti lidského myšlení. Jinými slovy, doposud nebyla vyvinut tak inteligentní systém, který by se rovnal inteligenci člověka.

Díky technologickému pokroku se však UI čím dál tím více lidské inteligenci přibližuje. Není proto od věci zapřemýšlet i nad často diskutovaným konceptem samostatné právní osoby, tzv. „elektronické osoby". Definici elektronické osoby můžeme formulovat jako *„útvar odlišný od člověka (fyzické osoby), který je nadaný schopností samostatně rozhodovat a jednat, resp. je nadaný právní osobností od svého vzniku do svého zániku (obdobně jako tomu je u právnické osoby)."*[21] Jedná se o velmi ambiciózní návrh, se kterým pochopitelně souvisí obsáhlá revize a adaptace současných právních předpisů, a zároveň překopání stěžejních právních myšlenek. Stejně jako u konceptu právnických osob, který se na počátku zdál být lidstvu zcela revoluční, by však nemuselo být natolik složité si postupem času na novou osobu v právu navyknout (více v kapitole 1.3.3).

V právu je obecně důraz kladen také na přesné vymezení definičních znaků a vlastností definovaného pojmu. Podle některých autorů[22] jsou to u UI především schopnost komunikace, vnitřní znalosti (tj. znalosti o sobě samé), vnější znalosti (tj. znalosti o světě kolem), cílevědomé chování a kreativita. Jiní[23] uvádějí další klíčové prvky jako (1) autonomie; (2) skutečnost, že rozhodování provádí jiná entita, než pro kterou je proces autonomního řešení přirozený v biologickém slova smyslu; a (3) schopnost řešit problémy prostřednictvím interakce s vnějším prostředím. Prvním a třetím prvkem se odlišuje od pouhé automatizace určitého procesu. Druhým prvkem od lidské, přesněji řečeno živočišné inteligence, protože zvířata se do jisté míry také rozhodují autonomně.

Ani státy a mezinárodní organizace nám rovněž nepodávají jednoznačný výklad pojmu. Právní řády zemí světa se teprve postupně připravují na nevyhnutelnou potřebu regulace oblasti UI, se kterou přijde i zakotvení právní definice. Nicméně, v posledních letech jsou přijímány nejrůznější národní strategie a doporučení pravidel obsahující alespoň výchozí rámec pro

[21] MIKEŠ, Stanislav. *Právo ve věku inteligentních strojů*. Online. Bulletin advokacie, 2018. Dostupné z: http://www.bulletin-advokacie.cz/pravo-ve-veku-inteligentnich-stroju [cit. 2024-02-19]
[22] HALLEVY, Gabriel. *The Criminal Liability of Artificial Intelligence Entities*. Online. SSRN Electronic Journal, 2010. s. 6. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.1564096 [cit. 2024-02-18]
[23] PROVAZNÍK, Jan a MULÁK, Jiří. Roboti za mřížemi - je české trestní právo připraveno na rozvoj umělé inteligence? In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 258. ISBN 9788087284957.

konkrétní definici.[24] V současné chvíli tak problém nejednoznačnosti pojmu UI v právním povědomí dál roste.[25] O jednotný přístup k UI pokouší Evropské unie v rámci činnosti expertní skupiny.[26] Toto snažení vyústilo v přijetí nařízení, tzv. Aktu o umělé inteligenci (více v kapitole 1.2.1), který definuje systém UI jako strojový systém navržený tak, aby fungoval autonomně, vykazující určitou schopnost adaptace, který k dosažení explicitních nebo implicitních cílů na základě přijatých vstupů odvozuje, jak nejlépe vygenerovat požadované výstupy jako jsou predikce, obsah, doporučení nebo rozhodnutí schopné ovlivnit fyzické nebo virtuální prostředí.[27]

V krajním případě může pomoci i samotná UI, která, mimo jiné, dokáže definovat i sama sebe jako *„komplexní soubor algoritmů, dat a pravidel, které jsou navrženy tak, aby umožnily počítačům simulovat lidskou inteligenci nebo vykazovat schopnosti spojené s inteligencí. Tato inteligence může zahrnovat schopnost učení, rozpoznávání vzorů, rozhodování, řešení problémů a komunikace s okolím. Systémy umělé inteligence mohou být navrženy k plnění specifických úkolů nebo mohou být obecnější a schopny se adaptovat na různé úkoly.“*[28]

S ohledem na účel a rozsah této práce budou stručně definovány i související podpojmy, které ústřední pojem UI zastřešuje. Činnost autonomního systému UI se může projevit jak ve fyzickém (**robotika**), tak i ve virtuálním světě. Používá různé výpočetní techniky a pracovní postupy jako je **algoritmus**, **neuronové (umělé) sítě** a **strojové učení** (*machine learning*). K učení autonomních systémů se používají velké **soubory testovacích dat** (*big data*).

Robotika je ztělesněním UI ve fyzickém světě vzájemně působící s dalšími systémy, která vyžaduje aplikaci strojního inženýrství a teorie. Robot se zabudovanou UI je schopný vnímat, logicky myslet, samostatně jednat a učit se. Alternativou Turingova testu pro roboty je tzv. kávový

[24] *Governments race to regulate AI tools*. Online. Reuters, 2024. Dostupné z: https://www.reuters.com/technology/governments-race-regulate-ai-tools-2023-10-13/ [cit. 2024-02-19]
[25] SHCHITOVA, A.A. *Definition of Artificial Intelligence for Legal Regulation*. Online. In: Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020). Paris: Atlantis Press, 2020. s. 616-620. ISBN 9789462392915. Dostupné z: https://doi.org/10.2991/aebmr.k.201205.104 [cit. 2024-02-19].
[26] *A Definition of AI: Main Capabilities and Scientific Disciplines*. Online. Brussels: European Commission, 2018. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines [cit. 2024-02-19]
[27] Překlad autora.
[28] [Jak bys jako umělá inteligence definovala "systém umělé inteligence"?] In: ChatGPT 3.5 version. Online. OpenAI, 2024. Dostupné z: https://chat.openai.com/share/bfd3b8a6-7b67-4d67-9d9c-5f847b462b10 [cit. 2024-02-19]

test (*barista test*),[29] kterým by prošel dostatečně inteligentní robot schopný zorientovat se v jakékoliv kuchyni a úspěšně připravit šálek kávy.[30]

Algoritmus je pracovní postup skládající se z několika prvků, který vždy vydá nějaký výsledek (prvek rezultativnosti) po konečném počtu provedených kroků (prvek finitnosti, konečnosti), kdy každá operace je přesně určena pomocí základních instrukcí, o kterých je jasné, jak se provedou (prvek elementárnosti, jednoduchosti), a na tento postup nemá žádný vliv náhoda nebo svobodná vůle vykonavatele (prvek determinovanosti, jednoznačnosti)[31]. Každému algoritmu je před započetím nebo v průběhu zadán určitý počet vstupů. Výsledkem je určitý výstup, kterým se rozumí výsledná veličina vztahující se ke vstupům.[32] Zjednodušeně řečeno, jde o *„metodu systematického a automatizovaného výpočtu pomocí souboru příkazů, které musí být provedeny, aby se dosáhlo požadovaného výsledku nebo řešení.“*[33]

Neuronové (umělé) sítě vzájemně propojují velké množství procesních výpočetních jednotek (neuronů), které zpracovávají vstupní data. V tréninkové fázi přidělují vstupním datům různou váhu tak, aby konečný výstup co nejblíže odpovídal vzoru, který byl použit během procesu učení. Závěrem by mělo být úspěšné posouzení konkrétního příkladu na základě předchozího učení, se kterým se systém setká poprvé.[34] Neuronové sítě mají tři vrstvy: vstupní vrstvu, do které se vloží data, skrytou vrstvu, kde se odehrává rozhodování a výstupní vrstvu, která vrací požadovaný výsledek.[35]

Strojové učení (*machine learning*) má za cíl, aby se systém na základě vložených dat sám naučil, jak nejlépe dosáhnout žádoucího výsledku. Nejrozšířenější jsou tři druhy strojového učení: učení s učitelem (*supervised learning*), učení bez učitele (*unsupervised learning*) a zpětnovazebné

---

[29] ROURK, Chris. *The Turing Test is so Last Century: Introducing the Barista Test for Artificial General Intelligence*. Online. Medium, 2023. Dostupné z: https://medium.com/predict/the-turing-test-is-so-last-century-the-barista-test-for-artificial-general-intelligence-faf91034fa8c [cit. 2024-03-02].

[30] KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. s. 16. ISBN 9788075987839.

[31] LESSNER, Dan; LÁNA, Martin; PODRÁZKOVÁ TOMKOVÁ Michala a HAUT Jiří. *Základy informatiky pro střední školy*. Online. Jihočeská univerzita v Českých Budějovicích, 2020. ISBN 978807394785-9. Dostupné z: https://popelka.ms.mff.cuni.cz/~lessner/mw/index.php/Hlavn%C3%AD_strana [cit. 2024-03-02].

[32] KNUTH, Donald E. *Umění programování. 1. díl, Základní algoritmy*. Brno: Computer Press, 2008. s. 5. ISBN 9788025120255.

[33] FIALOVÁ, Eva; MATEJKA, Ján a GÜTTLER, Vojen. *Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod*. Praha: Ústav státu a práva AV ČR, 2020. s. 20. ISBN 9788087439425. Dostupné z: https://www.ilaw.cas.cz/casopisy-a-knihy/knihy-a-e-knihy/profilovani-a-automatizovane-rozhodovani-(nejen)-ve-svetle-lidskych-prav-a-zakladnich-svobod.html [cit. 2024-03-02].

[34] KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. s. 14. ISBN 978807598783-9.

[35] HOLČÍK, Jiří a KOMENDA, Martin. *Matematická biologie: e-learningová učebnice*. Online. Brno: Masarykova univerzita, 2015. ISBN 9788021080959. Dostupné z: https://portal.matematickabiologie.cz/ [cit. 2024-03-02].

učení či učení posilováním (*reinforcement learning*). Při učení s učitelem má systém UI k dispozici příklady správných výstupů, podle kterých dokáže aplikovat postup na předem neznámé situace. V rámci techniky učení bez učitele by měl systém UI dospět ke správnému výstupu sám pouze na základě zpracování vstupních dat, aniž by měl k dispozici správné výstupy tím, že shlukuje sobě podobné elementy ve vstupním prostoru, které poté třídí do hledaných skupin. Učení posilováním nebo také Hebbovo učení funguje na principu motivace systému UI k co nejlepším výsledkům posilováním nebo oslabováním jednotlivých vazeb mezi vstupními daty, tzn. že pokud rozhodnutí směřuje ke správnému výstupu, jsou vazby posíleny; v opačném případě jsou oslabeny.[36] Aktuálně nejprogresivnějším druhem strojového učení je tzv. hluboké učení (*deep learning*) spočívající ve využití algoritmů především neuronových sítí s velkým počtem navrstvených dat. Hloubku modelu představuje počet vrstev zapojených do sebe tak, že výstup jedné z nich je vstupem následující vrstvy.[37]

Soubory testovacích dat (*big data*) používaných k učení systémů UI jsou takové velikosti, že není možné je v rozumném čase analyzovat běžně používanými softwarovými postupy. Vyznačují se tzv. „pěti V“: velikostí (*Volume*), variabilitou (*Variability*), hodnotou (*Value*), věrohodností (*Veracity*) a rychlostí (*Velocity*). Získávání užitečných informací z těchto souborů a jejich analýza je založena na procesu těžby dat (*data mining*).[38]

Obecně uznávaným a nejrozšířenějším dělením[39] je dělení UI podle stupně jejího vývoje či vývojových stádií: **1. Reaktivní** (*reactive*), která řeší pouze předem definované problémy a neučí se z předchozích výsledků a zkušeností (např. jednodušší algoritmy); **2. S omezenou pamětí** (*limited memory*), která sebe sama optimalizuje na základě předchozí činnosti (např. autonomní vozidla); **3. S teorií mysli** (*theory of mind*), která rozpoznává a chápe všechny složky vnitřního života člověka jako jsou emoce, postoje, představy (v praxi se teprve rozvíjí[40]); a **4. S vědomím sebe sama** (*self-aware*), která si uvědomuje vlastní existenci (zatím neexistuje a není ani shoda na

[36] Tamtéž.
[37] KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. s. 11-12. ISBN 9788075987839.
[38] Tamtéž. s. 13.
[39] BETZ, Sunny a WHITFIELD, Brennan. *7 Types of Artificial Intelligence: From chatbots to super-robots, here's the types of AI to know and where the tech's headed next*. Online. Built In, 2024. Dostupné z: https://builtin.com/artificial-intelligence/types-of-artificial-intelligence [cit. 2024-02-18]
[40] JOHN, Camila. *Theory of Mind AI: The Next Frontier in Artificial Intelligence*. Online. Medium, 2023. Dostupné z: https://medium.com/bestai/theory-of-mind-ai-the-next-frontier-in-artificial-intelligence-92cb1963ab5d [cit. 2024-02-19]

tom, jak by měla vypadat[41]). Dále můžeme UI dělit podle jejích schopností na **úzkou** (*narrow artificial inteligence*) nadanou řešit pouze omezený obor aktivit, tzn. že vyřeší jen konkrétní problém; **obecnou** (*general artificial inteligence*) způsobilou vykonávat všechno, čeho je schopný člověk na stejné úrovni, tzn. že se jedná o napodobení lidské inteligence (předpovědi hlásí, že se tento typ objeví do 5 let, ne-li dříve[42]); a **umělou superinteligenci** (*artificial super-inteligence*) schopnou překonat cokoliv, co zvládne člověk.

1.2 Trestněprávní rámec

Na mezinárodní úrovni zatím nedošlo k žádné konkrétní významné právní regulaci ohledně UI jako celku, natož pak v trestněprávní rovině. Vrcholem mezinárodní spolupráce jsou pro tuto chvíli pouze politická prohlášení, doporučení nebo studie.[43] Na používání UI lze však nepochybně aplikovat soudobé mezinárodní právo, neboť to je technologicky neutrální (jeho zásady platí pro staré i nové technologie), dostatečně obecné a natolik flexibilní, aby se přizpůsobilo i mimořádně rychlému technologickému vývoji jako tomu je v oblasti UI. Mezinárodní právo trestní se tedy vztahuje na používání UI jednak státy, které jsou vázány množstvím mezinárodních smluv, jednak do jisté míry i na korporace, které se podílejí na dodržování lidských práv a svobod, a částečně i na jednotlivce, kteří mohou vstupovat do mezinárodních trestněprávních vztahů (např. mohou páchat mezinárodní zločiny). Většina otázek sice spadá do výlučné pravomoci jednotlivých států, ovšem některé jsou inherentně předmětem práva mezinárodních organizací nebo nestátních subjektů (např. Mezinárodní trestní soud v Haagu).[44]

Evropská unie posledních 10 let prosazuje snahu o jednotný přístup k UI, která bude především důvěryhodná a bezpečná pro její uživatele s důrazem na ochranu osobních údajů.[45] První myšlenky na potřebu souhrnných legislativních pravidel pro UI vztahující se i k trestnímu

[41] GLOVER, Ellen a KOSS, Hal. *What Is Sentient AI?: Some experts believe it's only a matter of time before artificial intelligence systems can think and feel like humans*. Online. Built In, 2024. Dostupné z: https://builtin.com/artificial-intelligence/sentient-ai [cit. 2024-02-19]

[42] KARLÍK, Tomáš. *Obecná umělá inteligence tu bude do pěti let, věří šéf společnosti Nvidia*. Online. ČT24, 2024. Dostupné z: https://ct24.ceskatelevize.cz/clanek/veda/obecna-umela-inteligence-tu-bude-do-peti-let-veri-sef-spolecnosti-nvidia-346726 [cit. 2024-05-04].

[43] Například *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, kterou k únoru 2024 podepsalo přes 50 států (včetně České republiky), nebo *Bletchley Declaration*, jež vzešla z Konference o bezpečnosti UI v Británii.

[44] DIAS, Talita de Souza a SAGOO, Rashmin. *AI Governance in the Age of Uncertainty: International Law as a Starting Point*. Online. Just Security, 2024. Dostupné z: https://www.justsecurity.org/90903/ai-governance-in-the-age-of-uncertainty-international-law-as-a-starting-point/ [cit. 2024-02-20].

[45] *Evropský přístup k umělé inteligenci*. Online. Evropská komise, 2024. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/european-approach-artificial-intelligence [cit. 2024-02-20].

právu představil Evropský parlament už v roce 2017 v rámci evropských pravidel robotiky,[46] ve kterých předvídá dosud nevyjasněnou otázku právní odpovědnosti nebo problematiku autonomních vozidel a dálkově řízených letadlových systémů (dronů). V roce 2018 Evropský parlament poukazoval na rostoucí úlohu UI v oblasti kybernetické ofenzivy (zneužití ze strany nepřátelských států a organizovaných zločineckých skupin) i defenzivy (rozvoj v oblasti kybernetické ochrany).[47] Evropská komise ve stejném roce vydala sdělení k UI,[48] kde upozorňuje na rizika zneužití UI k páchání trestné činnosti a na výzvy, které přinese v oblasti kybernetického zabezpečení. Následoval koordinovaný plán pro UI,[49] který poprvé zmiňuje aktivní používání UI donucovacími orgány pro zlepšení prevence, odhalování a vyšetřování trestné činnosti a terorismu. Rok 2020 přinesl dokument obecné povahy, tzv. Bílou knihu,[50] která jako první varuje před algoritmy UI používaných k předpovídání recidivy trestné činnosti anebo analýze obličejů, kvůli jejich tendenci vykazovat genderovou a rasovou předpojatost, či diskriminaci na základě státní příslušnosti.

Podrobněji se Evropský parlament věnoval UI v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech také v roce 2021.[51] Navazuje na předešlé myšlenky a rozvíjí je v reakci na stále častější využití při prosazování práva za účelem snížení kriminality a využití v soudnictví ve snaze o zajištění objektivnějšího rozhodování. Podporuje zavedení jednotného přístupu Evropské unie k právní regulaci z důvodu značných rozdílů napříč členskými státy, a zároveň vybízí k zapojení třetích zemí k nalezení společných mezinárodních standardů a etických pravidel. K efektivnímu využití technologií UI prosazuje Evropský parlament navýšení finančních prostředků a odborných školení pro zaměstnance policie a soudů. Také formuluje konkrétní požadavky na nástroje UI používané policejními a soudními orgány, a to především zavedení jasných a srozumitelných pravidel pro vývojáře, nutnost posouzení rizik a dopadů před započetím

[46] *Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52017IP0051&qid=1716363778912 [cit. 2024-02-20].
[47] *Usnesení Evropského parlamentu ze dne 13. června 2018 o kybernetické obraně*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52018IP0258&qid=1709297406000 [cit. 2024-02-20].
[48] *Sdělení Komise Evropskému Parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru Regionů ze dne 25. dubna 2018 (Umělá inteligence pro Evropu)*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52018DC0237&qid=1716363810741 [cit. 2024-02-20].
[49] *Sdělení Komise Evropskému Parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru Regionů ze dne 7. prosince 2018 (Koordinovaný plán v oblasti umělé inteligence)*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52018DC0795 [cit. 2024-02-20].
[50] *Bílá kniha o umělé inteligenci - evropský přístup k excelenci a důvěře ze dne 19. února 2020*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020DC0065 [cit. 2024-02-20].
[51] *Usnesení Evropského parlamentu ze dne 6. října 2021 o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52021IP0405&qid=1716364055838 [cit. 2024-02-20].

používání systémů a zajištění odolnosti vůči vnějším útokům (např. *data poisoning*). Důraz klade na respektování základních práv a svobod, přísnější demokratickou kontrolu, nezávislý lidský dohled a transparentnost těchto systémů. Podstatnou pozornost věnuje Evropský parlament tématu biometrické identifikace, jejíž použití by mělo být omezeno jen na odůvodněné účely vymezené ve vnitrostátních předpisech členských států, a tématu ochrany osobních údajů ve spojení s již nastavenými unijními pravidly.[52] Varování se týká neprůhledného rozhodování systémů UI, možného vzniku nerovnosti mezi veřejnými a soukromými subjekty (např. obtíže při napadání výsledků UI u soudu, zejména ze strany vyšetřovaných osob) a přílišné důvěry ve zdánlivě objektivní povahu nástrojů UI používaných v trestním soudnictví. Obava z některých systémů UI vedla Evropský parlament k několika zákazům používání (např. *ClearView*) a omezení používání UI k navrhování soudních rozhodnutí nebo hromadnému rozpoznávání obličeje a dalších lidských prvků (např. chůze nebo hlasu).

Světovými tahouny technologického vývoje UI a s tím i související právní úpravy, jsou již delší dobu státy dálného východu, zejména Čína. Jak již bylo zmíněno na případě ujgurské menšiny, čínská vláda zneužívá UI převážně k potlačení osobních svobod svých občanů, a z toho důvodu se zabývat právní úpravou v čínském kontextu nebudeme.

Dalším velkým hráčem na trhu se systémy UI jsou Spojené státy americké, kde působí ty největší technologičtí giganti (např. *IBM*, *Microsoft*, *OpenAI*, *NVIDIA*, *Meta* a další).[53] Právní úprava UI v oblasti vymáhání práva se v USA prozatím vyskytuje převážně na úrovni jednotlivých měst. Většinou jde o zákazy používání automatizovaného rozpoznávání obličeje policejními orgány jako tomu je například v San Francisku.[54] V současné době tak v USA neexistují žádné komplexní federální zákony nebo jiné právní předpisy, které by byly uzákoněny speciálně pro regulaci UI.

Za trestněprávní regulaci UI bychom mohli považovat francouzskou právní úpravu režimu trestní odpovědnosti při řízení autonomních vozidel. Podle čl. L123-1 francouzského zákoníku o

[52] Například *Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L0680&qid=1716364190426 [cit. 2024-02-21].
[53] DUTTON, Tim. *An Overview of National AI Strategies*. Online. Medium, 2018. Dostupné z: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd [cit. 2024-02-21].
[54] METZ, Rachel. *San Francisco just banned facial-recognition technology*. Online. CNN Business, 2019. Dostupné z: https://edition.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html [cit. 2024-02-21].

silničním provozu[55] se trestní odpovědnost nevztahuje na řidiče vozidla ovládaného automatizovaným systémem řízení, pokud tento systém byl v době spáchání trestného činu aktivní. Řidič ponese trestní odpovědnost v případě, kdy nepřevezme řízení po upozornění systému, jinak se trestní odpovědnost přesouvá na výrobce vozidla, a to pouze za trestný čin usmrcení z nedbalosti nebo ublížení na zdraví z nedbalosti. Na tuto legislativu navazuje francouzský zákoník o přepravě[56] upravující podmínky pro provedení zásahu do automatizovaného systému řízení vozidla na dálku. Osoba provádějící zásah na dálku je trestně odpovědná za manévr vozidla, který byl učiněn v důsledku jejího zásahu, nebo který byl v rozporu s podmínkami použití systému. Stejně tak je osoba odpovědná, pokud opomene zásah na dálku provést, ačkoliv k tomu byla povinna (čl. L3151-5), anebo pokud osoba provádí zásah na dálku bez řidičského oprávnění (čl. L3151-6), či pod vlivem omamné látky (čl. L3151-11).

Žádné další země zatím konkrétní pravidla pro oblast UI v souvislosti s trestním právem do svých právních řádů neimplementovaly a setrvávají pouze na úrovni doporučení a nezávazných pokynů.[57]

Na poli českého práva nebyla v oblasti UI dlouhá léta vyvíjena žádná aktivita a české trestněprávní předpisy s pojmem UI, ani se souvisejícími pojmy, zatím skoro vůbec nepracují. Až v roce 2018 si Úřad vlády nechal vypracovat odbornou studii,[58] která však uvádí pouze doporučení v regulatorní oblasti trestní odpovědnosti. Klade také důraz na transparentnost systémů, aby nedocházelo ke zneužívání UI k páchání trestné činnosti. Jedním z posledních českých počinů bylo přijetí národní strategie k UI,[59] která se však soustředí spíše na ekonomické využití a v oblasti trestního práva nepřináší nic nového. Český právní řád doposud nereagoval ani na budoucnost autonomních vozidel a prozatím vychází z odpovědnostního režimu pro řidiče bez ohledu na stupeň automatizace vozidla, který však bude brzy nesporně relevantní. Ministerstvo dopravy

---

[55] *Code de la route (Version en vigueur depuis le 16 avril 2021). Dostupné z: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043371835* [cit. 2024-02-21].

[56] *Code des transports (Version en vigueur au 06 mai 2024). Dostupné z: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000023086525/LEGISCTA000043372079/#LEGISCTA000043372246* [cit. 2024-02-21].

[57] *Artificial Intelligence | Chapters*. Online. Legal 500, 2023. Dostupné z: https://www.legal500.com/guides/guide/artificial-intelligence/ [cit. 2024-05-06].

[58] FAŤUN, Martin; KUČERA, Zdeněk; KRÁL, Luboš; PĚCHOUČEK, Michal; KRAUSOVÁ, Alžběta; MATEJKA, Ján et al. *Výzkum potenciálu rozvoje umělé inteligence v České republice. Souhrnná zpráva.* Online. Úřad vlády ČR, 2018. Dostupné z: https://vlada.gov.cz/assets/evropske-zalezitosti/aktualne/AI-souhrnna-zprava-2018.pdf [cit. 2024-02-21].

[59] *Národní strategie umělé inteligence v České republice*. Online. Ministerstvo průmyslu a obchodu, 2019. Dostupné z: https://www.mpo.gov.cz/cz/podnikani/digitalni-ekonomika/umela-inteligence/ [cit. 2024-02-21].

nechalo v roce 2021 vypracovat analýzu právních předpisů týkajících se autonomní mobility,[60] která považuje současné trestněprávní předpisy do určité míry za dostačující. Obsahuje pouze doporučení právní úpravy formou doplnění některých trestných činů ve vztahu k nedbalostnímu jednání (např. trestný čin ohrožení z nedbalosti opomenutím aktualizovat kritický software), které by umožnilo stíhat trestnou činnost spojenou s provozem autonomních vozidel.

1.2.1 Akt o umělé inteligenci

Vůbec první právní regulací UI na světě má být Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (dále jako „nařízení" nebo „Akt o umělé inteligenci"),[61] ve kterém se významně promítl dosavadní přístup Evropské Unie k problematice UI zmíněný výše. Evropská Komise představila návrh legislativního rámce v roce 2021 a Evropský parlament spolu s Radou dosáhly předběžné dohody o konkrétní podobě pravidel v prosinci 2023. Zástupci členských států se začátkem února 2024 shodli na kompromisním znění. Nařízení musí ještě formálně schválit Evropský parlament, stane se tak nejspíš během roku 2024.[62] Vzhledem k tomu, že se současně jedná o první komplexní úpravu tohoto druhu na světě, má nařízení potenciál stanovit globální standard i pro ostatní světové jurisdikce. Kritici však vyčítají Evropské unii to, že podlehla tlaku velkých technologických firem a donucovacích orgánů, a nastavila laťku příliš nízko, především v oblasti použití biometrické identifikace. Regulace podle nich obsahuje plno ústupků a výjimek ze zákazů a neposkytuje tak nutnou ochranu základních práv a svobod občanů Evropské unie.[63] Význam a efektivitu Aktu o umělé inteligenci bude možné posoudit až časem, podle toho, jak bude vypadat jeho aplikace a dodržování v praxi.

„Hlavním cílem nařízení je zajistit, aby systémy UI, které jsou uváděny na evropský trh (a zde také používány) byly bezpečné, důvěryhodné, nediskriminační a v souladu se základními právy

---

[60] LOKAJ, Zdeněk; ZELINKA, Tomáš; FIALOVÁ, Eva; MATEJKA, Ján; ŠČERBA, Tomáš; STEHLÍK, Vít et al. *Návrh úpravy jednotlivých právních institutů a aspektů platných v České republice relevantních pro zavádění vozidel od stupně automatizace SAE 3 a výše do provozu a zajištění jejich provozu*. Online. Ministerstvo dopravy, 2022. Dostupné z: https://www.mdcr.cz/Uzitecne-odkazy/Autonomni-mobilita [cit. 2024-02-21].

[61] *Procedure file 2021/0106(COD) Artificial Intelligence Act*. Online. European Parliament. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/0106(COD) [cit. 2024-02-21].

[62] *EU schválila akt o umělé inteligenci. Je první svého druhu na světě*. Online. Aktuálně.cz, 2024. Dostupné z: https://zpravy.aktualne.cz/zahranici/staty-eu-definitivne-potvrdily-drive-odsouhlaseny-akt-o-umel/r~45068598174d11efb589ac1f6b220ee8/ [cit. 2024-06-01].

[63] Viz například https://corporateeurope.org/en/2023/11/big-tech-lobbying-derailing-ai-act [cit. 2024-05-1] a https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/ [cit. 2024-05-1]

a hodnotami EU. Obecně je kladen důraz na vysokou ochranu osobních údajů, lidskou kontrolu a transparentnost vůči uživatelům. Celkově je právní úprava postavena na principu posouzení rizik – čím vyšší riziko představuje použití systému UI, tím přísnější pro něj platí pravidla. Nařízení vyjmenovává v čl. 5 absolutně zakázané postupy a v čl. 6 (Příloha III) postupy s vysokým rizikem."[64] V trestněprávní rovině dopadá Akt o umělé inteligenci na technologie biometrické identifikace používané donucovacími orgány a algoritmy hodnocení a předvídání rizik recidivy. Upravuje také systémy UI v oblasti migrace, azylu a správy hraničních kontrol.

Nařízení **absolutně zakazuje** systémy UI, které donucovací orgány používají k biometrické identifikaci osob na dálku na veřejně přístupných místech „v reálném čase", tzn. že zachycení biometrického údaje, jeho porovnání a identifikace konkrétní osoby dle databáze probíhá okamžitě, nebo bez významného zpoždění. Nicméně, soud nebo nezávislý správní orgán může na základě odůvodněné žádosti udělit výjimku ze zákazu, a to v nezbytně nutných případech (i) vyhledávání pohřešovaných osob a potencionálních obětí únosu, obchodování s lidmi nebo sexuálního zneužívání, (ii) dále také v případech prevence bezprostředního ohrožení života a zdraví fyzických osob, nebo teroristických útoků, (iii) anebo při snaze lokalizovat fyzické osoby za účelem vyšetřování, trestního stíhání nebo výkonu trestu v souvislosti s vyjmenovanými trestnými činy s horní trestní sazbou nejméně 4 let jako například trestné činy vraždy, znásilnění, terorismu, nelegálního obchodu se zbraněmi, organizované nebo ozbrojené loupeže, nebo zločiny proti životnímu prostředí atd.

Tyto systémy zasahují zvláště rušivým způsobem do základních práv a svobod dotčených osob, především do práva na soukromí. Při jejich (výjimečném) použití je proto nutné dodržet všechny další podmínky a omezení vyplývající z vnitrostátní úpravy. Stejně tak je třeba zohlednit i povahu a závažnost situace, a rozsah a pravděpodobnost újmy způsobené v případě, že by systém použit nebyl. Každý takový systém musí být zároveň zaregistrován ve speciální veřejně dostupné databázi spravované Evropskou komisí. V naléhavých případech jej lze použít i bez podání odůvodněné žádosti nebo registrace, ale jen když tak bude učiněno dodatečně bez zbytečného odkladu. Nedodrží-li donucovací orgány některé z výše uvedených podmínek, používání systému musí být s okamžitou platností zastaveno a všechna data a výstupy tohoto použití vymazány. Každý členský stát si dále sám stanoví vlastní podrobná pravidla upravující celý proces a dohled nad ním.

[64] FOREJTOVÁ, Monika a ZÁRUBA, Viktor. *Kontury evropského Aktu o umělé inteligenci*. Online. Právní prostor, 2024. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/kontury-evropskeho-aktu-o-umele-inteligenci [cit. 2024-05-1].

Tím, že nařízení zakazuje použití těchto systémů pouze pro účely vymáhání práva, nepřímo povoluje soukromým subjektům, a dokonce i vládě (pro jiné účely než vymáhání práva) tímto způsobem bezmezně narušovat soukromí fyzických osob. V důsledku podmínky horní trestní sazby 4 let může také dojít k tomu, že donucovací orgány budou přeformulovávat skutečně stíhané trestné činy na trestné činy s vyšší trestní sazbou, aby dosáhly na výjimku pro použití biometrické identifikace „v reálném čase“.[65]

Zbytková kategorie systémů biometrické identifikace na dálku na veřejně přístupných místech, tj. jiné než systémy biometrické identifikace „v reálném čase“ neboli systémy „následné“ nebo „zpětné“ biometrické identifikace, spadají do vysoce rizikových postupů, ale jsou absolutně zakázané, pokud nepodléhají předchozímu povolení. Systémy biometrické identifikace „v reálném čase“ lze využít pouze k necílené identifikaci lidí na veřejně dostupných místech, zatímco systémy „zpětné“ mají sloužit k pozdější cílené identifikaci konkrétní osoby. Rozlišení mezi oběma způsoby biometrické identifikace je přesto v rámci nařízení nejasné, což umožňuje donucovacím orgánům jistou volnost při využívání této technologie. Kromě toho, osobní údaje fyzických osob budou shromažďovány bez ohledu na to, zda k nim donucovací orgány mají přístup v reálném čase, či nikoli. Otázka ochrany osobních údajů tak zůstává nařízením neupravena a bude se řídit dosavadními evropskými pravidly.

Absolutně zakázány jsou také systémy UI určené k hodnocení a předvídání rizik recidivy fyzických osob výhradně na základě jejich profilování anebo posouzení jejich osobnostních vlastností a charakteristik. Tento zákaz se však nevztahuje na systémy UI, které pouze podporují (doplňují) lidské posouzení založené na objektivních a ověřitelných skutečnostech relevantních pro konkrétní případ.

Do kategorie **vysoce rizikových** postupů se dále řadí systémy UI, které donucovací orgány používají k (a) posouzení rizika, že se fyzická osoba stane obětí trestného činu; (b) detekci lži jako jsou polygrafy a obdobné nástroje; (d) hodnocení spolehlivosti důkazů v průběhu vyšetřování nebo trestního stíhání; (e) posouzení rizika, že se fyzická osoba dopustí nebo opětovně dopustí trestné činnosti a (f) profilování fyzických osob v průběhu vyšetřování nebo trestního stíhání.[66]

---

[65] BRAVO, Maria V. *What U.S. Regulators can Learn from the EU AI Act*. EPIC, 2024. Online. Dostupné z: https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/ [cit. 2024-05-01].

[66] „Profilováním“ se rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu (definice ze *Směrnice Evropského parlamentu a Rady (EU)*

Použití těchto vysoce rizikových systémů UI donucovacími orgány vykazuje značný stupeň nerovnováhy mezi donucovacími orgány a fyzickými osobami. Může to mít negativní dopad na jejich základní práva a svobody v souvislosti se sledováním, zatčením nebo zbavením svobody, jakož i na základní procesní práva v trestním řízení (např. na účinnou právní ochranu, na spravedlivý proces, na obhajobu, presumpci neviny). Jde zejména o případy, kdy systém UI nebyl trénován na kvalitních datech, nebo kdy nesplňuje požadavky na přesnost a spolehlivost, čímž může dojít k diskriminačním výsledkům. V zájmu zabránění negativních dopadů vysoce rizikových systémů UI, na ně nařízení klade obecně přísnější požadavky, pokud jde o zřízení systému rizik; reprezentativnost a vhodnost souborů tréninkových dat a zabezpečení osobních údajů; vypracování technické dokumentace a její aktualizace; uchovávání záznamů o činnosti systému; transparentnost používaného systému; informační povinnost vůči uživatelům; umožnění lidského dohledu zaměřeného na prevenci nebo minimalizaci rizik; a spolehlivost, přesnost a kybernetickou bezpečnost s ohledem na účel, ke kterému systém slouží. Povinná je i registrace před uvedením systému do provozu.

1.3 Trestní odpovědnost

Právní odpovědnost UI obecně představuje značně diskutovaný problém mezi odbornou veřejností. Některé názory[67] se kloní k tomu, že současný právní rámec je schopný vypořádat se s otázkou trestní odpovědnost UI způsobem podobným odpovědnosti fyzických a právnických osob. Mnoho dalších autorů[68, 69] se však domnívá o opaku a tvrdí, že celkové nastavení trestní odpovědnosti se bude muset do budoucna proměnit. Jako jeden z předních argumentů používají prvek autonomního chování, který představuje schopnost systému UI samostatně fungovat a generovat vlastní kód nezávisle na původním tvůrci. Při takové míře autonomie pak tvůrce skutečně ztrácí vliv a kontrolu nad dalším jednáním systému a jen stěží lze toto chování přičíst konkrétní osobě, ať už fyzické či právnické.

2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů).

[67] HALLEVY, Gabriel. *When Robots Kill: Artificial Intelligence Under Criminal Law*. Boston: Northeastern University Press, 2013. ISBN 9781555538019.

[68] POLČÁK, Radim. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti*. Online. Bulletin advokacie, 2018. Dostupné z: http://www.bulletin-advokacie.cz/odpovednost-umele-inteligence-a-informacni-utvary-bez-pravni-osobnosti [cit. 2024-02-19].

[69] OSMANI, Nora. *The Complexity of Criminal Liability of AI Systems*. Online. Masaryk University Journal of Law and Technology, Vol. 14, No. 1, 2020. s. 75. ISSN 1802-5951. Dostupné z: https://doi.org/10.5817/MUJLT2020-1-3 [cit. 2024-02-26].

Trestní odpovědnost UI si můžeme zjednodušeně promítnout do tří modelů: **(1)** UI jako nástroj k páchání trestné činnosti (*perpetration-by-another liability model*); **(2)** selhání UI jako způsob naplnění objektivní stránky nedbalostních trestných činů (*natural-probable-consequence liability model*); a **(3)** UI jako subjekt trestního práva (*direct liability model*).[70, 71] Naznačené rozdělení modelů dokonale neodpovídá nejaktuálnějšímu vývoji UI, dobře však demonstruje problematiku ve vztahu k trestní odpovědnosti a odkrývá některé sporné otázky, které jsou v současné koncepci trestního práva v zásadě neřešitelné. Vliv UI na téma posuzování trestní, či jakékoliv jiné právní odpovědnosti se bude v budoucnu zvětšovat souběžně s vývojem sofistikovanějších systémů, které se budou blížit lidské inteligenci.

1.3.1 První model

V rámci prvního modelu vycházíme z předpokladu, že UI nemá žádné lidské atributy (příčetnost, rozumová a mravní vyspělost), tzn. hledáme trestně odpovědného pachatele, který UI používá pouze jako nástroj k jím páchané trestné činnosti. Jde tedy o způsob, jakým pachatel jedná (objektivní stránka trestného činu), a který je v kontextu trestní odpovědnosti stejně relevantní jako užití jakéhokoliv jiného nástroje například z hlediska právních následků, kdy může užití UI představovat obecně přitěžující okolnost kvůli zvláštní sofistikovanosti provedení trestného činu. UI zde vystupuje jako nevinný zprostředkovatel vůle programátora, který ji přímo vytvoří k páchání trestné činnosti, příp. uživatele, který ji k tomuto účelu zneužije.

Model pokrývá případy úmyslného zneužití i případy trestných činů nedbalostních. Při úmyslném zneužití pachatel sám ovládá UI, byť i jen k dílčím operacím (např. počítačový hacker použije software k prolomení zabezpečené databáze, ze které neoprávněně získá uživatelská data). Tyto situace se často připodobňují případům, kdy páníček (pachatel) poštve svého psa (systém UI) proti cizímu člověku (oběť trestného činu).[72] U nedbalostních trestných činů funguje UI správně, avšak k pochybení dojde při jejím neodborném použití pachatelem (např. lékař neprostuduje

[70] PROVAZNÍK, Jan a MULÁK, Jiří. Roboti za mřížemi - je české trestní právo připraveno na rozvoj umělé inteligence? In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 256-279. ISBN 9788087284957.
[71] HALLEVY, Gabriel. *The Criminal Liability of Artificial Intelligence Entities*. Online. SSRN Electronic Journal, 2010. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.1564096 [cit. 2024-02-18].
[72] Tamtéž. s. 12-15.

manuál k operačnímu robotovi, zadá mu špatný pokyn, v jehož důsledku dojde ke vzniku újmy na zdraví[73]).

1.3.2 Druhý model

Ve druhém modelu vzniká trestní odpovědnost osobě při nedbalostním zavinění selhání UI, tzn. že postihuje nežádoucí následky při použití vadně fungující UI, kterým však bylo možné předejít při zachování potřebné míry opatrnosti, zejména v důsledku nedodržení potřebných bezpečnostních norem, profesionálních standardů, nebo dalších zvláštních povinností.[74] Tento model se od prvního modelu odlišuje tím, že v něm jde výlučně o nedbalostní zavinění. Programátor nebo uživatel UI nemají v úmyslu spáchat trestný čin prostřednictvím UI (postrádají složku volní), ale zároveň se určitým způsobem podílí na její kontrole, dohledu, dozoru, nebo servisu. Nedbalostně potom jedná *„ten, kdo nedodržuje potřebnou míru opatrnosti, ke které je v rámci okolností povinen (objektivní hledisko) a podle svých možností schopen (subjektivní hledisko).“*[75] Jako objektivní hledisko se ve vztahu k UI patrně předpokládá určitý rejstřík práv a povinností, který určuje, jak UI správně užívat.

V souvislosti s tímto modelem se nejvíce diskutuje trestní odpovědnost za trestné činy v dopravě související s užíváním autonomních vozidel. Základním východiskem pro určení odpovědnosti jsou obecně uznávané standardy rozlišení vozidel do pěti, resp. šesti stupňů automatizace systémů řízení.[76] Výchozí **0. stupeň** bez jakékoliv automatizace, kdy vozidlo plně ovládá člověk (nanejvýš je vybaveno varovnými systémy, např. na námrazu vozovky); **1. stupeň** (*hands-on*) s podporou řidiče systémy, které mírně zasahují do řízení (např. udržování vozu v jízdním pruhu) s tím, že aktivní může být pouze jeden z těchto systémů; částečně automatizovaný **2. stupeň** (*hands-off*) s více něž jedním aktivním systémem podpory řidiče (např. parkovacího asistenta, který reguluje rychlost, a zároveň otáčí volantem), kdy řidič musí být ostražitý a případně schopen převzít řízení; podmíněně automatizovaný **3. stupeň** (*eyes-off)*, který za určitých podmínek provádí úkony vozidla zcela automaticky (např. jízda na rovné dálnici za

[73] PROVAZNÍK, Jan a MULÁK, Jiří. Roboti za mřížemi - je české trestní právo připraveno na rozvoj umělé inteligence? In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 262-264. ISBN 9788087284957.
[74] Tamtéž. s. 264-266.
[75] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část.* 8. aktualizované vydání. Praha: Leges, 2022. s. 244 a násl. ISBN 9788075025760.
[76] SAE International. *SAE Levels of Driving Automation™ Refined for Clarity and International Audience*. Online. SAE Blog, 2021. Dostupné z: https://www.sae.org/site/blog/sae-j3016-update [cit. 2024-02-15].

dobrých viditelnostních podmínek v režimu autopilota nebo řízení v dopravní zácpě), avšak po upozornění musí být řidič připraven převzít řízení; vysoce automatizovaný **4. stupeň** (*mind-off)* s komplexním řízením vozidla, které bezpečně zastaví, pokud řidič nereaguje na upozornění k převzetí řízení (s ojedinělými výjimkami, kdy musí vozidlo řídit sám řidič, např. při velmi špatném počasí); a nejvyšší plně automatizovaný **5. stupeň** (*steering wheel optional)*, kdy vozidlo samostatně vyřeší všechny dopravní situace a člověk je pouhým pasažérem, nebo nemusí být ve vozidle vůbec přítomen. Dnes je možné se setkat s autonomními vozy 3. stupně v Německu (např. Mercedes-Benz, BMW)[77] a v Japonsku, kde se začalo s vymezováním speciálních pásem pro osobní i nákladní automobily 4. stupně.[78]

Podle českého právního pojetí nebude u řidiče vozidla 5. stupně připadat do úvahy trestní odpovědnost s výjimkou nedbalostního spáchání trestného činu, kdy řidič poruší zvláštní povinnost konat.[79] Odpovědnost se tedy ve většině případů přesune buď na výrobce, nebo provozovatele vozidla, jelikož odpovídají za fungování automatizovaných funkcí systému řízení. V případě 4. a 3. stupně bude řidič trestně odpovědný, pokud bude na základě upozornění systémem vozidla povinen k převzetí řízení, nebo to bude vyplývat ze zřejmých okolností. Vždy však bude nutné zkoumat konkrétní okolnosti (technická úroveň vybavení vozidla) a možnosti řidiče vyvarovat se dopravní nehodě (přiměřená reakční doba řidiče). Pro řidiče vozidel 2. a 1. stupně se uplatní stejná odpovědnost jako u klasických neautomatizovaných vozidel.[80] Pokud se vyskytne vícero trestně odpovědných osob najednou, odpovídá každá zvlášť za „svou“ nedbalost, a tak u dopravní nehody způsobené autonomním vozidlem může být souběžně odpovědný řidič vozidla, výrobce automobilu anebo dodavatel hardwarového a softwarového příslušenství.[81]

V souvislosti s trestní odpovědností při řízení autonomních vozidel musíme věnovat pozornost také otázce jednání fyzické osoby. Při „řízení“ autonomních vozidel si lze jednání schopné založit trestněprávní důsledky představit jak ve formě konání (např. záměrná aktivace

[77] POULTNEY, Leon. *BMW matches Mercedes-Benz with huge autonomous driving upgrade for 7 Series*. Online. TechRadar, 2023. Dostupné z: https://www.techradar.com/vehicle-tech/hybrid-electric-vehicles/bmw-matches-mercedes-benz-with-huge-autonomous-driving-upgrade-for-7-series [cit. 2024-02-15].
[78] HIROSAWA, Mayumi. *Japan to assign bandwidth for Level 4 self-driving vehicles*. Online. NikkeiAsia, 2023. Dostupné z: https://asia.nikkei.com/Business/Technology/Japan-to-assign-bandwidth-for-Level-4-self-driving-vehicles [cit. 2024-02-15].
[79] Například když si řidič všimne vady v softwaru vozidla, ale přesto jej nadále používá, poruší tím povinnost udržovat vozidlo v řádném technickém stavu podle pokynů pro obsluhu a údržbu stanovených výrobcem dle § 36 Zákona o podmínkách provozu vozidel na pozemních komunikacích.
[80] ŠELLENG, Dalibor. Autonomní vozidla – vybrané otázky vzniku trestní odpovědnosti. In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 294-304. ISBN 9788087284957.
[81] Tamtéž. s. 294-304.

autonomního systému řidičem v situaci, u které je použití vyloučeno výrobcem, načež dojde k dopravní nehodě), tak ve formě opomenutí (např. nepřevzetí kontroly nad řízením po upozornění systému). U opomenutí je navíc vždy nutné zkoumat, zda došlo k porušení zvláštní povinnosti podle § 112 trestního zákoníku.

Od povolení provozu autonomních vozidel ve veřejné dopravě některých zemí evidujeme případy dopravních nehod v souvislosti s automatizovaným řízením. K jedné z těch prvních došlo v roce 2018, kdy vozidlo v testovacím režimu (Volvo, 2. stupeň automatizace) srazilo a usmrtilo chodkyni, která vešla do vozovky v Arizoně. Vůz ji zaregistroval několik vteřin před srážkou, ale systém nouzového brždění se neaktivoval správně v důsledku vady na vozidle. Zavinění však bylo na straně řidičky, která, pokud by se dostatečně věnovala dění na komunikaci, mohla nehodě zabránit. Soud kvalifikoval skutek jako usmrcení z nedbalosti a řidičku odsoudil k podmíněnému trestu odnětí svobody s dohledem ve výši tří let.[82] Obvinění z obecného ohrožení bylo také sděleno řidiči, který spal při jízdě po dálnici v Kanadě (Tesla Model S, 2. stupeň automatizace).[83]

1.3.3 Třetí model

V režimu třetího modelu je trestně odpovědná samotná UI. Jedná se o (prozatím) hypotetickou představu, která nepředpokládá odpovědnost žádné jiné osoby, ale přímo konkrétního systému UI.[84] Základním východiskem je předpoklad a přiznání právní subjektivity systémům UI a vytvoření již zmiňované nové „elektronické“ právní osoby. Od fyzické osoby by se odlišovala umělým vytvořením a absencí kvalit lidské bytosti. Zároveň by byla schopna vlastním jednáním fakticky zavázat sebe sama k právům a povinnostem, na rozdíl od právnické osoby, za kterou vždy musí jednat osoba fyzická. Otázka vzniku a zániku by mohla být řešena zápisem do speciálního rejstříku systémů UI, podobně jako tomu je u právnických osob.

Přiznáním subjektivity sice umožníme formálně vyvodit trestní odpovědnost UI, ale otevřeme s tím i mnoho problematických otázek. Vzhledem k tomu, že by systém UI v tomto scénáři byl samostatným subjektem práva, mohl by na páchání trestné činnosti spolupracovat

[82] *Backup driver for self-driving Uber that killed Arizona pedestrian pleads guilty*. Online. The Guardian, 2023. Dostupné z: https://www.theguardian.com/technology/2023/aug/01/uber-self-driving-arizona-deadly-crash [cit. 2024-02-16].
[83] *Canada Tesla driver charged over 'napping while speeding'*. Online. BBC News, 2020. Dostupné z: https://www.bbc.com/news/world-us-canada-54197344 [cit. 2024-02-16].
[84] HALLEVY, Gabriel. *The Criminal Liability of Artificial Intelligence Entities*. Online. SSRN Electronic Journal, 2010. s. 21-31. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.1564096 [cit. 2024-02-18].

s člověkem, nebo dokonce s jiným systémem UI. Jak se potom bude řešit otázka spolupachatelství a dalších forem účastenství tak, aby všechny strany zapojené do trestné činnosti nesly odpovědnost na základě svých rolí? Stejně nejasné je, jaké formy trestů bychom systémům UI ukládali, což je naprosto zásadní problém pro řešení jejich trestní odpovědnosti. Rovněž chybí předpoklad koherentní identity systémů UI, jelikož mohou být kdykoliv restartovány, aktualizovány, nebo přeprogramovány, čímž by ukládání některých trestů zcela ztratilo smysl. Pokud bude UI schopna účinné lítosti nebo doznání, bude to mít určitý vliv i na instituty umožňující zmírnění trestů.

V návaznosti na otázku subjektu by bylo nezbytné pojmenovat i ostatní obecné znaky trestného činu – objekt, resp. výčet trestných činů, kterých se UI může, nebo nemůže dopustit, příp. konstituování trestných činů zcela nových; objektivní stránku neboli schopnost UI mít vlastní vůli (ne pouze replikovat vůli někoho jiného[85]), a tu posléze projevit ve vnějším světě; a subjektivní stránku (zavinění), která by závisela na tom, jestli bude UI vybavena všemi psychickými a emocionálními vnitřními procesy relevantními pro trestní právo (složka rozumová i volní, vnitřní ustálený hodnotový systém, morální referenční rámec atd.), a tudíž i schopna vytvořit si vnitřní psychický vztah ke skutečnostem, které zakládají trestný čin.[86] Model tak vylučuje situace, kdy by za protiprávní jednání UI, na které nemá fyzická ani právnická osoba žádný vliv, nebyl nikdo trestně odpovědný (např. srážka plně autonomního vozidla s běžným vozidlem, ke které došlo v důsledku vjezdu plně autonomního vozidla do křižovatky na červenou barvu semaforu).[87]

1.3.4 Koordinace modelů

Tři výše popsané modely trestní odpovědnosti nejsou výhradně alternativní a vzájemně se nevylučují. Lze je použít kombinovaně za účelem vytvoření úplného obrazu trestní odpovědnosti ve specifickém kontextu zapojení UI do páchání trestné činnosti.

Nepochybně by vždy měla existovat konkrétní fyzická nebo právnická osoba, která UI vyvinula, nebo ji spravuje, a která by měla nést odpovědnost za její protiprávní jednání. Problém

[85] KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. s. 23. ISBN 9788075987839.
[86] PROVAZNÍK, Jan a MULÁK, Jiří. Roboti za mřížemi - je české trestní právo připraveno na rozvoj umělé inteligence? In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 266-270. ISBN 9788087284957.
[87] BECK, Susanne. Legal Responsibility in the Case of Robotics. Online. In: KARAFILLIDIS, Athanasios a WEIDNER, Robert (ed.). *Developing Support Technologies. Biosystems & Biorobotics*. Online. Springer International Publishing, 2018. s. 265. Dostupné z: https://doi.org/10.1007/978-3-030-01836-8_26 [cit. 2024-02-19].

však může nastat při větvení systémů, kdy UI sama naprogramuje jinou UI a ta spáchá trestný čin. Bude se patrně jednat o použití UI jako nástroje. Programátorem tak bude samotná UI a aplikuje se na ní první model ve spojení s modelem třetím, tudíž původní vývojář, nebo správce UI nebude v této situaci trestně odpovědný. Komplikovaná bude i situace, kdy UI spáchá trestný čin jako vedlejší důsledek její legální činnosti. Programátor UI bude trestně odpovědný z nedbalosti podle prvního modelu, pokud měl od počátku v úmyslu spáchat jiný trestný čin. Pokud ovšem žádný trestný čin předem neplánoval, bude v této situaci odpovídat za nedbalostní zavinění selhání UI podle druhého modelu. Znovu také platí, že jestliže je programátorem samotná UI, použije se přirozeně (ve spojení s ostatními) i třetí model trestní odpovědnosti.[88]

1.4 Nové podoby trestné činnosti

Zatímco tradiční kriminalita v západních zemích postupně klesá, u počítačové kriminality (kyberkriminality) naopak dochází k jejímu exponenciálnímu růstu.[89] To není vůbec překvapivé, jelikož šance na dopadení kyberzločince jsou mnohem nižší, než u pachatele tradiční kriminality a zisk z kyberzločinů může být, ve srovnání s „offline kriminalitou“, několikanásobně vyšší, a tudíž pro pachatele lákavější. Navíc značná část majetku je dnes typicky obsažena v nehmotných statcích. Europol za rok 2023 evidoval obrovský nárůst online podvodníků, kteří zneužívají například Ruské invaze na Ukrajinu a vytvářejí falešné domény humanitárních organizací, rozesílají emaily předstírající získání finančních prostředků na humanitární úsilí, nebo se vydávají za celebrity, které vedly nebo podporovaly skutečné kampaně.[90] Prostřednictvím virtuálních tržišť na *darkwebu*[91] se do virtuálního prostoru přesunula také tradiční trestná činnost, zejména organizovaný zločin obchodu s drogami, zbraněmi a lidmi, nebo šíření dětské pornografie.

V kyberprostoru tak UI hraje čím dál tím větší roli jako nástroj[92] používaný pachateli k *hackingu*, *stalkingu*, či pokročilých technik podvodů. Systémy UI pachatelům umožňují hromadné útoky s nižší časovou i technickou náročností. Součet způsobených škod tak může dosahovat

[88] HALLEVY, Gabriel. *The Criminal Liability of Artificial Intelligence Entities*. Online. SSRN Electronic Journal, 2010. s. 31-33. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.1564096 [cit. 2024-02-18].
[89] Viz například https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime [cit. 2024-04-26] nebo https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-kyberneticka-kriminalita-je-v-cesku-na-vzestupu-pomohl-tomu-i-covid-40446871 [cit. 2024-04-26].
[90] *Internet Organised Crime Threat Assessment (IOCTA)*. Online. Publications Office of the European Union, 2023. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023 [cit. 2024-04-26].
[91] Část internetu, která nebyla indexována vyhledávači a je přístupná pouze se speciálním softwarem.
[92] Použití se pohybuje v rámci prvního modelu trestní odpovědnosti UI popsaného v kapitole 1.3.1.

obrovského rozsahu. Jeden z prvních případů zneužití UI k páchání trestné činnosti vedl ke škodě až bilion dolarů, když indický burzovní makléř způsobil nečekaný propad na amerických finančních trzích pomocí tzv. *spoofingových* algoritmů, kterými uměle manipuloval s akciemi.[93] Používání těchto algoritmů k obchodování na trzích s finančními nástroji je nyní regulováno i na úrovni Evropské unie nařízením[94] a evropská úprava dokonce zavedla požadavek pro *compliance* pracovníky, aby alespoň obecně rozuměli fungování obchodních a investičních algoritmů.

Zneužití UI představuje vysoké bezpečnostní riziko. V praxi jsme se mohli setkat se sabotáží celých struktur systémů kybernetickými útoky na kritické instituce jako jsou třeba nemocnice.[95] Pachatelé mohou využít UI i k manipulaci nemocničních dat (např. 3D lékařských skenů) a takto kompromitovat zdravotnické infrastruktury.[96] Varovnou ukázkou budiž také úspěšný čínský pokus o zmatení autopilota automobilu Tesla Model S k vjetí do protisměru za pomoci papírových štítků na vozovce,[97] stejně tak ošálení systémů rozpoznávání obličejů[98] nebo kompletní přeprogramování systému UI k zcela jiné činnosti.[99] Dalším možným zneužitím UI pachateli může být přeprava nelegálního nákladu. S rozvojem autonomních dopravních prostředků, které se sami dokáží v případě potřeby vyhnout policejním hlídkám, poslat signál operátorovi při úspěšném doručení nákladu, nebo při odhalení zničit usvědčující důkazy (nebo sebe sama), se přeprava jakéhokoliv nelegálního nákladu a osob (za účelem obchodování s lidmi) stává pro pachatele snadněji proveditelnou a méně riskantní. Naopak pro policejní orgány je složitější tuto trestnou činnost odhalovat.[100]

---

[93] CHATURVEDI, Amit. *Navinder Singh Sarao: How This Indian Trader Wiped Off $1 Trillion From US Market*. Online. NDTV, 2024. Dostupné z: https://www.ndtv.com/feature/navinder-singh-sarao-how-this-indian-trader-wiped-off-1-trillion-from-us-market-5062729 [cit. 2024-04-26].

[94] *Nařízením Komise v přenesené pravomoci (EU) 2017/589 ze dne 19. července 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/65/EU, pokud jde o regulační technické normy upřesňující organizační požadavky na investiční podniky zabývající se algoritmickým obchodováním*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2017.087.01.0417.01.CES [cit. 2024-04-26].

[95] Viz například https://ct24.ceskatelevize.cz/clanek/regiony/pristroje-stale-nefunguji-benesovska-nemocnice-kvuli-kryptoviru-omezi-provoz-i-v-pondeli-56462 [cit. 2024-04-26].

[96] MIRSKY, Yisroel; MAHLER, Tom; SHELEF, Ilan a ELOVICI Yuval. *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. Online. 28th USENIX Security Symposium, 2019. ISBN 9781939133069. Dostupné z: https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky [cit. 2024-04-26].

[97] *Experimental Security Research of Tesla Autopilot*. Online. Ars Electronica, 2019. Dostupné z: https://ars.electronica.art/center/en/experimental-security-research-of-tesla-autopilot/ [cit. 2024-04-26].

[98] KOMKOV, Stepan a PETIUSHKO, Aleksandr. *AdvHat: Real-World Adversarial Attack on ArcFace Face ID System*. Online. In: 2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021. s. 819-826. ISBN 9781728188089. Dostupné z: https://doi.org/10.1109/ICPR48806.2021.9412236 [cit. 2024-04-26].

[99] ELSAYED, Gamaleldin F; GOODFELLOW, Ian; SOHL-DICKSTEIN, Jascha. *Adversarial Reprogramming of Neural Networks*. Online. Cornell University, 2018. Dostupné z: https://doi.org/10.48550/arXiv.1806.11146 [cit. 2024-04-26].

[100] SHARKEY, Noel; GOODMAN, Marc a ROS, Nick. The Coming Robot Crime Wave. Online. Computer. 2010, Vol. 43, No. 8. ISSN 0018-9162. Dostupné z: https://doi.org/10.1109/MC.2010.242 [cit. 2024-04-26].

Většina technologií UI zneužívaných k páchání trestné činnosti je založena na dolování dat (*data mining*) a strojovém učení (*machine learning*) a zaměřuje se na rozpoznávání vzorců, které jsou následně použity k personalizovaným útokům vytvořených na míru obětím.[101] Mezi nejrozšířenější techniky patří tzv. A/B optimalizace, která se zakládá na automatizovaném testování více verzí webové stránky nebo aplikace na uživatelích. Cílem je určit, která z verzí funguje u uživatelů nejlépe (v jaké se uživatel nejdéle zdrží, v jaké klikne na reklamu, nebo si něco koupí apod.). Pachatelé využívají A/B optimalizační techniky ke zvýšení efektivity svých podvodných aktivit nebo kybernetických útoků jako je *phishing* (např. k získání podrobnosti o bankovním účtu svých obětí), *ransomware* (např. k zamknutí počítače nebo soubory svých obětí a požadovaní výkupného) nebo podvody přes komunikační aplikace (např. ve snaze přesvědčit své oběti, aby převedly peníze příteli v nouzi). Ve všech případech se snaží přesvědčit oběť, aby klikla na odkaz nebo přílohu, která nainstaluje škodlivý počítačový program, nebo která přímo převede peníze z účtu oběti na účet pachatele. Testováním různých verzí svých podvodných technik mohou pachatelé identifikovat nejúspěšnější postup oklamání svých cílových obětí. Falešné obrazovky tak vypadají stále reálněji a rozlišování toho, co je skutečné, je pro laickou veřejnost téměř nemožné.[102] Stejně jako techniky A/B optimalizace zvyšují věrohodnost a přesvědčivost podvodných emailů i jazykové modely UI, které se automaticky učí kombinovat nejefektivnější funkce z různých kyberútoků a jsou natolik sofistikované, že úspěšně obelstí i spamové filtry nevyžádané pošty.[103]

Pachatelé využívají také techniku algoritmického profilování, která jim pomáhá identifikovat charakteristiky a preference lidí. Tyto informace lze využít k přesvědčení oběti podobně jako u předešlých technik, ale také k výběru toho, kteří jednotlivci a skupiny lidí jsou vůči kyberútokům nejzranitelnější. Na rozdíl od A/B optimalizace, algoritmické profilování vyžaduje zpracování osobních údajů, většinou prostřednictvím souborů *cookies* a jiných online *trackerů*. Pachatelé sesbíraná osobní data využívají k různým variacím podvodů jako je tzv. *CEO fraud*, ve kterém pachatel odešle falešný příkaz finančnímu oddělení společnosti jménem jejího generálního (nebo finančního) ředitele k převodu peněz na účet pachatele, nebo tzv. *WhatsApp*

[101] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 2. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-04-26].
[102] Tamtéž. s. 3.
[103] BAHNSEN, Alejandro C; TORROLEDO, Ivan; CAMACHO, Luis D; a VILLEGAS, Sergio. *DeepPhish: Simulating Malicious AI*. Online. Computer Science, 2018. Dostupné z: https://www.semanticscholar.org/paper/DeepPhish-%3A-Simulating-Malicious-AI-Bahnsen-Torroledo/ae99765d48ab80fe3e221f2eedec719af80b93f9#citing-papers [cit. 2024-04-26].

fraud, kdy se pachatel vydává za přítele nebo člena rodiny a předstírá finanční nouzi ve snaze vylákat peníze.[104]

1.4.1 *Deepfake*

Největším bezpečnostním rizikem blízké budoucnosti je technologie *deepfake*. Jak už bylo řečeno s postupným vývojem UI je čím dál tím těžší (nejen) pro laickou veřejnost rozeznat uměle vytvořené výtvory od reality.[105] *Deepfake* jsou obvykle vytvářeny pomocí hlubokého učení (odtud první část slova *deep*) a umožňují vytvářet falzifikáty (odtud druhá část slova *fake*). Jde o realistickou úpravu zvukových nahrávek, obrázků a videí, především přetváření rysů v tváři zobrazovaných osob (např. velmi věrohodná změna jejich mimiky, i samotné řeči). Dále lze také uměle dosadit obličej jednotlivých aktérů na videu za jiný, či vygenerovat vysoce realistické záběry existujících i neexistujících osob a přivádět již zesnulé osoby zpět k životu.

Podle Europolu[106] *deepfake* technologie významně usnadňují páchání trestné činnosti jako je obtěžování jednotlivců na internetu, falšování online identit a padělání nebo manipulace s elektronickými důkazy (např. falešné video, na kterém podezřelý páchá trestnou činnost může vést policejní orgány k pronásledování nesprávné osoby, což skutečnému pachateli umožní utéct[107]). Potenciálně nejnebezpečnějším zneužitím *deepfake* videí je šíření dezinformací a manipulace s veřejným míněním, které může mít zásadní dopad i na průběh demokratických voleb (např. tím, že pachatelé budou kandidátům vkládat do úst slova a věty, které však nikdy nevyřkli). Vytvoření zavádějících sdělení *deepfake* formou mohou být také zneužity k podpoře narativů extrémistických skupin a podněcování terorismu. Dalším závažným zneužitím je tvorba pornografických obrázků, či videí bez souhlasu dotyčné osoby.[108] Tato technologie „svléká“

[104] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 6. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-04-26].
[105] JODKA, Sara H. *Manipulating reality: the intersection of deepfakes and the law*. Online. Reuters, 2024. Dostupné z: https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01/ [cit. 2024-04-27].
[106] RIEHLE, Cornelia. *Europol Report Criminal Use of Deepfake Technology*. Online. eucrim, 2022. Dostupné z: https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/ [cit. 2024-04-27].
[107] Europol. *Facing reality? – Law enforcement and the challenge of deepfakes – An observatory report from the Europol innovation lab*. Online. Publications Office of the European Union, 2024. s. 14. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/06099c52-dc33-11ee-b9d9-01aa75ed71a1/language-en [cit. 2024-04-27].
[108] SCOTT, Daniella. *Deepfake Porn Nearly Ruined My Life*. Online. ELLE, 2020. Dostupné z: https://www.elle.com/uk/life-and-culture/a30748079/deepfake-porn/ [cit. 2024-04-27].

vybrané jednotlivce (převážně celebrity, ale objevuje se také ve virtuální dětské pornografii) a spojuje existující záběry s pornografickými obrázky v jedno.

S případem podvodných *deepfake* videí se setkala už i česká policie. Byli na nich vyobrazováni politici nabádající k investicím prostřednictvím aplikace, kterou si oběť musí stáhnout do počítače. Ve skutečnosti se však jednalo o program, který umožňuje vzdálený přístup k počítači a s jehož pomocí se pachatel dostal do internetového bankovnictví oběti. Ve věci byly zahájeny úkony trestního řízení pro podezření ze spáchání trestných činů podvodu a neoprávněného opatření, padělání a pozměnění platebního prostředku.[109] U *deepfake* výtvorů, které se rozšíří po sítích, je však velmi složité dopátrat se původního pachatele. Proto je třeba apelovat na to, aby si lidé vždy důkladně ověřovali pravost informací a nevěřili všemu, co vidí na internetu.

Ve Velká Británii bude vytvoření sexuálně motivovaného *deepfake* bez souhlasu zobrazované osoby nově považováno za trestný čin.[110] Můžeme téměř s jistotou očekávat, že něco podobného se odehraje i v dalších zemích, které budou Velkou Británii následovat. Poslanecká sněmovna ČR momentálně projednává návrh novely trestního zákoníku, který podalo Ministerstvo spravedlnosti v návaznosti na připravovanou unijní úpravu. Novela by zakotvila nový trestný čin „Zneužití identity k výrobě pornografie a její šíření“ jako nástroj trestního práva k potírání této trestné činnosti u nás.[111] Podle nového § 191a trestního zákoníku *„ten, kdo vyrobí, nebo rozšíří pornografické dílo, které zobrazuje nebo jinak využívá osobu, která k takovému zobrazení nebo využití nedala souhlas, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“* Z důvodové zprávy k návrhu zákona vyplývá, že doteď bylo možné v podobných případech uvažovat o naplnění skutkové podstaty trestného činu poškození cizích práv (§ 181 trestního zákoníku) nebo trestného činu pomluvy (§ 184 trestního zákoníku). Ovšem na problematiku nekonsenzuální *deepfake* pornografie tyto trestné činy nedopadají přímo, jelikož chrání jiný objekt trestního práva. Očekává se, že novela tento nedostatek trestněprávní úpravy zacelí.

---

[109] SKOUPILOVÁ, Ivana. *Umělá inteligence už okrádá důvěřivce*. Online. Policie České republiky – KŘP Olomouckého kraje, 2024. Dostupné z: https://www.policie.cz/clanek/umela-inteligence-uz-okrada-duverivce.aspx [cit. 2024-01-05].

[110] COONEY, Christy. *Creating sexually explicit deepfakes to become a criminal offence*. Online. BBC News, 2024. Dostupné z: https://www.bbc.com/news/uk-68823042 [cit. 2024-02-22].

[111] KRÁL, Petr. *Dopad deepfake pornografie má řešit soud. Satira a vtip ale nemají za cíl poškodit, upozorňuje náměstek*. iROZHLAS, 2024. Dostupné z: https://www.irozhlas.cz/zpravy-domov/dopad-deepfake-pornografie-ma-resit-soud-satira-a-vtip-ale-nemaji-za-cil_2404082223_tkz [cit. 2024-05-22].

1.5 Vliv na rozhodování v trestním řízení

Hlavním důvodem pro uplatnění UI v justici je snaha o zefektivnění činnosti soudů (např. vyhledávání v soudních databázích, anonymizace rozsudků, či vydávání platebních rozkazů) a zajištění objektivního rozhodování bez předsudků a zaujatosti, někdy nazýváno jako „matematická spravedlnost“ (*actuarial justice*). Do soudní soustavy ji už začlenily některé státy, zejména Čína, Spojené státy, Kanada, Austrálie, Velká Británie a v menší míře i několik dalších zemí včetně Nizozemska, Francie, Maďarska, Finska a Estonska.[112, 113] České soudnictví za ostatními státy zaostává ve využití digitálních technologií celkově, a tím pádem i v oblasti UI. Ministerstvo spravedlnosti za účelem implementace UI do českého soudnictví vytvořilo Expertní pracovní skupinu pro právní aspekty umělé inteligence.[114]

Praktickým využitím UI s největším dopadem do trestního řízení je hodnocení rizikovosti pachatele s ohledem na pravděpodobnost recidivy pomocí speciálního algoritmu. Dochází v něm ke kategorizaci pachatele na základě psychologických rysů vyvozených z předchozího chování a dalších (ne)biometrických údajů o jeho osobě jako je například věk, bydliště a vzdělání. Podle těchto údajů algoritmus sestaví profil pachatele, který má předpovědět jeho budoucí kriminogenní chování.[115] Vyhodnocení profilu následně slouží jako pomůcka k rozhodnutí v trestním řízení hlavně pro stanovení délky trestu odnětí svobody, či k rozhodnutí o podmíněném propuštění, resp. setrvání ve výkonu trestu odnětí svobody.

Použití algoritmu pro prediktivní analýzu přináší systematický a konzistentní přístup k hodnocení pachatelů, které má pomoci soudcům k informovanějšímu rozhodování a efektivnějšímu vyhodnocování rizika recidivy.[116] Přesná prognóza budoucího kriminálního

[112] TERZIDO, Kalliopi. *The Use of Artificial Intelligence in the Judiciary and its Compliance with the Right to a Fair Trial*. Online. 31 Journal of Judicial Administration 154, 2022. Dostupné z: https://ssrn.com/abstract=4495715 [cit. 2024-02-22].
[113] *Předsedové nejvyšších soudů řešili umělou inteligenci. V justici se uplatní třeba při anonymizaci*. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/11/predsedove-nejvyssich-soudu-resili-umelou-inteligenci-v-justici-se-uplatni-treba-pri-anonymizaci/ [cit. 2024-02-22].
[114] PASEKOVÁ, Eva. *ČR v justici málo využívá umělou inteligenci či práci z domova, říká zpráva EK*. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/06/cr-v-justici-malo-vyuziva-umelou-inteligenci-ci-praci-z-domova-rika-zprava-ek/ [cit. 2024-02-22].
[115] FIALOVÁ, Eva. *Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva*. Online. Časopis pro právní vědu a praxi, roč. 26, č. 2, 2018. s. 230-231. ISSN 1805-2789. Dostupné z: https://doi.org/10.5817/CPVP2018-2-3 [cit. 2024-02-23].
[116] HANNAH-MOFFAT, Kelly. *Actuarial Sentencing: An "Unsettled" Proposition*. Online. Justice Quarterly Vol. 30, No. 2, 2013. s. 271. ISSN 0741-8825. Dostupné z: https://doi.org/10.1080/07418825.2012.682603 [cit. 2024-02-23].

chování může pomoci soudním orgánům připravit lepší opatření a strategii dohledu pro vysoce rizikové jednotlivce.[117] Algoritmus je také oproštěn od emocionálních vlivů, což může v závislosti na kontextu případu představovat pro účastníka trestního řízení jak výhodu, tak i nevýhodu.

Skutečnost, že v řízení je používán algoritmus bývá osobám, o nichž se rozhoduje, často skryta, popř. tyto osoby vůbec netuší, podle jakých kritérií je algoritmus hodnotí, tzn. že použití v trestním řízení není transparentní a osoby se proti němu nemohou bránit. Současně ani samotní soudci leckdy nevědí, jak algoritmus funguje, a tudíž nepoznají, jestli třeba není vadný.[118] Algoritmy jsou také zranitelné po technické stránce (poruchy systému, kybernetické útoky, narušení ochrany osobních dat), což může ohrozit integritu a spolehlivost soudních procesů.[119]

Další problém se týká odpovědnosti za rozhodnutí provedené algoritmem. Soudci by se mohli chtít raději tomuto rozhodnutí podřídit ve snaze vyhnout se odpovědnosti při odchýlení od rozhodnutí, které bylo vygenerované algoritmem.[120] Umocnění tíhy odpovědnosti pro soudce představuje také povinnost odůvodnit odlišné rozhodnutí.[121] Soudce může být v pokušení měnit vstupní hodnoty o pachatelích tak, aby dosáhl algoritmem preferovaného výsledku a vyhnul se tak povinnosti vypracovávat sáhodlouhé odůvodnění. Tímto se naruší celý systém algoritmického rozhodování a v případě propojení algoritmů v rámci jednotlivých soudů budou tyto vyfabulované výsledky následně doporučovány i všem ostatním soudcům.[122]

Při algoritmickém rozhodování rovněž chybí prostor pro vlastní uvážení soudce o okolnostech jednotlivých případů, neboť některé algoritmy pracují jen s předdefinovanými hodnotami. Individuální aspekty případu, které nelze přiřadit pod některou z předem definovaných

[117] BARNES, Geoffrey C. a M. HYATT, Jordan. *Classifying Adult Probationers by Forecasting Future Offending*. Online. Office of Justice Programs, 2012. s. 10. Dostupné z: https://www.ojp.gov/ncjrs/virtual-library/abstracts/classifying-adult-probationers-forecasting-future-offending [cit. 2024-02-23].
[118] HANNAH-MOFFAT, Kelly. *Actuarial Sentencing: An "Unsettled" Proposition*. Online. Justice Quarterly Vol. 30, No. 2, 2013. s. 278. ISSN 0741-8825. Dostupné z: https://doi.org/10.1080/07418825.2012.682603 [cit. 2024-02-23].
[119] TERZIDO, Kalliopi. *The Use of Artificial Intelligence in the Judiciary and its Compliance with the Right to a Fair Trial*. Online. 31 Journal of Judicial Administration 154, 2022. s. 155. Dostupné z: https://ssrn.com/abstract=4495715 [cit. 2024-02-22].
[120] FIALOVÁ, Eva. *Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva*. Online. Časopis pro právní vědu a praxi, roč. 26, č. 2, 2018. s. 236. ISSN 1805-2789. Dostupné z: https://doi.org/10.5817/CPVP2018-2-3 [cit. 2024-02-23].
[121] Například povinnost v rámci Federálního posouzení rizika v době po odsouzení (*Federal Post Conviction Risk Assessment*) ve Spojených státech
[122] HANNAH-MOFFAT, Kelly. *Actuarial Sentencing: An "Unsettled" Proposition*. Online. Justice Quarterly Vol. 30, No. 2, 2013. s. 285. ISSN 0741-8825. Dostupné z: https://doi.org/10.1080/07418825.2012.682603 [cit. 2024-02-23].

kategorií, jsou tak při rozhodování opomenuty.[123, 124] Nepřímým důsledkem může být i ztráta důvěry v samotný lidský úsudek a upnutí se k mechanickému rozhodování do té míry, že funkce soudce nebude v trestním řízení zapotřebí.[125] Vytratí se tak lidský prvek, o kterém by se dalo uvažovat jako o důležité součásti práva na spravedlivý proces.[126] Algoritmus navíc musí být dostatečně aktuální v době rozhodování, aby mohl reagovat na posuzované okolnosti, které se mohou v průběhu trestního řízení měnit. Algoritmy k posouzení rizikovosti recidivy nemusí pracovat jen s předdefinovanými hodnotami, ale mohou se učit posuzovat jednotlivé případy na základě předešlých statistických dat. Problém nastane v případě, kdy některé skutečnosti začne algoritmus upřednostňovat, nebo jiné zase nezohlední vůbec, přestože by byly pro rozhodnutí relevantní.

Je důležité poznamenat, že algoritmické prediktivní analýzy mohou vykazovat nežádoucí zkreslení výsledků, pokud jde o skupinovou spravedlnost,[127] v důsledku čehož se mnohdy dostávají do rozporu se zásadami trestního řízení, zejména se zákazem diskriminace a právem na spravedlivý proces. Matematické metody v trestním řízení pracují většinou se statistickými předpověďmi o kriminalitě skupin (nebo skupinových znaků), a podle toho určují výsledky trestního řízení pro konkrétního jednotlivce. Soudci pak mohou získat nepřesnou představu o tom, že oprávněně trestají členy určité skupiny, protože tato skupina páchá trestnou činnost statisticky více než skupiny jiné. Fakticky jde pouze o zesílení již zakořeněných společenských předsudků vůči určité kategorií lidí, které se projevují v datech, ale které algoritmus sám nevytvořil. V důsledku toho je pro pachatele návrat do normálního života obtížnější, protože ztratí motivaci ke změně chování po propuštění,[128] což paradoxně vede ke zvýšené pravděpodobnosti opakování trestné činnosti.[129]

---

[123] Nemožnost přihlédnout k těmto okolnostem porušuje zákonná pravidla pro ukládání trestů (§ 39 trestního zákoníku), upuštění od potrestání (§ 46 trestního zákoníku) a podmíněné propuštění (§ 88 trestního zákoníku), nebo také zásadu volného hodnocení důkazů (§ 2 odst. 6 trestního řádu).

[124] FIALOVÁ, Eva. *Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva*. Online. Časopis pro právní vědu a praxi, roč. 26, č. 2, 2018. s. 232. ISSN 1805-2789. Dostupné z: https://doi.org/10.5817/CPVP2018-2-3 [cit. 2024-02-23].

[125]

[126] Tamtéž s. 258.

[127] MIRON, Marius; TOLAN, Songül; GÓMEZ, Emilia a CASTILLO, Carlos. *Evaluating causes of algorithmic bias in juvenile criminal recidivism*. Online. Artificial Intelligence and Law, Vol. 29, 2021. s. 138. ISSN 0924-8463. Dostupné z: https://doi.org/10.1007/s10506-020-09268-y [cit. 2024-02-23].

[128] Tamtéž. s. 258.

[129] HARCOURT, Bernard E. *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age*. Online. SSRN Electronic Journal, 2005. s. 33-36. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.756945 [cit. 2024-02-23].

Ke zkreslení při algoritmickém rozhodování může dojít dvojím způsobem. Výsledek může být buď **falešně pozitivní** (pachatel je označen za jedince s vysokým rizikem recidivy, v budoucnu však žádný trestný čin nespáchá), nebo **falešně negativní** (pachatel je nesprávně označen jako osoba s nízkým rizikem recidivy, ačkoli se v blízké době znovu dopustí trestného činu).[130] Čím více se algoritmus spoléhá na **statistické prvky**, zejména demografické a sociálně ekonomické faktory, tím méně je vůči určitým pachatelům spravedlivý, jelikož tyto prvky pachatel nemůže nijak ovlivnit. Naproti tomu **dynamické prvky** (např. snaha o napravení protiprávního stavu, užívání návykových látek, sociální vyloučení), které pachatel může aktivně ovlivnit, ať už ke svému prospěchu, či neprospěchu, lépe odrážejí pravděpodobnost jeho recidivy.[131] Objevuje se i riziko nepřímé diskriminace, kdy se na první pohled neutrální hodnoty propojí s hodnotami, které mohou být diskriminační.[132] Kupříkladu údaj o rase se sice nepředpokládá jako hodnoticí prvek pachatele, ale údaj o jeho bydlišti může být ukazatelem pro oblast, která bývá tradičně obydlována příslušníky určité etnické nebo národnostní menšiny. Algoritmus si tyto dva údaje propojí a ve výsledku bude přísněji trestat osoby ze stejné oblasti, resp. osoby stejného etnika nebo národnosti.[133]

V roce 2016 došlo k přelomovému (a také značně kontroverznímu[134]) soudnímu rozhodnutí, ve kterém Nejvyšší soud USA ve Wisconsinu povolil používání algoritmu *COMPAS* (*Correctional Offender Management Profiling for Alternative Sanctions*) pro predikci kriminální recidivy.[135] Žalobce Eric Loomis vznesl žalobu proti státu Wisconsin poté, co ho algoritmus zařadil do kategorie vysoce rizikových osob, v důsledku čehož dostal 6letý trest odnětí svobody. Jako hlavní argumenty uvedl netransparentnost fungování algoritmu *COMPAS*, jelikož výpočty, které měly představovat skóre hodnocení rizik, nebyly nikde veřejně přístupné. Obviněným se tak nedostávalo možnosti algoritmus zpochybnit, napadnout, ani pochopit na jakém základě bylo jejich hodnocení rizik vypočteno. Investigativní novináři také upozornili na předpojatost tohoto

[130] BARNES, Geoffrey C. a M. HYATT, Jordan. *Classifying Adult Probationers by Forecasting Future Offending*. Online. Office of Justice Programs, 2012. s. 21-22. Dostupné z: https://www.ojp.gov/ncjrs/virtual-library/abstracts/classifying-adult-probationers-forecasting-future-offending [cit. 2024-02-23].
[131] MIRON, Marius; TOLAN, Songül; GÓMEZ, Emilia a CASTILLO, Carlos. *Evaluating causes of algorithmic bias in juvenile criminal recidivism*. Online. Artificial Intelligence and Law, Vol. 29, 2021. s. 138. ISSN 0924-8463. Dostupné z: https://doi.org/10.1007/s10506-020-09268-y [cit. 2024-02-23].
[132] Tamtéž. s. 133.
[133] FIALOVÁ, Eva. *Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva*. Online. Časopis pro právní vědu a praxi, roč. 26, č. 2, 2018. s. 240-241. ISSN 1805-2789. Dostupné z: https://doi.org/10.5817/CPVP2018-2-3 [cit. 2024-02-23].
[134] YONG, Ed. *A Popular Algorithm Is No Better at Predicting Crimes Than Random People*. Online. The Atlantic, 2018. Dostupné z: https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/ [cit. 2024-02-22].
[135] *State Wisconsin v. Loomis* [Wis. 2017] 881 N.W.2d 749

algoritmu vůči černošským obviněným (v porovnání s bělochy), kteří byli hodnoceni jako vysoce rizikoví, ale k recidivě u nich prokazatelně docházelo méně častěji. Jinými slovy, algoritmus uváděl nepřiměřený počet černošských obviněných jako falešně pozitivní.[136] Vývojáři algoritmu *COMPAS* se bránili tím, že ten pouze přímo odrážel data z minulosti, podle nichž se černoši častěji dopouštěli trestné činnosti po propuštění a při předvídání recidivy byl stejně úspěšný bez ohledu na rasu pachatele.[137] Pozdější vědecké průzkumy však prokázaly, že úspěšnost systému (okolo 65 %) se blíží výsledkům dosahovaným nejen lidskými soudci, ale i náhodně vybranými dobrovolníky, kteří v rámci experimentu určovali riziko podle stejných kritérií jako algoritmus.[138] Tento případ rozpoutal diskuzi o potřebě přísnějšího dohledu a jasnějších pravidel při nasazení UI v americkém trestním soudnictví.[139]

Kanadský Nejvyšší soud řešil v roce 2018 podobný případ, ve kterém vězeň domorodého původu J. Ewert napadl prediktivní algoritmus používaný vězeňskou nápravnou službou (*Correctional Service of Canada*) k posuzovaní rizika recidivy.[140] Tvrdil, že algoritmus byl trénován pouze na datech o nepůvodních obyvatelích a nemá tak dostatek dat o domorodém obyvatelstvu, aby byl vůči jeho příslušníkům spravedlivý. Soud uznal, že přesnost algoritmu ohledně skupiny obyvatel, na které nebyl nikdy testován, může být natolik snížená, že použití bude v rozporu se zákonným požadavkem na úplné informace o pachateli předtím, než bude podroben hodnocení rizika recidivy. Rozhodnutí slouží jako připomínka toho, že dosažení skutečné rovnosti před zákonem pro všechny obyvatele musí zahrnovat respektování kulturních práv ve všech aspektech systému trestního soudnictví, včetně správy nápravného systému.[141]

---

[136] ANGWIN, Julia; LARSON, Jeff; MATTU, Surya a KIRCHNER, Lauren Lauren Kirchner. *Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks*. Online. ProPublica, 2016. Dostupné z: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [cit. 2024-02-22].

[137] SPIELKAMPARCHIVE, Matthias. *Inspecting Algorithms for Bias*. Online. MIT Technology Review, 2017. Dostupné z: https://www.technologyreview.com/2017/06/12/105804/inspecting-algorithms-for-bias/ [cit. 2024-02-22].

[138] DRESSEL, Julia a FARID, Hany. *The accuracy, fairness, and limits of predicting recidivism*. Online. Science Advances, Vol. 4, No. 1, 2018. ISSN 2375-2548. Dostupné z: https://doi.org/10.1126/sciadv.aao5580 [cit. 2024-02-22].

[139] CHAWLA, Mallika. *COMPAS Case Study: Investigating Algorithmic Fairness of Predictive Policing*. Online. Medium, 2022. Dostupné z: https://mallika-chawla.medium.com/compas-case-study-investigating-algorithmic-fairness-of-predictive-policing-339fe6e5dd72 [cit. 2024-02-22].

[140] *Ewert v. Canada* [2018] 2 S.C.R. 165

[141] TRAN, Dominic. *Supreme Court of Canada rules use of psychological risk assessment tools on Indigenous offenders illegal*. Online. Human Rights Law Centre, 2018. Dostupné z: https://www.hrlc.org.au/human-rights-case-summaries/2018/12/17/supreme-court-of-canada-rules-use-of-psychological-risk-assessment-tools-on-indigenous-offenders-illegal [cit. 2024-02-22].

Vězeňská služba ČR se inspirovala nástrojem na hodnocení rizik *OASys* (*Offender Assessment System*) používaný vězeňskou a probační službou v Anglii a Walesu[142] a od roku 2012 zavedla vlastní nástroj nazývaný *SARPO* (Souhrnná Analýza Rizik a Potřeb Odsouzených). Program usnadňuje vytváření komplexních zpráv pro další zacházení s odsouzenými ve věznici. Primárně tedy nebyl vyvinut pro potřeby soudu. Ve střednědobé budoucnosti by však mohl sloužit jako podklad, který by věznice zasílala pro potřeby rozhodnutí soudu o podmíněném propuštění.[143]

[142] *A compendium of research and analysis on the Offender Assessment Systém (OASys) 2009-2013*. Online. Ministry of Justice Analytical Series (National Offender Management Service), 2015. Dostupné z: https://www.gov.uk/government/publications/research-and-analysis-on-the-offender-assessment-system [cit. 2024-02-27].
[143] *SARPO*. Online. Vězeňská služba České republiky. Dostupné z: https://www.vscr.cz/sekce/sarpo [cit. 2024-02-27].

2. Použití umělé inteligence při vyšetřování trestných činů

Konkrétní využití UI donucovacími orgány má mnoho podob. Jedná se především o technologie rozpoznávání obličeje (např. prohledávání databází podezřelých osob, identifikaci obětí obchodování s lidmi či sexuálního vykořisťování a zneužívání dětí, 3D rekonstrukce obličeje z neidentifikované lebky), rozpoznávání řeči (např. softwarem *Phonexia Voice Inspector* s funkcí identifikace mluvčího a automatického označování mluvčích, dále např. technologie odezírání ze rtů, odšumování nahrávek, aktivace při vyslovení spouštěcího slova) a dalších lidských vlastností (např. rozpoznání srdečního rytmu, určení pohlaví kosterních pozůstatků), automatické rozpoznávání registračních značek (např. aplikacemi *BriefCam Investigator* nebo *CertiConVis*), algoritmy pro detekci výstřelu, křiku, tříštění skla (např. *ShotSpotter* nebo *Sound Event Detector*), inteligentní systémy detekce lži (např. již zmiňovaný *iBorderCtrl*), pokročilé virtuální nástroje pitvy pro pomoc při zjišťování příčiny smrti (např. odhad doby od úmrtí, odhad věku zubů), nástroje k odhalování finančních podvodů a financování terorismu, monitoring sociálních sítí, termovizní kamery, rozpoznávání vzorců aktivity pachatelů (např. otisky prstů, rtů a bot, stopy po kulkách), rozkrývání zločineckých skupin (např. v rámci projektu *ROXANNE* policie analyzuje text, řeč, videa a sítí v reálném čase) odhalování anomálií nebo nesrovnalostí ve virtuálním prostoru, upozorňování na podezřelé transakce a automatizovaném zjišťování kybernetických hrozeb atd.[144, 145]

Při prověřování a vyšetřování v rámci trestního řízení může UI zrychlit, zjednodušit nebo dokonce nahradit některé části policejní práce. Automatizace opakujících se úkolů v administrativě a při shromažďování informací z různých zdrojů (např. bankovní účty, sociální sítě, emaily) umožňuje vyšetřovatelům soustředit se na složitější a strategičtější aspekty své práce.[146] Systémy UI umí absorbovat specializované znalosti a poskytovat doporučení na základě

[144] JADHAV, Ekta; SANKHLA, M. Singh a KUMAR Rajeev. *Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation*. Online. Journal of Seybold Report, Vol. 15, No. 8, 2020. s. 2067-2072. ISSN 1533-9211. Dostupné z: https://www.researchgate.net/publication/343826071_Artificial_Intelligence_Advancing_Automation_in_Forensic_Science_Criminal_Investigation [cit. 2024-03-01].

[145] MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. s. 47-57. Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/ [cit. 2024-05-2].

[146] KUPPALA, Jishitha; SRINIVAS, K. Kalyana; ANUDEEP, P.; KUMAR, R. Sravanth a VARDHINI, P. A Harsha. *Benefits of Artificial Intelligence in the Legal System and Law Enforcement*. Online. In: 2022 International Mobile and Embedded Technology Conference (MECON). IEEE, 2022. s. 221-225. ISBN 9781665420204. Dostupné z: https://doi.org/10.1109/MECON53876.2022.9752352 [cit. 2024-03-01].

analýzy dat, čímž doplňují a vylepšují lidské rozhodovací procesy kriminalistů.[147] Podpora UI u policie může spočívat i v rozuzlení složitých dosud nevyřešených případů nebo porovnávání důkazů z různých míst činu mezi sebou.[148] Úplné nahrazení lidské policejní práce zatím očekávat nemůžeme, jelikož poptávka po kvalifikovaném a individuálním lidském přístupu bude u policie trvalá.[149] To ovšem neznamená, že UI nebude stále častěji a ve větší míře integrována do oblasti vymáhání práva. V současné době UI nejvýznamněji pomáhá policejním orgánům s předpovídáním vzorců kriminality, zpracováním důkazních materiálů a plošným sledováním obyvatel.

2.1 Predikce trestné činnosti

Predikcí trestné činnosti se rozumí předvídání míst, kde se trestný čin pravděpodobně odehraje, kdo bude jeho možným pachatelem nebo obětí a jak se dál budou vyvíjet zločinecké sítě na určitém území nebo ve virtuálním prostředí.[150] Predikce pomocí systémů UI spočívá v analýze dat o typu, místě a času minulých trestných činů algoritmem, který vytvoří předpověď budoucích trestných činů, které s největší pravděpodobností nastanou. Policejním orgánům informace o pravděpodobném výskytu trestné činnosti umožňuje efektivněji přerozdělovat zdroje dle potřeby (např. cíleně nasazovat policejní hlídky v rizikových místech) a také překonat jejich tradičně reakční přístup ke zločinu, tzn. proaktivně zasáhnout ještě předtím, než k němu vůbec dojde (např. parkovací garáže na letištích mohou těžit z přítomnosti policie, která odrazuje od krádeží automobilů anebo která zloděje aut rovnou dopadne).[151]

[147] FAQIR, Raed S. A. *Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview*. Online. International Journal of Cyber Criminology, Vol. 17, No. 2, 2023. s. 88. Dostupné z: https://doi.org/10.5281/zenodo.4766706 [cit. 2024-03-01].
[148] TAUBER, Alejandro. *How the Dutch police are using AI to unravel cold cases*. Online. TNW, 2018. Dostupné z: https://thenextweb.com/news/how-the-dutch-police-is-using-ai-to-unravel-cold-cases [cit. 2024-03-01].
[149] *Koncepce rozvoje Policie ČR do roku 2027*. Online. Policie ČR. Dostupné z: https://www.policie.cz/clanek/dokumenty-policie-ceske-republiky.aspx [cit. 2024-03-01].
[150] FERGUSON, Andrew Guthrie. *Predictive Policing Theory*. Online. In: LAVE, Tamara Rice a MILLER, Eric J. The Cambridge Handbook of Policing in the United States. Cambridge University Press, 2019. s. 491-510. ISBN 9781108354721. Dostupné z: https://doi.org/10.1017/9781108354721.025 [cit. 2024-03-03].
[151] BERK, Richard A. *Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement*. Online. Annual Review of Criminology, Vol. 4, No. 1, 2021. s. 216. ISSN 2572-4568. Dostupné z: https://doi.org/10.1146/annurev-criminol-051520-012342 [cit. 2024-03-03].

2.1.1 Mapy kriminality

Předpovídání trestné činnosti se obvykle odvozuje zaznamenaných údajů o trestných činech v čase (měsíc, týden, den nebo určitá denní doba, kdy se trestný čin odehrál, nebo byl nahlášen) a prostoru (celá města nebo čtvrť, ale i konkrétní roh ulice výskytu trestného činu). Prostorové statistiky zahrnují analýzu rozložení trestných činů a identifikaci tzv. hotspotů (*crime hotspots*), kde se trestná činnost koncentruje.[152] K zobrazení prostorové statistiky se nejčastěji používají mapy kriminality (*crime heat maps*), které jsou už dnes rozšířené po celém světě.[153] Jedná se nejen o statické mapy, ale také o mapy dynamické v reálném čase. Sofistikovanější mapy kriminality jsou založeny na vzájemném zkoumání geografických faktorů z různých rizikových oblastí, které podporují růst trestné činnosti, tzv. *Risk Terrain Modelling*.[154] Například průnik výskytu prodejen potravin, prádelen a opuštěných domů na jednom místě přitahuje drogovou kriminalitu – dealeři oslovují zákazníky v prodejnách, v prádelnách probíhá transakce a v opuštěných domech konzumace drog.

V České republice vznikl pod záštitou Ministerstva vnitra v roce 2014 projekt s názvem „Mapy budoucnosti“. Zaměřoval se na vyhodnocení možných přístupů k predikci kriminality u nás. V roce 2019 na něj navázal projekt „Mapy budoucnosti II“, který měl na základě prostorových dat o kriminalitě přispět k vytvoření nástrojů k mapování, analýze a predikci kriminality. Jedním z výstupů určených pro potřeby veřejnosti byla „Mapa kriminality ČR“. Pro potřeby policie byla do mapové aplikace implementována tzv. funkcionalita predikce kriminality, která v čtvercové síti (100 x 100 metrů) předpovídá zvýšené riziko trestné činnosti na základě 236 proměnných charakteristických pro daný čtverec.[155] Proměnnými jsou data o trestných činech a jejich interakce s okolím (čas a místo v daném čtverci), klasifikace území (charakter území v daném čtverci), významnost data (pracovní dny, svátky), historická data počasí (teplota, úhrn srážek, rychlost větru, vlhkost vzduchu, index příjemnosti počasí) atd. Mapa rovněž usnadňuje určení místní příslušnosti policejního oddělení, pod které spadá vyšetřování konkrétního trestného činu v daném území.[156]

---

[152] Tamtéž. s. 216.
[153] Například česká aplikace Mapa kriminality (https://kriminalita.policie.cz/) nebo *Crime map* ve Spojeném království (https://www.police.uk/pu/your-area/metropolitan-police-service/junction/?tab=crimemap)
[154] JOEL M. Caplan a LESLIE W. Kennedy. *Risk Terrain Modeling: Crime Prediction and Risk Reduction*. Oakland: University of California Press, 2016. ISBN 9780520282933.
[155] *Mapy budoucnosti II*. Online. Ministerstvo vnitra, 2019. Dostupné z: https://www.mvcr.cz/clanek/mapy-budoucnosti-ii.aspx [cit. 2024-03-03].
[156] BRAVENEC, Vojtěch. *Predikce kriminality v práci Policie ČR – ukázka prediktivních map a možnosti využití predikce při plánování služeb, neuronové sítě*. Online. Ministerstvo vnitra, 2022. Dostupné z:

Díky začlenění predikčních modelů s technologií UI do mapových aparátů je možné ohlížet se zpět v čase, ale také dívat se vpřed na možný vývoj kriminality v budoucnosti.[157] Informace získané v reálném čase umožňují policejním orgánům zasahovat na místech, kde je pravděpodobnost dopadení pachatele nejvyšší. Ačkoli tento přístup může nabídnout výhody z hlediska účinnosti a rychlosti policejního zásahu, měl by být aplikován s určitou mírou opatrnosti, jelikož to může trestnou činnost pouze vytlačit (rozšířit) do okolních oblastí, kde se původně vůbec nevyskytovala.[158] Přesto jsou mapy kriminality účinným nástrojem prevence trestné činnosti, jehož používání policejními orgány s sebou nenese žádné riziko.

2.1.2 Prediktivní modely

Ve Spojených státech[159] a Velké Británii[160] jsou ve velké míře rozšířeny prediktivní nástroje společností *Geolitica* (dříve *PredPol*), který vyhodnocuje spíše místní faktory a platformu na dolování dat *Palantir*, který zpracovává hlavně údaje o jednotlivcích. Software společnosti *Geolitica* generuje denní mapy podle četnosti trestné činnosti, které nasměrují policejní hlídky na konkrétní místo s potenciálním ohniskem zločinu. Systém pracuje s minimálním počtem vstupních dat, kterými jsou pouze hlášení o incidentech, druh trestného činu, čas a místo výskytu trestného činu.[161] *Palantir* používá americká policie k automatizovanému profilování potencionálních pachatelů a obětí, na základě sledování vazeb na členy gangů, kriminální minulosti, monitoringu sociálních sítí a dalších osobních údajů o vybraných jednotlivcích.[162] Zatímco prvotní zprávy z většiny policejních oddělení o fungování těchto systémů byly pochvalné,[163] pozdější studie

https://www.mvcr.cz/clanek/prezentace-z-konference-projektu-mapy-budoucnosti-ii-v-narodni-technicke-knihovne-9-cervna-2022.aspx [cit. 2024-03-03].

[157] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 8-9. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-03-01].

[158] WEISBURD, David; WYCKOFF, Laura A.; READY, Justin; ECK, John E.; HINKLE, Joshua C. et al. *Does Crime Just Move Around The Corner? A Controlled Study of Spatial Displacement and Diffusion of Crime Control Benefits*. Online. Criminology, Vol. 44, No. 3, 2006. ISSN 0011-1384. Dostupné z: https://doi.org/10.1111/j.1745-9125.2006.00057.x [cit. 2024-03-03].

[159] COLLINS, Dave. *Should police use computers to predict crimes and criminals?* Online. Associated Press, 2018. Dostupné z: https://apnews.com/article/14bb35110b644edc8798365ade767bd2 [cit. 2024-03-03].

[160] KELION, Leo. *Crime prediction software 'adopted by 14 UK police forces'*. Online. BBC news, 2019. Dostupné z: https://www.bbc.com/news/technology-47118229 [cit. 2024-03-03].

[161] Na rozdíl od jiných softwarů – například *HunchLab* do výpočtu predikce trestné činnosti započítává data specifická pro konkrétní oblast včetně socioekonomických ukazatelů jako je roční období nebo počasí.

[162] WINSTON, Ali. *Palantir has secretly been using New Orleans to test its predictive policing technology*. Online. The Verge. 2018. Dostupné z: https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd [cit. 2024-03-04].

[163] VOUNG, Zen. *Alhambra police chief says predictive policing has been successful*. Online. Pasadena Star-News, 2017. Dotupné z: https://www.pasadenastarnews.com/government-and-politics/20140211/alhambra-police-chief-says-predictive-policing-has-been-successful/ [cit. 2024-03-04].

ukázaly, že predikce byly úspěšné pouze v 1 % zkoumaných případů nebo že byly předpojaté vůči černošskému a hispánskému obyvatelstvu.[164, 165] Některá města používání těchto prediktivních systémů, po provedení vnitřních auditů a tlaku veřejnosti, ukončila.[166, 167] Zrušení se týkalo i osm let aktivně používaného systému *SSL* (*Strategic Subject List*), který shromažďoval data o rezidentech a přiděloval jim skoré na stupnici od 0 do 500 odrážející pravděpodobnost jejich účasti na střelbě v pozici pachatele nebo jako oběti střelby.[168] Ukončení bylo zdůvodněno také zaznamenáním nulového přispění systému ke snižování kriminality a celkové finanční nákladnosti na údržbu systému.[169] Policie také testovala nebo rovnou nasadila prediktivní nástroje UI na místní úrovni v Německu (např. *Pre Crime Observation System*), Nizozemsku (např. *Crime Anticipation System*), Japonsku (např. *Vaak*) a Číně (např. *Dahua Technology*).[170]

Prediktivní modely UI používané policejními orgány nejvíce sužuje kritika kvůli potencionálnímu zkreslení výsledků, do kterých se propisují historické předsudky schopné vyvolat přehnanou (nebo nedostatečnou) kontrolu určité skupiny osob, a to zejména těch, kteří pocházejí z ekonomicky chudých oblastí nebo rasových menšin. To naznačuje, že se v prediktivních modelech odráží strukturální diskriminace ve společnosti. Tyto modely jsou mnohdy také nedostatečně transparentní a narušují rovnováhu (proporcionalitu) mezi veřejnou bezpečností a základním právem na ochranu osobních údajů.[171] K této problematice se vyjádřil i Evropský soud pro lidská práva, který v případě mírového aktivisty konstatoval porušení práva na

---

[164] SANKIN, Aaron a MATTU, Surya. *Predictive Policing Software Terrible At Predicting Crimes*. Online. The Markup, 2023. Dostupné z: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes [cit. 2024-03-04].

[165] *Automating Banishment part 5: Racial Terror and White Wealth in South Central*. Online. Stop LAPD Spying Coalition, 2021. Dostupné z: https://automatingbanishment.org/section/5-racial-terror-and-white-wealth-in-south-central/ [cit. 2024-03-04].

[166] BHUIYAN, Johana. *LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws*. Online. The Guardian, 2021. Dostupné z: https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform [cit. 2024-03-04].

[167] V Německu označil ústavní soud používání prediktivního nástroje firmy *Palantir* za protiústavní, blíže viz https://www.euractiv.com/section/artificial-intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/ [cit. 2024-03-04].

[168] GORNER, Jeremy. *With violence up, Chicago police focus on a list of likeliest to kill, be killed*. Online. Chicago Tribune, 2019. Dostupné z: https://www.chicagotribune.com/2016/07/22/with-violence-up-chicago-police-focus-on-a-list-of-likeliest-to-kill-be-killed/ [cit. 2024-03-04].

[169] SWEENEY, Annie a GORNER, Jeremy. *For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.* Online. Chicago Tribune, 2020. Dostupné z: https://www.chicagotribune.com/2020/01/24/for-years-chicago-police-rated-the-risk-of-tens-of-thousands-being-caught-up-in-violence-that-controversial-effort-has-quietly-been-ended/ [cit. 2024-03-04].

[170] MCCARTHY, Odhran J. *AI & Global Governance: Turning the Tide on Crime with Predictive Policing*. Online. UNU-CPR, 2019. Dostupné z: https://unu.edu/cpr/blog-post/ai-global-governance-turning-tide-crime-predictive-policing [cit. 2024-03-04].

[171] CASTETS-RENARD, Céline. *Human Rights and Algorithmic Impact Assessment for Predictive Policing*. Online. In: MICKLITZ, Hans-W.; POLLICINO, Oreste; REICHMAN, Amnon; SIMONCINI, Andrea; SARTOR, Giovanni et al. (ed.). Constitutional Challenges in the Algorithmic Society. Cambridge University Press, 2021. s. 93-110. ISBN 9781108914857. Dostupné z: https://doi.org/10.1017/9781108914857.007 [cit. 2024-03-04].

soukromí ve vztahu k jeho osobním údajům, které byly shromážděny a uchovány policií v „extremistické databázi“, přestože on sám nikdy nebyl odsouzen pro žádný trestný čin.[172] Soud navázal na předchozí judikaturu, která považovala široké shromažďování informací za účelem předcházení trestné činnosti za zákonné a legitimní, avšak v projednávaném případě označil uchovávání citlivých údajů o politické příslušnosti a příslušnosti k zaměstnaneckým odborům v databázi za nepřiměřené a nadbytečné. Rovněž upozornil na nejednoznačnou povahu právního rámce pro tuto policejní databázi a nedostatek vhodných záruk, které by zabránily zneužití uchovaných osobních údajů o jednotlivcích v ní vedených.[173] Prediktivní modely UI používané policejními orgány v Evropské unii tak (i na základě tohoto rozhodnutí) mohou pracovat pouze s omezeným okruhem vstupních hodnot, které nezasahují do práv na ochranu osobních údajů.

2.2 Shromažďování a analýza důkazů

Při shromažďování a analýze důkazního materiálu pro účely trestního řízení může UI pomoct mnoha způsoby, ať už se jedná o usnadnění přijímání trestního oznámení na dálku, vyhledávání ve velkém množství digitálních důkazů, či vyhodnocování technických důkazů v různých formách (otisky prstů, vzorky DNA, balistika, toxikologický rozbor, lokalizace spermatu).[174] Systémy UI rovněž ulehčují vizualizaci a rekonstrukci místa činu ve 3D prostoru, nebo určování věku a pohlaví osoby na základě fotografií, videí, zubních rysů nebo CT skenů. Stejně tak UI pomáhá rozpoznávat příčiny smrti oběti odhalováním přítomnosti rozsivek v tkáních a orgánech, které nepřímo dokazují, že oběť utonula. Mezi hlavní výhody využití UI ve forenzních vědách tak patří především zvýšení efektivity práce, automatizace úkolů, snížení subjektivních zkreslení a zpřesnění analýzy založené na datech.

2.2.1 Přijímání trestních oznámení

Jazykové modely s podporou UI mohou přispívat ke zjednodušení a zefektivnění procesu přijímání oznámení o trestné činnosti na dálku v online prostředí. Poté, co oznamovatel sepíše

[172] Rozsudek Evropského soudu pro lidská práva ze dne 24. ledna 2019, *Catt v. United Kingdom*, stížnost č. 43514/15
[173] Global Freedom of Expression. *Catt v. the United Kingdom*. Online. Columbia University. Dostupné z: https://globalfreedomofexpression.columbia.edu/cases/catt-v-the-united-kingdom/ [cit. 2024-03-04].
[174] PIRAIANU, Alin-Ionut; FULGA, Ana; MUSAT, Carmina Liana; CIOBOTARU, Oana-Roxana; POALELUNGI, Diana Gina et al. *Enhancing the Evidence with Algorithms: How Artificial Intelligence Is Transforming Forensic Medicine*. Online. Diagnostics, Vol. 13, No. 18, 2023. s. 6. ISSN 2075-4418. Dostupné z: https://doi.org/10.3390/diagnostics13182992 [cit. 2024-03-05].

trestní oznámení a odešle jej policii, jazykové modely samostatně extrahují a vyhodnotí informace z textu oznámení. Dokáží převést nestrukturovaný text oznámení do systematičtější analýzy i s grafickým zpracováním a automaticky se doptají oznamovatele na potřebné podrobnosti.[175] Na základě informací UI následně sama strukturuje nahlášené incidenty do vhodných scénářů, vizualizuje vztahy mezi jednotlivými aktéry zmíněných v oznámení a přiřazuje váhu dostupným důkazům podle jejich významu pro daný případ, příp. upozorní na mezery ve scénářích, které je nutné podpořit dalšími důkazy. Při porovnání s již známými scénáři určí, o jaký druh trestné činnosti se pravděpodobně jedná a navrhne další potup vyšetřování.[176] Oznamovatelé tak mají k dispozici intuitivnější a uživatelsky přívětivější způsob, jak nahlásit a popsat případy trestné činnosti, což je může motivovat k poskytnutí jasnějších a podrobnějších informací, které posílí pochopení nahlášených případů policií.

2.2.2 Zpracování digitálních dat

Současná forenzní věda a kriminalistika čelí výzvám kvůli obrovskému množství dat, mikroskopických důkazů a nepřehlednému virtuálnímu prostředí, kterým už tradiční laboratorní struktury nestačí. V situacích, kdy orgány činné v trestním řízení zabaví digitální paměťová zařízení (chytré telefony, tablety, notebooky, USB flashdisky apod.) jako důkazní materiál, jsou tato zařízení následně ohledávána a prohlížena forenzními experty. Kromě problémů s poškozením na zařízení nebo zašifrováním představuje náročnou překážku identifikace a zpracování digitálních informací relevantních pro daný případ. Většinou jde pouze o malé fragmenty z celkově obrovského množství dat a pátrání po nich tak připomíná hledání jehel v kupce sena.[177] Systémy UI zvládnou tato data automaticky analyzovat, identifikovat ty nejpodstatnější, a ještě propojovat se souvislostmi, které by lidský mozek mohl přehlédnout, a to bez nutnosti vynaložení jakéhokoliv manuálního úsilí.[178]

---

[175] SCHRAAGEN M. P.; BEX F. J.; ODEKERKEN D a TESTERINK B. J. G. *Argumentation-driven information extraction for online crime reports*. Online. In: International Workshop on Legal Data Analysis and Mining. CEUR workshop proceedings, 2018. s. 5 Dostupné z: https://research.tilburguniversity.edu/en/publications/argumentation-driven-information-extraction-for-online-crime-repo [cit. 2024-03-05].

[176] BEX, Floris; PETERS, Joeri a TESTERINK Bas. *A.I. for Online Criminal Complaints: From Natural Dialogues to Structured Scenarios*. Online. Utrecht University, 2016. Dostupné z: https://www.ai.rug.nl/~verheij/AI4J/papers/AI4J_paper_20_bex.pdf [cit. 2024-03-05].

[177] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 12. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-03-01].

[178] HOELZ, Bruno W. P.; RALHA, Célia Ghedini a GEEVERGHESE, Rajiv. *Artificial intelligence applied to computer forensics*. Online. In: Proceedings of the 2009 ACM symposium on Applied Computing. New York: ACM, 2009. s. 884. ISBN 9781605581668. Dostupné z: https://doi.org/10.1145/1529282.1529471 [cit. 2024-03-05].

Nizozemský forenzní institut za tímto účelem vyvinul nástroj UI zvaný *Hansken,*[179] který dokáže zpracovat několik terabajtů dat z různých zdrojů, a i v různých formátech (text, video, zvuk atd.), včetně automatizovaného označování a ukládání těchto dat do trestního spisu. Kriminalistický ústav v Praze zase vytvořil unikátní databázi s názvem „Reliéf", která využívá technologii UI k porovnávání poznatků ze zkoumání mechanoskopických stop na povrchu lisovaných zásilek drog s podobnými případy ze spolupracujících států. Policisté vkládají informace o zadržených balících do databáze a software je automaticky upozorní, zdali už v jiné zemi nedošlo k zadržení obdobné zásilky a rovnou zobrazí i všechny indicie, které se k případu podařilo tamním policejním orgánům získat. Díky tomu policie odhalí vazby mezi zločineckými organizacemi, které se zabývají výrobou, přepravou nebo obchodem s drogami i napříč několika státy. Interpol v roce 2016[180] databázi doporučil pro všechny členské státy Evropské unie za účelem posílení mezinárodní spolupráce v boji proti nelegálnímu obchodu s drogami a v roce 2019[181] byla přiřazena k mezinárodním databázím vedeným Interpolem, který ji začal využívat celosvětově. Tyto systémy přináší zrychlení procesů analýzy dat, což může v naléhavých případech znamenat rozhodující faktor úspěchu ve vyšetřování jak s ohledem na identifikaci, sledování a dopadení podezřelých osob, tak s ohledem na shromažďování forenzních důkazů. Policie ČR pro digitální forenzní analýzu a kryptoanalýzu dále používá například software *EnCase*, který dokáže zanalyzovat velké objemy digitálních dat (např. vytáhnout data z profilů na sociálních sítí nebo obnovit smazaná data na pevném disku) a software *Cellebrite*, který zvládne prolomit zabezpečení prakticky každého mobilního telefonu.[182]

Se shromažďováním dat se významně pojí ochrana osobních údajů, které tyto data většinou tvoří. V roce 2022 řešil tento vztah Evropský inspektor na ochranu údajů, když nařídil Europolu smazat z databáze trestních spisů a veřejných databázích členských států všechna data, které uchovává déle než šest měsíců. Hlavním důvodem byla problematika věrohodnosti zpracovaných údajů, nespolehlivá analýza dat algoritmy a rozpor se zásadami o minimalizaci údajů a omezení

[179] *Hansken*. Online. Netherlands Forensic Institute. Dostupné z: https://www.forensicinstitute.nl/products-and-services/forensic-products/hansken [cit. 2024-03-05].
[180] KUDLÁČKOVÁ, Barbora. *Interpol doporučil databázi Reliéf*. Online. Policie ČR, 2016. Dostupné z: https://www.policie.cz/clanek/interpol-doporucil-databazi-relief.aspx [cit. 2024-03-01].
[181] SRNKOVÁ, Petra. *RELIÉF převzal Interpol*. Online. Policie ČR, 2019. Dostupné z: https://www.policie.cz/clanek/relief-prevzal-interpol.aspx [cit. 2024-03-01].
[182] MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. s. 54 Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/ [cit. 2024-05-2].

jejich uchovávání.[183] Tato data obsahující informace nejen o konkrétních odsouzených, ale také osobní údaje o dalších jednotlivcích, kteří nebyli nikdy podezříváni z žádné trestné činnosti, plánoval Europol vytěžit pomocí systémů UI, k čemuž v důsledku povinnosti smazání nedošlo.

2.2.3 Otisky prstů a vzorky DNA

Vyspělé technologie UI ještě zdaleka nejsou zařazeny mezi běžné forenzní vědy používané v současné kriminalistické praxi,[184] přestože už UI některé tradiční metody překonala. Jednou z nich je teorie o jedinečnosti otisků prstů, která stála na neprokázaném předpokladu, že žádné dva otisky prstů, dokonce ani z různých prstů téže osoby, nejsou stejné. Výzkum za pomoci hlubokého učení a neuronových sítí však odhalil, že člověk může mít shodné znaky otisku prstu s úplně odlišnou osobou a velmi silnou podobnost mohou mít i různé prsty téže osoby.[185] Sami výzkumníci s jistotou nevědí, jak UI dokázala s více než 99,99 % spolehlivostí správně určit otisky prstů pocházející od jediného člověka. Domnívají se, že se UI zaměřila na orientaci hřebenů ve středu prstu a nikoli na způsob, jakým jednotlivé hřebeny končí a rozvětvují se, tzn. neřídila se tradičními markanty (*minutiae*), které kriminalisté používají už desítky let. Tento průlom může pomoci forenzním expertům třeba v případech, kdy se na různých místech činu najdou dva otisky různých prstů, které by se tradičními metodami nepodařilo propojit s člověkem, kterému oba otisky patří.[186]

Analýzy technických důkazů (otisky prstů, vzorky DNA atd.) také vykazují určité riziko chybovosti nebo odchylky. Při porovnávání vzorků DNA z místa činu s DNA profily v policejní databázi nebo když je vzorek DNA směsicí z více individuálních profilů poměrně často dochází k falešně negativním i falešně pozitivním výsledkům.[187] Za pomoci UI je však možné úspěšně určit, zda se něčí DNA skutečně nachází i ve smíšených stopách nalezených na místě činu.

---

[183] European Data Protection Supervisor. *EDPS orders Europol to erase data concerning individuals with no established link to a criminal aktivity*. Online. The Office of the EDPS, 2022. Dostupné z: https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en [cit. 2024-03-09].

[184] GALANTE, Nicola; COTRONEO, Rosy; FURCI, Domenico; LODETTI, Giorgia a CASALI, Michelangelo Bruno. *Applications of artificial intelligence in forensic sciences: Current potential benefits, limitations and perspectives*. Online. International Journal of Legal Medicine, Vol. 137, No. 2, 2023. s. 455. ISSN 0937-9827. Dostupné z: https://doi.org/10.1007/s00414-022-02928-5 [cit. 2024-03-05].

[185] GUO, Gabe; RAY, Aniv; IZYDORCZAK, Miles; GOLDFEDER, Judah; LIPSON, Hod et al. *Unveiling intra-person fingerprint similarity via deep contrastive learning*. Online. Science Advances, Vol. 10, No. 2, 2024. ISSN 2375-2548. Dostupné z: https://doi.org/10.1126/sciadv.adi0329 [cit. 2024-05-04].

[186] KLEINMAN, Zoe. *Our fingerprints may not be unique, claims AI*. BBC, 2024. Dostupné z: https://www.bbc.com/news/technology-67944537 [cit. 2024-05-04].

[187] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 12. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-03-01].

Výzkum v rámci Syracuské univerzity v New Yorku představil nový přístup hybridního strojového učení k analýze směsi DNA, která kombinuje silné stránky lidských analytických přístupů s poznatky strojového učení. Přístup vyžaduje minimální výpočetní a finanční zdroje a poskytuje informativní a vysoce spolehlivé závěry.[188] Díky samoučícím systémům, které zvládnou zpracovat velké množství dat, lze tak dosáhnout přesnější spolehlivosti, při porovnávání vzorků DNA.

K tomu, aby důkazy shromážděné pomocí UI obstály u soudu, by měly být transparentní, tzn. přístupné veřejnosti (zvláště všem účastníkům trestního řízení) a procesy, včetně všech technických aspektů, na kterých jsou tyto systémy založeny, by měly být zpětně dohledatelné a srozumitelně vysvětlitelné.[189] Jeden z prvních případů použití neprůhledného systému UI k forenzní analýze řešil Vrchní soud státu Pensylvánie v roce 2012.[190] Obžalovaný Foley byl odsouzen za vraždu své manželky na základě vzorku sebraného zpod nehtu oběti, který obsahoval DNA dvou osob – oběti a osoby, která ji pravděpodobně zavraždila. Tři soudní znalci podali tři odlišné posudky o pravděpodobnosti shody odebraného vzorku DNA od obžalovaného a vzorku nalezeném na místě činu. Ten, který přisuzoval obžalovanému nejvyšší shodu byl proveden za pomoci softwaru *TrueAllele* pro analýzu vzorků DNA, který nebyl nikdy předtím použit u soudu. Argumenty, že vnitřní fungování softwaru nebylo veřejně přístupné a prováděné postupy nebylo možné nijak ověřit, a dokonce ani replikovat, odvolací soud zamítl a rozhodl se důkaz připustit.[191] Toto soudní rozhodnutí podpořilo oprávněnost nové počítačové metodiky výpočtu pravděpodobnosti shody vzorků DNA u amerických soudů. V roce 2015 americký Nejvyšší soud ve státě New York tentokrát vyjádřil obavy ohledně nedostatečné transparentnosti podobného forenzního statistického nástroje, který tentokrát označil za neprůhledný a výstupy z tohoto nástroje jako důkazy v řízení nepřipustil.[192] Jakmile byl pak systém zveřejněn, odborníci v něm našli nespočet nedostatků, a i přesto byl bez patřičného odůvodnění uznán za spolehlivý řadou

[188] BERNARDI, Dan. *Forensic Scientists Design the First Machine Learning Approach to Forensic DNA Analysis*. Online. Syracuse University News, 2021. Dostupné z: https://news.syr.edu/blog/2021/07/28/forensic-scientists-design-the-first-machine-learning-approach-to-forensic-dna-analysis/ [cit. 2024-03-05].
[189] RAAIJMAKERS, Stephan. *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*. Online. IEEE Security & Privacy, Vol. 17, No. 5, 2019. s. 74. ISSN 1540-7993. Dostupné z: https://doi.org/10.1109/MSEC.2019.2925649 [cit. 2024-03-05].
[190] *Commonwealth v. Foley* [PA. Super. Ct. 2012] 38 A.3d 882
[191] KWONG, Katherine. *The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence*. Online. Harvard Journal of Law & Technology, 2017. s. 286. Dostupné z: https://www.semanticscholar.org/paper/The-Algorithm-Says-You-Did-It%3A-The-Use-of-Black-Box-Kwong/60aada8e8d409702c3243668ffe5a47a341a83ba [cit. 2024-03-05].
[192] *People v. Collins* [N.Y. Sup. Ct. 2015] 15 N.Y.S.3d 564

amerických soudů v dalších případech.[193] Bez přístupu ke zdrojovému kódu algoritmů používaných v trestním řízení jako důkaz nemá obhajoba dostatek možností potřebných k prozkoumání alternativních scénářů a potencionálních slabin obžaloby. To je v rozporu se základními procesními právy trestního řízení, zejména pak práva na obhajobu a práva na spravedlivý proces. Soudy by proto neměly jako důkaz připustit výsledky algoritmické analýzy, pokud algoritmus nebude dostatečně transparentní alespoň pro účely obhajoby, tedy ne nutně pro ostatní veřejnost. Zároveň by procesy algoritmu užitého v trestním řízení měly být srozumitelné a vysvětlitelné.

2.3 Biometrická identifikace

Biometrie odkazuje na měření fyzických vlastností lidského těla, které jsou pro člověka jedinečné a v průběhu času neměnné. Může zahrnovat vzory kůže (otisky prstů) nebo sítě krevních cév pod kůží, genetický kód (DNA), vzhled obličeje (vzdálenost mezi obličejovými rysy jako jsou oči, nos nebo ústa) a behaviorální rysy (chůze). Tyto znaky se následně digitalizují a převádí do formátu, který je propojen s algoritmem automatizovaného ukládání a vyhledávání v nejrůznějších databázích.[194] Od klasifikace otisků prstů, přes DNA analýzu a konečně rozpoznání obličeje se biometrie začala postupně aplikovat při vyšetřování trestných činů.

2.3.1 Automatizované rozpoznávání obličeje

Rozpoznávání obličeje je jednou z nejrychleji rozvíjejících se metod biometrické identifikace, a to hlavně díky její výjimečné schopnosti propojení s dalšími technologiemi jako je kamerový systém, sociální sítě, a právě systémy UI.[195] Hodnota trhu s technologiemi rozpoznávání obličeje má podle nejnovějších předpovědí do roku 2033 dosáhnout 24 miliard dolarů, a to především v závislosti na potřebě zajištění bezpečnosti policejními orgány.[196] Policie používá

[193] GARRETT, Brandon L. a RUDIN, Cynthia. *Interpretable algorithmic forensics*. Online. Proceedings of the National Academy of Sciences, Vol. 120, No. 41, 2023. s. 6. ISSN 0027-8424. Dostupné z: https://doi.org/10.1073/pnas.2301842120 [cit. 2024-03-09].
[194] SMITH, Marcus a MILLER, Seumas. *Biometric Identification, Law and Ethics*. Online. Springer International Publishing, 2021. ISBN 9783030902551. s. 1-2. Dostupné z: https://doi.org/10.1007/978-3-030-90256-8 [cit. 2024-03-09].
[195] Tamtéž. s. 21-36.
[196] *Report: Facial recognition market to reach $24 billion by 2033, driven by law enforcement and security needs*. Online. Police1, 2024. Dostupné z: https://www.police1.com/police-products/police-technology/police-software/facial-recognition/report-facial-recognition-market-to-reach-24-billion-by-2033-driven-by-law-enforcement-and-security-needs [cit. 2024-03-09].

rozpoznávání obličeje převážně k identifikaci, tj. porovnání fotografie se sadou fotografií v policejních databázích; ztotožňování, tj. ztotožňování obličeje v reálném čase z kamerových záznamů a jeho přiřazení ke konkrétnímu jednotlivci; a ověřování, tj. porovnání živého obličeje s fotografií v dokladu totožnosti, tzv. mobilními inspekčními biometrickými systémy nebo biometrickými kontrolními branami (např. *eGATE* na letištích). Dohled v reálném čase policie provádí většinou ve veřejném prostoru s vysokou koncentrací lidí a rizikem masových útoků na obyvatelstvo. Převážně tedy na letištích (např. na Letišti Václava Havla je zavedena softwarová technologie *NEC NeoFace Watch* a *NeoFace Archiver*), nádražích, dopravních uzlech a hraničních přechodech.[197]

Přes 100 zemí na světě používá, nebo alespoň povolilo používání systémů biometrické identifikace obličeje k dopadení pachatelů trestných činů nebo hledání nezvěstných osob.[198] Zavádění plošného sledování obyvatel donucovacími orgány provází celosvětová debata o právních a etických otázkách. Například Dánský úřad pro ochranu osobních údajů posvětil používání biometrické identifikace nežádoucích osob na fotbalových stadionech.[199] Naopak český úřad na ochranu osobních údajů používání na stadionech zakázal, jelikož k tomu nenašel dostatečný právní důvod.[200] Také v několika amerických městech platí pro tamější policejní a ostatní vládní orgány absolutní zákaz používání programů pracujících s automatizovaným rozpoznáváním obličejů.[201] Systém biometrické identifikace využívá i řada mezinárodních policejních organizací jako je Interpol, který má k dispozici snímky obličejů získané z více než 179 zemí, což z ní dělá jedinečnou globální databázi zločinců.[202] V březnu 2024 bylo přijato nařízení Prüm II,[203] které má usnadnit policejní spolupráci na předávání biometrických

---

[197] KHAN, Zubair Ahmed a RIZVI, Asma. *AI BASED FACIAL RECOGNITION TECHNOLOGY AND CRIMINAL JUSTICE: ISSUES AND CHALLENGES*. Online. Turkish Journal of Computer and Mathematics Education, Vol. 12, No. 14, 2021. s. 3385-3386. ISSN 13094653. Dostupné z: https://www.proquest.com/docview/2623929941/abstract/86DEF3AAEA4342F3PQ/1?sourcetype=Scholarly%20Journals [cit. 2024-03-09].

[198] *The Facial Recognition World Map*. Online. Surfshark. Dostupné z: https://surfshark.com/facial-recognition-map [cit. 2024-03-09].

[199] LUND, Jesper. *Danish DPA approves Automated Facial Recognition*. Online. European Digital Rights, 2019. Dostupné z: https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/ [cit. 2024-03-09].

[200] *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech*. Online. Úřad pro ochranu osobních údajů, 2019. Dostupné z: https://uoou.gov.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech [cit. 2024-03-09].

[201] HASKINS, Caroline. *Oakland Becomes Third U.S. City to Ban Facial Recognition*. Online. Vice Media Group, 2019. Dostupné z: https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz [cit. 2024-03-09].

[202] *Facial Recognition*. Online. Interpol, 2020. Dostupné z: https://www.interpol.int/How-we-work/Forensics/Facial-Recognition [cit. 2024-03-09].

[203] *Nařízení Evropského parlamentu a Rady (EU) 2024/982 ze dne 13. března 2024 o automatizovaném vyhledávání a výměně údajů pro policejní spolupráci a o změně rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nařízení*

údajů mezi členskými státy v rámci jednotného informačního systému. Prümská soustava bude propojovat jednotlivé policejní databáze (např. databáze otisků prstů a hran dlaní) s ostatními systémy (jako je např. Vízový informační systém nebo Evropský informační systém rejstříků trestů). V budoucnu se počítá s rozšířením soustavy o identifikaci dle oční duhovky či sítnice a fonetickou identifikaci mluvčího.

Policie ČR už v roce 2019 žádala Magistrát hlavního města Prahy, aby systém automatického rozpoznávání obličejů aktivoval na šesti místech ve městě. Pražské vedení však odmítlo.[204] O rok později vyšlo najevo, že policie používá systém rozpoznávání obličejů od firmy *Cogniware*, v rámci kterého využívala k identifikaci osob i fotografie z veřejně dostupných zdrojů jako jsou sociální sítě.[205] V současné době česká policie využívá systém Digitální podoby osob (DPO) na rozpoznávání tváří od firmy *AUTOCONT*, který umožňuje pouze zpětné propojování fotografií s databází fotografií občanů ze státních registrů.[206] „Zpětnou" biometrickou identifikaci tak policie provádí se zapojením databází obsahující fotografie prakticky všech osob zdržující se na území ČR, jelikož může čerpat z evidence občanských průkazů, cestovních dokladů, diplomatických a služebních pasů, (centrálního) registru řidičů a informačního systému cizinců, a to v souladu s § 66a odst. 1 ve spojení s § 66 odst. 1 a 2 zákona o Policii České republiky. Důvodová zpráva k zákonu dokonce výslovně umožňuje využití *„softwarového vyhledávání a rozpoznávaní obličejů, která v případě potřeby dokáže významným způsobem zkrátit čas k odhalení pachatele, případně zabránit dalším hrozícím útokům."*[207] Zákon však explicitně nezpravomocňuje Policii ČR k zachycování obrazových záznamů osob za účelem sestavení jejich biometrické reprezentace obličeje a s těmito dále pracovat. Otázkou dále zůstává, zdali je policie, na základě výkladu ustanovení zákona o Policii České republiky, dle kterých může pořizovat zvukové, obrazové nebo jiné záznamy osob na veřejně přístupných místech (§ 62 odst. 1) a zpracovávat osobní údaje (§ 79 odst. 1 a 2), oprávněna i k používání biometrické identifikace na

Evropského parlamentu a Rady (EU) 2018/1726, (EU) 2019/817 a (EU) 2019/818 (nařízení Prüm II). Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32024R0982&qid=1716365481048 [cit. 2024-03-09].

[204] *Policie chce v Praze testovat technologii automatického rozpoznávání obličejů*. Online. Advokátní deník, 2019. Dostupné z: https://advokatnidenik.cz/2019/11/20/policie-chce-v-praze-testovat-technologii-automatickeho-rozpoznavani-obliceju/ [cit. 2024-03-09].

[205] TROJÁNEK, Hynek. *Jednou nohou v dystopii. Systém rozpoznávání obličejů používá i česká policie*. Online. Deník Referendum, 2023. Dostupné z: https://denikreferendum.cz/clanek/35457-jednou-nohou-v-dystopii-system-rozpoznavani-obliceju-pouziva-i-ceska-policie [cit. 2024-03-09].

[206] *Policie využívá nástroj na rozpoznávání tváří k objasňování trestných činů*. Online. Advokátní deník, 2023. Dostupné z: https://advokatnidenik.cz/2023/07/24/policie-vyuziva-nastroj-na-rozpoznavani-tvari-k-objasnovani-trestnych-cinu/ [cit. 2024-03-09].

[207] *Důvodová zpráva k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, č. 111/2019 Dz*

dálku „v reálném čase“ na veřejně přístupných místech. V takovém případě je zároveň také povinna zveřejnit informace o pořizování záznamů, pokud je provádí prostřednictvím stálých automatických technických systémů (§ 62 odst. 2). Ve vyjádření k provozování systému DPO ovšem policie tvrdí, že tímto způsobem systém používán není a že zavedla dostačující vnitřní opatření, které zabraňují jakémukoliv zneužití.[208]

Při plošném sledování obyvatelstva se jedná o tzv. necílené sledování, které probíhá prakticky bezdůvodně. Opakem je tzv. cílené sledování konkrétní osoby z důvodu podezření ze spáchání trestného činu, dopadení pachatele nebo vyhledání pohřešované osoby apod. Zachycení a analýza rysů obličeje při plošném sledování probíhá bez souhlasu dotčených osob[209] a je problematické z hlediska toho, že fakticky ubírá jednotlivcům anonymitu na veřejných prostranstvích a dochází tak k porušování práva na soukromí, příp. i dalších základních práv a svobod.[210] Potvrdil to i Evropský soud pro lidská práva v rozsudku k případu ruského demonstranta, kterého zatkla protiextremistická policie na základě technologií rozpoznávání obličeje.[211, 212]

V posledních letech vzrostla také obava v souvislosti s ochranou osobních údajů při použití automatizovaného rozpoznání obličeje policejními orgány.[213] V roce 2020 vyšlo najevo, že policie (a také některé soukromé společnosti) ve Spojených státech,[214] Austrálii[215] a dalších zemích po celém světě používá algoritmus k rozpoznávání obličeje vyvinutý technologickou společností *Clearview AI*, který k identifikaci osob využíval obrázky z internetu, nejčastěji z uživatelských

[208] BOCÁN, Josef. *AKTUALIZACE: Vyjádření k provozování informačního systému Digitálních podob osob*. Online. Policie ČR, 2023. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx [cit. 2024-03-09].
[209] BACALU, Filip. *Digital Policing Tools as Social Control Technologies: Data-driven Predictive Algorithms, Automated Facial Recognition Surveillance, and Law Enforcement Biometrics*. Online. Analysis and Metaphysics, Vol. 20, 2021. s. 80. ISSN 1584-8574. Dostupné z: https://doi.org/10.22381/AM2020215 [cit. 2024-03-10].
[210] MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. s. 8. Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/ [cit. 2024-05-2].
[211] VÁLOVÁ, Irena. *Policie našla muže technologií rozpoznávání obličeje. Jde o porušení práv, uvedl Štrasburk*. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/07/policie-nasla-muze-technologii-rozpoznavani-obliceje-jde-o-poruseni-prav-uvedl-strasburk/ [cit. 2024-03-10].
[212] Rozsudek Evropského soudu pro lidská práva ze dne 4. července 2023, *Glukhin v. Russia*, stížnost č. 11519/20
[213] K tomu viz například https://uoou.gov.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech [cit. 2024-03-10] a https://www.theguardian.com/technology/2023/oct/06/mps-and-peers-call-for-immediate-stop-to-live-facial-recognition-surveillance [cit. 2024-03-10].
[214] HILL, Kashmir. *The Secretive Company That Might End Privacy as We Know It*. Online. The New York Times, 2020. Dostupné z: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [cit. 2024-03-10].
[215] BOGLE, Ariel. *Australian Federal Police officers trialled controversial facial recognition tool Clearview AI*. Online. ABC News, 2020. Dostupné z: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [cit. 2024-03-10].

účtů na sociálních sítí. Po řadě hromadných žalob[216] a přezkumů státních dozorových úřadů[217] bylo společnosti *Clearview AI* nařízeno vymazat stávající údaje a trvale zakázáno zpřístupňovat svoji databázi obličejů soukromým subjektům, dočasně i policejním orgánům. Otázka zpracování citlivých osobních údajů jako jsou obličejové rysy, u kterých je pravděpodobné, že takový druh zpracování vzhledem k jeho povaze povede k vysokému riziku neoprávněného zásahu do práv a svobod subjektů ze strany policejních orgánů, vybízí k revizi a přizpůsobení zákonů na ochranu osobních údajů a zákonů upravujících pravomoci policie k použití této technologie.[218]

Klíčovým rozhodnutím pro používání automatizovaného rozpoznávání obličeje policií na veřejně dostupných místech byl rozsudek Vrchního soudu Spojeného království z roku 2019 v případu aktivisty Edwarda Bridgese.[219] Software, který používala policie v jižním Walesu za účelem dopadení hledaných osob, pracoval na principu porovnávání obrázků z kamerových záznamů s policejní databází hledaných osob v reálném čase. Pokud software nedetekoval žádnou shodu, automaticky živě pořízený snímek obličeje vymazal. Pokud shodu zaznamenal, upozornil příslušné policisty. Podle Bridgese donucovací orgány nasazením této technologie porušily jeho právo na respektování soukromého života podle čl. 8 Evropské úmluvy o lidských právech a zákona na ochranu osobních údajů. Soud však dospěl k názoru, že použití bylo oprávněné.[220] Policie jednala v rámci svých pravomocí a pro použití technologie existoval dostatečně jasný právní rámec, čímž byl splněn požadavek „souladu se zákonem“ dle Evropské úmluvy o lidských právech. Rozpor nespatřoval ani s požadavky na ochranu osobních údajů, jelikož nasazení technologie bylo provedeno otevřeným a transparentním způsobem – bylo předem oznámeno a používalo se jen po omezenou dobu a na vymezené ploše. Použití automatického rozpoznávání obličejů Waleskou policií tak bylo přiměřené i s ohledem na potencionální přínosy v porovnání s malým dopadem na práva jednotlivce.

---

[216] SMALLEY, Suzanne. *Long-running Clearview AI class action biometric privacy case settles*. Online. The Record from Recorded Future News 2023. Dostupné z: https://therecord.media/clearview-ai-class-action-privacy-suit-settles-bipa-illinois [cit. 2024-03-10].
[217] *Clearview AI data use deemed illegal in Austria, however no fine issued*. Online. noyb, 2023. Dostupné z: https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued [cit. 2024-03-10].
[218] CIDLINA, Václav a PROKŮPEK, Jan. *Legalita zavedení technologie rozpoznávání obličeje*. Online. Advokátní deník, 2020. Dostupné z: https://advokatnidenik.cz/2020/09/14/legalita-zavedeni-technologie-rozpoznavani-obliceje/ [cit. 2024-03-10].
[219] *R (Bridges) v. CCSWP and SSHD* [2019] EWHC 2341 (Admin)
[220] WRIGHT, Finley. *Bridges V CCSWP: A Landmark Case In The Era Of Automated Facial Recognition*. Online. Human Rights Pulse, 2020. Dostupné z: https://www.humanrightspulse.com/mastercontentblog/bridges-v-ccswp-a-landmark-case-in-the-era-of-automated-facial-recognition [cit. 2024-03-10].

Prvotní studie[221] ukázaly, že systémy automatizovaného rozpoznávání obličejů mají tendenci vykazovat diskriminační výsledky s vyšší chybovostí při identifikaci jedinců z určitých demografických skupin, zejména lidí s tmavší barvou pleti, také žen a mladších jedinců, v důsledku čehož jsou tyto osoby častějším cílem policejních kontrol. Na podkladě biometrického rozpoznání obličeje došlo v minulosti i k mnoha neoprávněným zatčením, kterých stále přibývá.[222] Hlavní příčinou tohoto jevu je nedostatek rozmanitosti v souborech testovacích dat, která nejsou reprezentativní pro určitou skupinu populace. Pokud je systém UI primárně trénován na sadě obrázků obličejů světlejší pleti, jeho přesnost je pochopitelně horší, když jsou mu prezentovány obrázky lidí s tmavší pletí. Vyřešení algoritmické zaujatosti společně s adaptivním právním rámcem je zásadní pro zajištění spravedlivého používání těchto nástrojů ve vyšetřovacích postupech.[223] Nicméně, nejnovější výzkumy[224] tvrdí, že rozdíl v přesnosti napříč demografickými údaji je už dnes paradoxně statisticky nevýznamný. Přestože je tato informace povzbudivá, policie by měla neustále monitorovat přesnost softwaru, který používá k automatizovanému rozpoznávání obličeje a dalších biometrických údajů, a zároveň zavádět vhodná opatření, která by zabraňovala algoritmické diskriminaci.

[221] BUOLAMWINI, Joy a GEBRU, Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Online. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency: Proceedings of Machine Learning Research 81, 2018. Dostupné z: https://proceedings.mlr.press/v81/buolamwini18a.html [cit. 2024-03-09].

[222] K tomu viz https://www.biometricupdate.com/tag/false-arrest

[223] SCHUETZ, Peter N. K. *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework*. Online. Law and Inequality: A Journal of Theory and Practice, Vol. 39, No. 1, 2021. Dostupné z: https://heinonline-org.ezproxy.is.cuni.cz/HOL/P?h=hein.journals/lieq39&i=221 [cit. 2024-03-10].

[224] MANSFIELD, Tony. *Facial Recognition Technology in Law Enforcement, Equitability Study, Final Report*. Online. National Physical Laboratory, 2023. ISSN 1754-2960. Dostupné z: https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf [cit. 2024-03-09].

3. Budoucnost umělé inteligence v trestním právu

Společnost *NVIDIA*, která je světovým lídrem v oblasti součástek pro moderní elektroniku, představila na začátku roku 2024 nový grafický procesor jménem *Blackwell*. Model čipu má být až třikrát výkonnější a energeticky úspornější než předchozí generace schopný pohánět ještě výkonnější systémy UI.[225] Zvyšováním výpočetního výkonu se budou funkce systémů UI používaných v oblasti trestního práva posouvat kupředu – trestná činnost bude sofistikovanější, kdy už například nerozeznáme *deepfake* video od reálného, zpřesní se analýza důkazů i biometrická identifikace, soubory dat pro prediktivní modely trestné činnosti budou mnohem větší a rozmanitější atd. V poslední době se také často mluví o tom, že UI nahradí lidskou práci v nejrůznějších profesích, ale že také nabídne příležitosti nové.[226] To se v budoucnu může dotknout i policistů, zejména těch na pozicích administrativní podpory. V blízké době můžeme být svědky nahrazení operátorů přijímající hovory na tísňové lince jazykovými modely, které se už dnes využívají ke komunikaci v jiných odvětvích. Nové pozice může policie nabídnout například v řadách pilotů policejních dronů, které budou významným nástrojem k pokrývání kriminality. Vyšetřování trestných činů je však práce natolik komplexní vyžadující určitou kreativitu a mezilidské dovednosti, že šance přechodu na vyšší nebo úplnou automatizaci je v tomto oboru velmi nízká. O soudcích v trestním řízení nemluvě, neboť jejich nahrazení roboty by nepřicházelo v úvahu už jen z nemožnosti spolehlivého zaručení základních požadavků na nestrannost, nezávislost a morálních vlastností soudce.

3.1 Diskuze a doporučení

Celou oblast UI trápí neexistence základní **definice** této technologie, a to nejen té právní, ale i obecné definice, na které by panovala většinová shoda mezi odborníky. Pro právo obecně bude legální definice v právních řádech zárukou právní jistoty, jelikož nemůžeme účinně regulovat objekt práva, který není jasně definován.

Trestněprávní rámec by měl zajistit zákonné standardy užívání UI a umožnit jejich účinné vymáhání. K tomu, aby UI efektivně sloužila potřebám trestního práva, bude třeba především:

[225] BLATNÝ, Jiří. *Nvidia má nový superčip. Jmenuje se po slavném vědci a umělá inteligence s ním zařadí vyšší rychlost*. Online. CzechCrunch, 2024. Dostupné z: https://cc.cz/nvidia-ma-novy-supercip-jmenuje-se-po-slavnem-vedci-a-umela-inteligence-s-nim-zaradi-vyssi-rychlost/ [cit. 2024-05-06].

[226] Viz například https://zpravy.aktualne.cz/datavize/kdo-muze-prijit-o-praci-kvuli-ai/r~33182af0d4b111eeabbe0cc47ab5f122/ [cit. 2024-05-06] nebo https://www.nexford.edu/insights/how-will-ai-affect-jobs [cit. 2024-05-06].

náležité finanční podpory od státu k implementaci systémů do pracovních postupů policie a trestního soudnictví; zavedení odpovědnosti za systémy ještě předtím, než budou v těchto oblastech široce využívány; vyžadování transparentnosti systémů; umožnění lidského dohledu například udělením přístupu uživatelům k tlačítku vypnutí celého systému; a zajištění ochrany základních lidských práv a svobod, zejména práva na spravedlivý proces a práva na soukromí. S trestněprávním rámcem by se mělo automaticky pojit i šíření osvěty o fungování těchto systémů v rámci činnosti orgánů veřejné moci. Je však třeba počítat s neustálým vývojem těchto technologií. Než dojde ke shodě na znění konkrétního zákonu, nařízení, či mezinárodní smlouvy, technologie UI už nejspíš budou o několik kroků napřed a připravovaný legislativní rámec nebude vybaven vhodnými prostředky. Interpretovat (nejen) trestní právo v kontextu UI tak rozhodně není snadný úkol. To vše vyžaduje především kolektivní úsilí všech aktérů, tj. vývojářů, programátorů, distributorů a uživatelů technologií UI. Praktický dopad první právní regulace na vývoj a používání UI v oblasti trestního práva bude možné posoudit brzy poté, co v platnost vstoupí schválené nařízení Evropské unie o umělé inteligenci (Akt o umělé inteligenci).

V **trestní odpovědnosti**, konkrétně v rámci třetího modelu, je třeba vyřešit základní otázku, zdali vůbec trestní odpovědnost UI přiznávat. Někteří autoři[227] se kloní k názoru, že ve výsledku nejspíše ano, a to z důvodu stále většího zásahu UI do trestněprávních vztahů. Jiní[228] jsou spíše proti především proto, že přiznání subjektivity je eticky nepřijatelné a jediné co způsobí bude právní chaos. Problematika vlastní trestní odpovědnosti UI však může být v budoucnu natolik složitá, že dnešní právní koncepty jí nebudou stačit a bude je třeba výrazně modifikovat. To lze pozorovat kupříkladu na institutech účastenství (Je UI schopna účastenství? Jak se bude řešit situace, kdy systém UI spáchá trestný čin ve spolupachatelství s dalším systémem UI, nebo fyzickou osobou?), ukládání trestů (Jaké druhy trestů jsou vhodné pro systémy UI? Bude možné vyřadit UI na určitou dobu z provozu jako určitá forma trestu podobnému odnětí svobody u fyzických osob? Nebo se přistoupí k úplnému vypnutí a smazání dat? Z čeho UI bude platit odškodnění?) a institutech okolnosti vylučující protiprávnost a polehčující okolnosti (Zavede se okolnost vylučující protiprávnost pro UI v případě zavirování systému? Může systém UI vyjádřit účinnou lítost?). Světové právní systémy v současné době nejsou dostatečně vybaveny na to, aby vzniklé otázky rozřešily. Zákonodárci a soudci by proto měli přehodnotit obecný přístup k trestní

[227] STANILA, Laura. *Living in the Future: New Actors in the Field of Criminal Law – Artificial Intelligence*. Online. In: Legal Science: Functions, Significance and Future in Legal Systems II. University of Latvia, 2020. ISBN 9789934185304. Dostupné z: https://doi.org/10.22364/iscflul.7.2.24 [cit. 2024-05-03].
[228] BRYSON, Joanna J.; DIAMANTIS, Mihailis E. a GRANT, Thomas D. *Of, for, and by the people: the legal lacuna of synthetic persons*. Online. Artificial Intelligence and Law, Vol. 25, No. 3, 2017. ISSN 0924-8463. Dostupné z: https://doi.org/10.1007/s10506-017-9214-9 [cit. 2024-05-03].

odpovědnosti jako celku i s ohledem na to, že už nyní se UI dokáže rozhodovat v jistém smyslu podle vlastní vůle, znalostí a zkušeností, pročež se nelze spolehnout na tradiční pojetí trestní odpovědnosti tak, jak je nastavené dnes.[229] Jako určité řešení se nabízí třeba zavedení povinnosti naprogramování systémů UI tak, aby při vlastním učení dodržovaly předem daná pravidla, a současně aby při vybočení z těchto pravidel bylo vždy možné dovodit něčí trestní odpovědnost a ta nezůstala pouze „viset ve vzduchu“. V této chvíli není možné předvídat, kam až se tento proces může posunout, protože svět vstupuje do nové éry, kdy je dokonce možné propojit lidské myšlení se strojem pomocí mozkového implantátu.[230] Nová právní úprava trestní odpovědnosti proto musí být nastavena takovým způsobem, aby jí technologický vývoj UI neutekl.

Právní regulace se bude muset vypořádat i s trestní odpovědností při řízení vozidel kontrolovaných autonomními systémy a upravit zvláštní podmínky převzetí kontroly nad vozidlem řidičem spolu s důsledky jejího nepřevzetí. Ideálně by předpisy měly být navázány na stupně automatizace řízení. Až se autonomní vozidla dostanou na adekvátní technologickou a bezpečnostní úroveň, mohou postupně vytlačit veškerá klasická (neautomatizovaná) vozidla z veřejné dopravy. V tom případě bychom mohli uvažovat o plně automatizovaném provozu, a i o plošném zákazu lidského řízení, který by zpomaloval jeho plynulost.[231] Zavedení autonomní dopravy pak může statisticky snížit počet dopravních nehod způsobených člověkem.

Nové podoby trestné činnosti při zneužití UI se projevují jak ve formě digitálního ohrožení (kybernetické útoky), tak fyzického ohrožení (útočné využití dronů a jiných typu zbraní), ale i politického ohrožení (masové šíření propagandy, manipulace s fakty, *deepfake*).[232] S vývojem moderních technologií se nebezpečí, které představuje zneužití UI bude stále stupňovat. Útoky v kybernetickém prostoru budou sofistikovanější, jelikož UI proniká do oblastí, které jsou běžně považovány za jedinečně lidské (např. sociální interakce), a proto bude těžší (i pro odborníky) je rozeznat a bránit se jim. Počítačových systémů, které lze napadnout a kompromitovat je kolem nás nespočet, a i kvůli tomu můžeme být svědky epidemie inteligentních virů, neoprávněných průniků

[229] DREMLIUGA, Roman a PRISEKINA, Natalia. *The Concept of Culpability in Criminal Law and AI Systems*. Online. Journal of Politics and Law, Vol. 13, No. 3, 2020. ISSN 1913-9055. Dostupné z: https://doi.org/10.5539/jpl.v13n3p256 [cit. 2024-05-03].
[230] KARLÍK, Tomáš. *Neuralink funguje, oznámil Musk. První pacient dokáže myšlenkami ovládat kurzor*. Online. ČT24, 2024. Dostupné z: https://ct24.ceskatelevize.cz/clanek/veda/neuralink-funguje-oznamil-musk-prvni-pacient-dokaze-myslenkami-ovladat-kurzor-346261 [cit. 2024-05-3].
[231] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020. s. 184. ISBN 9788073808037.
[232] BRUNDAGE, Miles; AVIN, Shahar; CLARK, Jack; TONER, Helen; ECKERSLEY, Peter et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Online. Cornell University, 2018. Dostupné z: https://doi.org/10.48550/arXiv.1802.07228 [cit. 2024-04-26].

do sítí a krádeží osobních dat. Zajištění silného kybernetického zabezpečení je proto klíčové. Na hrozbu kyberzločinů už v minulosti reagovali i čeští zákonodárci například zákonem č. 181/2014 Sb., o kybernetické bezpečnosti nebo založením Národního úřadu pro kybernetickou a informační bezpečnost. Je třeba vzít v úvahu výpočetní sílu UI a připravit obranné systémy schopné odrazit kybernetické útoky, zejména na kritické instituce. Je také více než žádoucí, aby se kriminalisté plně zabývali technologiemi UI, pokud chtějí mít nějakou šanci na jejich odhalování a potrestání. To platí i v rámci kriminalistických oborů, které se musejí přizpůsobit novým podobám trestné činnosti a přehodnotit některé stávající teorie zločinu a metodologické postupy vyšetřování. Některé projekty policejní spolupráce už existují, jako třeba projekt *STARLIGHT* (*Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats*)[233] zaměřený na boj proti zločinu souvisejícímu s UI, který hledá řešení, jak nejlépe mají policejní orgány reagovat na nové kybernetické hrozby. Proti útokům se zapojením UI lze jako obranný mechanismus využít i samotnou UI, která se sama naučí té nejefektivnější obraně[234] jako třeba nedávno vyvinutý jazykový model UI zvaný *Panacea*,[235] který samostatně reaguje na příchozí podvodné e-maily a účelově zapojuje útočníky do konverzace, aby získal informace o jejich skutečné identitě, a plýtval jejich časem.

Specifickou hrozbou jsou *deepfake* technologie, u kterých je vysoce pravděpodobné, že je pachatelé budou zneužívat v nejbližší době čím dál tím více, a to nejen k usnadnění různých trestných činů, ale zejména za účelem dezinformačních kampaní s cílem ovlivnit veřejné mínění. Do boje proti *deepfake* technologiím se spolu s orgány veřejné moci musí zapojit také poskytovatelé online služeb, kteří by měly investovat do nástrojů prevence, detekce a odstranění upravených videí a audionahrávek.[236] Nejčastěji se jako obranné řešení navrhuje povinné označování *deepfake* výtvorů (něco na způsob elektronického vodoznaku). Vzhledem k celosvětovému dosahu internetu by muselo dojít ke shodě na zavedení tohoto značení na nadnárodní nebo mezinárodní úrovni. Již dnes by se měl připravovat vědecký a technologický

[233] MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. s. 79. Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/ [cit. 2024-05-2].
[234] HUTSON, Matthew. *AI can now defend itself against malicious messages hidden in speech*. Online. Nature, 2019. ISSN 0028-0836. Dostupné z: https://doi.org/10.1038/d41586-019-01510-1 [cit. 2024-05-03].
[235] DALTON, Adan; AGHAEI, Ehsan; AL-SHAER, Ehab; BHATIA, Archna; CASTILLO, Esteban et al. *The Panacea Threat Intelligence and Active Defense Platform*. Online. Cornell University, 2020. Dostupné z: https://doi.org/10.48550/arXiv.2004.09662 [cit. 2024-05-3].
[236] *Facing reality? Law enforcement and the challenge of deepfakes*. *An Observatory Report from the Europol Innovation Lab*. Online. Luxembourg: Publications Office of the European Union, 2022. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/06099c52-dc33-11ee-b9d9-01aa75ed71a1/language-en [cit. 2024-05-3].

základ pro detekci *deepfake* výtvorů i na vnitrostátní úrovni. Pokud některá veřejně dostupná neuronová síť dokáže vygenerovat přesvědčivé falešné video, jehož zveřejněním se naplní znaky některého trestného činu, pak i policejní orgány musí mít k dispozici neméně efektivní nástroj schopný takové video rozpoznat a dohledat jejího tvůrce nebo šiřitele. Odpovědí na rozvoj technologie *deepfake* by tedy měl být vývoj nové videoskopické expertízy schopné rozpoznat nejzranitelnější aspekty této technologie, které prozradí, že se jedná o *deepfake* (jako je například přítomnost nebo nepřítomnost odrazu v očích osob na videu) a sdílení osvědčených postupů mezi donucovacími orgány po celém světě.[237] Účinným opatřením proti používání *deepfake* technologií k vytváření a šíření sexuálně motivovanému videoobsahu bude také zakotvení nového trestného činu, který bude přímo potírat toto společensky škodlivé jednání v trestním zákoníku.

Klíčovou otázkou **vlivu UI na rozhodování v trestním řízení** je to, zda by vůbec UI měla být vpuštěna do soudních soustav. Přes všechny možné nedostatky UI je velmi pravděpodobné, že se tak stane v dohledné době, ať už z důvodu zefektivnění administrativní práce soudů, nebo snahy o co nejobjektivnější rozhodování právě v trestním soudnictví. Předpokladem účinné a spravedlivé algoritmické spravedlnosti je objektivnost, nezaujatost a omezení diskriminace. Nedílnou součástí lidského posuzování je vždy jistá míra předsudků, které není možné očistit od přirozeně získané zkušenosti, ale u systémů UI s tím jde pracovat. Když budou systémům UI používaných v trestním řízení předkládány pouze „tvrdá“ (objektivní) data, měly by být alespoň částečně schopny určit odchylky, které vznikají pod vlivem lidských subjektivních vstupů, a vyhnout se tak zkreslení, které tyto historické předsudky způsobují.[238] Zbavení diskriminačních tendencí v rámci rozhodování v trestním řízení, by mělo být podchyceno už na počátku vývoje systémů UI. Důraz by měl být kladen na vystavění těchto systémů na zásadách antidiskriminačních předpisů a předpisů definujících přímou a nepřímou diskriminaci. Někteří autoři[239] dále navrhují, aby v případě, kdy je v rámci algoritmické spravedlnosti hodnotícím znakem recidivy rasa, pohlaví, státní příslušnost nebo další diskriminační znaky, bylo důkazní břemeno přeneseno na stranu uživatelů prediktivních algoritmů, tj. orgánů veřejné moci. Prediktivní analýzy pro hodnocení recidivy by také měly být tzv. barvoslepé (nediskriminační) a fungovat s určitým elementem náhody, který pomůže neutralizovat negativní vlivy UI na rozhodování v trestním řízení z hlediska

[237] SPIRIDONOV, M. S. *Artificial Intelligence Technologies in Criminal Procedural Proving*. Online. Journal of Digital Technologies and Law, Vol. 1, No. 2, 2023. s. 487. ISSN 2949-2483. Dostupné z: https://doi.org/10.21202/jdtl.2023.20

[238] KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. s. 110. ISBN 9788075987839.

[239] HARCOURT, Bernard E. *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age*. Online. SSRN Electronic Journal, 2005. s. 31. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.756945 [cit. 2024-02-23].

dopadů na společenskou kriminalitu. K zajištění spravedlivých výsledků a zmírňování algoritmického zkreslení v trestním soudnictví bude zapotřebí dalšího výzkumu a zavedení komplexnějších opatření, jinak se rozhodování v trestním řízení stane pouze matematickým vzorcem bez vlastního uvážení soudce a lidského faktoru. Tato problematika otevírá otázky, proč algoritmy používané v trestním řízení stále nejsou takové, jaké bychom je chtěli mít. Je to tím, že jsme ještě nevytvořili ten správný model? Nebo neobjevili tu správnou proměnnou? Možná ano. Možná ale samotná spravedlnost nejde jednoduše přepsat do algoritmu, a budeme se proto muset spolehnout na lidské soudce tak, jako tomu bylo doposud.

Je poněkud zarážející že shromažďování údajů je (nejen) v trestním právu přísně regulováno, ale zpracování a analýzy těchto údajů už upraveny nejsou. Jinými slovy, jakmile jsou osobní údaje v držení orgánů činných v trestním řízení, mohou je podrobit všemožným druhům analýz bez toho, aniž by byli nuceni dodržovat stejně přísná pravidla jako při jejich shromažďování. Regulace a transparentnost zacházení s osobními údaji v souvislosti se systémy UI používaných v trestním soudnictví by měla přispět k lepší právní ochraně a právní jistotě účastníků trestního řízení.

Automatizované systémy s prvky UI **používané k vyšetřování trestných činů** dosud nebyly předmětem hlubší veřejné diskuze a jejich používání policejními orgány se v praxi odehrávalo bez toho, aniž by se braly na vědomí právní a etické důsledky.[240] Implementace nových technologií v policii je poměrně nákladná a vyžaduje notné investice do infrastruktury, školení policistů a údržby. V rámci přizpůsobení policejních orgánů na nové technologie by se mělo dbát i na dodržování zákonných ustanovení trestního práva procesního, která si však policie často vykládá velmi široce. Předmětem zkoumání by proto měly být policejní pravomoci v kontextu používání UI – zdali poskytují dostatečné kompetence k využití jejího potenciálu při vyšetřování trestných činů a jestli není zapotřebí je v této souvislosti upravit. Před nasazením do aktivního policejního provozu by měly být aplikace UI podrobeny vnější nezávislé kontrole, která by zhodnotila představující rizika jejího použití policejním orgánem, a to především poruchovost (chybovost), netransparentnost, zkreslení výsledků a diskriminační tendence systémů vůči určitým skupinám, které zapříčiňují prohlubování nerovností ve společnosti. Pokud jde o trestní právo hmotné, je třeba zkoumat možnosti začlenění nových ustanovení do trestních zákoníků, která by zajišťovala, aby nežádoucí jednání umožněné UI, bylo trestné. Důležitým aspektem je také

[240] MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. s. 7. Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/ [cit. 2024-05-2].

zaručení toho, aby samoučící UI sama nevykazovala nezákonné chování poté, co bude nějakou dobu působit v kriminálním prostředí.[241]

K dosažení nejefektivnější **predikce trestné činnosti** s využitím UI neexistuje jeden univerzální způsob a nepostačí aplikovat ten nejsofistikovanější a nejmodernější prediktivní model. Důležité je vzít v úvahu celkovou prediktivní strategii policie v konkrétním místě na základě mnoha dalších místně specifických faktorů.[242] Nelze se tedy spoléhat pouze na statistická data kriminality v dané lokalitě. Policejní orgány by proto měly hodnotit výstupy prediktivních modelů s odstupem a v kontextu dalších činitelů, které mají na výskyt kriminality v určité oblasti vliv. Jinak může docházet k předpojatým výsledkům vůči určitým skupinám obyvatel a oblastí, které budou v důsledku podrobovány zvýšenému počtu policejních kontrol.

Používání systémů UI ke **shromažďování a analýze důkazů** při vyšetřování trestných činů s sebou nese určitá rizika. Tyto systémy ale nabízejí příliš mnoho potenciálních výhod nato, abychom je jednoduše odmítly, a to i přes značné obavy spojené s jejich používáním. Forenzní věda se v důsledku používání UI tak může zcela proměnit. Důraz se může ještě více přesunout od faktů k číslům a pravděpodobnosti. Současně tím, kdo bude důkazy posuzovat už nemusejí být právní experti, ale výpočetní technici. Žádný odborník však není schopen zohlednit všechny právní aspekty případu a naproti tomu ani žádný soudce není obeznámen se všemi složitostmi forenzních technologií. Uživatelé UI si musí v rámci trestního řízení vzájemně vypomoci tak, aby výpočetní technici věděli, jakými právně relevantními proměnnými mají „nakrmit“ forenzní systémy, a aby soudci měli jasný a srozumitelný vhled do fungování těchto systémů. Jedině tímto vyvážením lidské odbornosti a výpočetní síly technologie UI zachováme spravedlivý a etický systém trestního soudnictví. Pokud chceme využívat systémy UI v trestních věcech, měli bychom vyžadovat především jejich transparentnost, abychom účastníkům trestního řízení zaručily základní procesní práva, příp. odhalili škodlivé forenzní systémy, které tyto požadavky nesplňují. Soudy by měly zakázat statistické důkazy generované pravděpodobnostním softwarem, jehož provozovatelé odmítají zveřejnit jejich kód, nebo alespoň umožnit dotčeným osobám napadnout tyto důkazy právními prostředky. Tato problematika se bude se zvýšenou aplikací UI při shromažďování a analýze důkazů dále prohlubovat.

---

[241] CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. s. 14-15. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759 [cit. 2024-03-01].

[242] FERGUSON, Andrew Guthrie. *Predictive Policing Theory*. Online. In: LAVE, Tamara Rice a MILLER, Eric J. The Cambridge Handbook of Policing in the United States. Cambridge University Press, 2019. s. 491-510. ISBN 9781108354721. Dostupné z: https://doi.org/10.1017/9781108354721.025 [cit. 2024-03-03].

Podle některých autorů[243] je použití **automatizovaného rozpoznávání obličeje** v místech s vyšší mírou kriminality legální a legitimní jen v případě dodržení všech zákonných podmínek, tj. pokud použití nebude narušovat osobnostní práva jednotlivců a pouze minimálně zasahovat do ochrany osobních údajů. Dalším kritériem je také pravidelný přezkum toho, zda nedošlo ke snížení kriminality v dané lokalitě do takové míry, že nasazení této technologie už není vzhledem k zásahu do osobnostní práv a ochrany osobních údajů proporční. Na druhou stranu zavedení celoplošného sledování není přípustné, jelikož to by mohlo vést ke vzniku policejního státu a narušení základních demokratických hodnot. Používání této technologie policejními orgány k vyšetřování trestných činů vyvolává mnoho eticko-právních otázek, které je třeba zvážit, prozkoumat a podrobně zodpovědět pro účely vymáhání práva, a které se navíc promítnou do dalšího vývoje UI v této oblasti. Pro jaké účely a v jakých souvislostech je přijatelné používat plošné sledování obyvatelstva nebo pořizování snímků jednotlivců v reálném čase? Jaké kontrolní mechanismy nastavit, aby bylo možné bránit se zneužití této technologie? Jak se biometrická identifikace vypořádá s technologiemi, které zabraňují sledování jako jsou brýle navržené za účelem oklamání systému rozpoznávání obličeje?

Biometrická identifikace bude zanedlouho umožňovat policejním orgánům identifikovat jednotlivce i třeba na základě způsobu chůze a jiných behaviorálních znaků, které dohromady poskládají celkový obraz o konkrétní fyzické osobě. V takové situaci se orgánům veřejné moci naskytuje možnost sociálně bodovat a kategorizovat obyvatele na základě osobního kreditu jako se to děje v některých autoritářských zemích, zejména v Číně. Právní úprava by proto měla stanovit jasné a detailní požadavky pro nasazení biometrické identifikace u vyjmenovaných trestných činů. Jakékoli mezery v legislativě umožní vládám snadno kontrolovat své občany. K zajištění všech právních předpokladů, by se měla tato technologie používat jen ve veřejném prostoru, nejlépe tam, kde se očekává nízká úroveň soukromí jako jsou náměstí, letiště, nádraží apod. Měly by se také zvážit omezení na vybraných citlivých místech jako jsou náboženské instituce a školy v souladu s požadavkem nezbytnosti a přiměřenosti. Legitimním odůvodněním použití na těchto a dalších místech může být jen zvýšená pravděpodobnost přítomnosti podezřelých a jiných hledaných osob. Současně je třeba zajistit adekvátní způsob použití této technologie a implementovat určitá časová

[243] CIDLINA, Václav a PROKŮPEK, Jan. *Legalita zavedení technologie rozpoznávání obličeje*. Online. Advokátní deník, 2020. Dostupné z: https://advokatnidenik.cz/2020/09/14/legalita-zavedeni-technologie-rozpoznavani-obliceje/ [cit. 2024-03-10].

omezení pro její použití.[244] K tomu může sloužit zakotvení předchozího souhlasu udělovaného soudem.

[244] GIKAY, Asress Adimi. *REGULATING USE BY LAW ENFORCEMENT AUTHORITIES OF LIVE FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SPACES: AN INCREMENTAL APPROACH*. Online. The Cambridge Law Journal, Vol. 82, No. 3, 2023. s. 443-444. ISSN 0008-1973. Dostupné z: https://doi.org/10.1017/S0008197323000454 [cit. 2024-05-03].

Závěr

Na několika ukázkových příkladech z praxe jsme si mohli udělat alespoň přibližný obrázek o tom, jak může technologie UI zlepšit fungování trestněprávního prostředí například při vyhodnocování faktorů, které ovlivňují problémy ve věznicích, nebo v překonávání tradičních forenzních teorií a zpřesnění analýzy důkazních materiálů. Bylo však upozorněno i na případy zneužití UI k páchání trestné činnosti anebo k perzekuci vybrané skupiny obyvatel orgány veřejné moci. Je tedy evidentní, že už dnes má UI na trestní právo obrovský vliv, který bude v budoucnu pouze sílit. Na základě některých prognóz to vypadá, že potenciál UI v trestním právu může dosáhnout až vědeckofantastických rozměrů. Naznačují to třeba úvahy o přiznání právní subjektivity systému UI, nebo také pokusy o nahrazení lidských soudců robotickými napodobeninami. S používáním UI v různých oblastech trestního práva tak souvisí nejen právní, ale i etické otázky a jejich řešení.

Automatizace celého právního prostředí je podle všeho nevyhnutelná a UI k tomu bude významně přispívat. Neobejde se to ovšem bez nutného zamyšlení nad některými problematickými aspekty, které opakovaně prostupují i celým textem této práce. Jedná se především o chybovost (poruchovost), diskriminační tendence, zkreslení výsledků a netransparentnost systémů UI. Chybovost se nejvíce objevovala v případech použití biometrické identifikace, když systémy automatizovaného rozpoznávání obličejů ignorovaly nebo nedokázaly s jistotou rozlišit tváře určité skupiny lidí, zejména jedinců tmavší pleti. I přestože se chybovost bude s postupným zlepšováním UI snižovat, stále přetrvává v současně aktivních systémech biometrické identifikace využívaných donucovacími orgány. Pokud nebude možné tyto nedostatky zcela odstranit, musí být přinejmenším zohledněny při vyhodnocování výstupních hodnot z těchto systémů získaných. Stejně tak můžeme poukázat i na poruchovost autonomních vozidel, kvůli které dochází k dopravním nehodám v automobilové dopravě. Diskriminační tendence algoritmů a nežádoucí zkreslení výsledků jsme mohli pozorovat zvláště u prediktivních modelů používaných soudy k předpovědi recidivy v rámci trestního řízení, a to zejména vůči příslušníkům určité etnické nebo národnostní menšiny. Příčinou bylo užití nespolehlivých a nereprezentativních souborů dat k trénování těchto modelů, které potom nepřímo vedlo k narušování základních procesních práv účastníků, zejména zákazu diskriminace a rovnosti před zákonem. Zásadním krokem ke zdokonalení prediktivních modelů bude proto zajištění takových souborů dat, která budou objektivně odrážet realitu ve společnosti, ale zároveň nebudou porušovat zásady ochrany osobních údajů. Netransparentnost a tzv. problém černé skříňky, kdy uživatelé UI (a někdy i samotní vývojáři) nedokázali patřičně vysvětlit probíhající procesy uvnitř systému, včetně výsledných

rozhodnutí, se projevila při uplatnění forenzních softwarů jako důkazu u soudu. K tomu, aby bylo rozhodování orgánů činných v trestním řízení čitelnější a srozumitelnější pro veřejnost, ale hlavně pro přímo dotčené osoby, je jediným možným řešením zprůhlednění celého procesu od zpřístupnění zdrojového kódu po vyhodnocování jednotlivých výstupů. Celkově vzato se praktické použití systémů UI velmi často dostávalo do rozporu se základními právy a svobodami, především právem na spravedlivý proces, zákazem diskriminace a právem na obhajobu.

Jako dalším kritickým faktorem na poli trestního práva se ukázala být absence právní úpravy UI. Z přehledu o trestněprávním rámci bylo patrné, že ten prozatím setrvává pouze na úrovni doporučení a národních strategií. Současné mezery v pravidlech pro využití systémů UI donucovacími orgány jim umožňují pohybovat se až na samotné hraně zákona, což bylo evidentní zejména z případů, kdy police používala technologii biometrické identifikace neoprávněně a bez legitimních důvodů. Uvidíme, co změní připravovaná legislativa v podobě evropského nařízení (Akt o umělé inteligenci), která by měla sjednotit používání UI v oblasti vymáhání práva a zajistit zákonné záruky proti jejímu zneužití donucovacími orgány. Nařízení podmiňuje použití biometrické identifikace souhlasem soudu a dalšími požadavky na transparentnost jako je registrace systému do evropské databáze, které by měly dohromady předcházet narušování základních práv a svobod, především práva na soukromí. Od evropského přístupu by se potom měly odrazit i národní zákonodárci, kteří zatím v trestněprávní legislativě UI značně zaostávají. Vnitrostátní úprava použití UI donucovacími orgány by se měla ještě specificky přizpůsobit právním řádům jednotlivých zemí a jelikož jsou evropská pravidla nastavena poněkud zdrženlivě, můžeme na národní úrovni očekávat jejich zpřísňování.

Neexistence právní regulace UI se promítla i do proměny trestné činnosti pachatelů, kteří ji začali intenzivněji zneužívat ke kybernetickým útokům, internetovým podvodům a sexuálně motivovaným trestným činům, obzvlášť za pomoci *deepfake* technologie. Zavedení nového trestného činu výroby a šíření pornografických *deepfake* výtvorů je zásadním krokem z hlediska prevence a ochrany před touto vzrůstající trestnou činností. S rozvojem nové trestné činnosti souvisí i zajištění takových nástrojů pro bezpečnostní sbory, které budou alespoň na stejné technologické úrovni, jakou disponují pachatelé, jinak nebude možné tuto trestnou činnost odhalit a trestat. Z opačného hlediska bude i začlenění moderních technologií u policie vyžadovat adekvátní technické zabezpečení, ať už se jedná o umožnění lidského dohledu, informační povinnosti nebo třeba registrace aktivních systémů UI do speciální databáze k tomuto účelu stvořenou.

Je třeba důrazně varovat před značným rizikem, které UI v trestněprávním kontextu představuje. Ve výsledku se však nelze absolutně vymezit proti používání UI v trestním právu (se zaměřením na použití při vyšetřování trestných činů), jelikož to, jak se bude tato aplikační praxe dál vyvíjet určí v první řadě nezastavitelný technologický pokrok, který bude hranice možností stále posouvat, a až na druhém místě bude způsob, jakým se k této problematice postaví právo.

Seznam použitých zdrojů

1. Seznam použité literatury

BACALU, Filip. *Digital Policing Tools as Social Control Technologies: Data-driven Predictive Algorithms, Automated Facial Recognition Surveillance, and Law Enforcement Biometrics*. Online. Analysis and Metaphysics, Vol. 20, 2021. ISSN 1584-8574. Dostupné z: https://doi.org/10.22381/AM2020215

BAHNSEN, Alejandro C; TORROLEDO, Ivan; CAMACHO, Luis D; a VILLEGAS, Sergio. *DeepPhish: Simulating Malicious AI*. Online. Computer Science, 2018. Dostupné z: https://www.semanticscholar.org/paper/DeepPhish-%3A-Simulating-Malicious-AI-Bahnsen-Torroledo/ae99765d48ab80fe3e221f2eedec719af80b93f9#citing-papers

BERK, Richard A. *Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement*. Online. Annual Review of Criminology, Vol. 4, No. 1, 2021. ISSN 2572-4568. Dostupné z: https://doi.org/10.1146/annurev-criminol-051520-012342

BEX, Floris; PETERS, Joeri a TESTERINK Bas. *A.I. for Online Criminal Complaints: From Natural Dialogues to Structured Scenarios*. Online. Utrecht University, 2016. Dostupné z: https://www.ai.rug.nl/~verheij/AI4J/papers/AI4J_paper_20_bex.pdf

BRUNDAGE, Miles; AVIN, Shahar; CLARK, Jack; TONER, Helen; ECKERSLEY, Peter et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Online. Cornell University, 2018. Dostupné z: https://doi.org/10.48550/arXiv.1802.07228

BRYSON, Joanna J.; DIAMANTIS, Mihailis E. a GRANT, Thomas D. *Of, for, and by the people: the legal lacuna of synthetic persons*. Online. Artificial Intelligence and Law, Vol. 25, No. 3, 2017. ISSN 0924-8463. Dostupné z: https://doi.org/10.1007/s10506-017-9214-9

BUOLAMWINI, Joy a GEBRU, Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Online. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency: Proceedings of Machine Learning Research 81, 2018. Dostupné z: https://proceedings.mlr.press/v81/buolamwini18a.html

CASTETS-RENARD, Céline. *Human Rights and Algorithmic Impact Assessment for Predictive Policing*. Online. In: MICKLITZ, Hans-W.; POLLICINO, Oreste; REICHMAN, Amnon; SIMONCINI, Andrea; SARTOR, Giovanni et al. (ed.). Constitutional Challenges in the Algorithmic Society. Cambridge University Press, 2021. s. 93-110. Dostupné z: https://doi.org/10.1017/9781108914857.007

CUSTERS, Bart. *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*. Online. SSRN Electronic Journal, 2023. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4331759

DALTON, Adan; AGHAEI, Ehsan; AL-SHAER, Ehab; BHATIA, Archna; CASTILLO, Esteban et al. *The Panacea Threat Intelligence and Active Defense Platform*. Online. Cornell University, 2020. Dostupné z: https://doi.org/10.48550/arXiv.2004.09662

DOBREV, Dimiter. *A Definition of Artificial Intelligence*. Online. Mathematica Balkanica, New Series, Vol. 19, 2005. Dostupné z: https://doi.org/10.48550/arXiv.1210.1568

DREMLIUGA, Roman a PRISEKINA, Natalia. *The Concept of Culpability in Criminal Law and AI Systems*. Online. Journal of Politics and Law, Vol. 13, No. 3, 2020. ISSN 1913-9055. Dostupné z: https://doi.org/10.5539/jpl.v13n3p256

DRESSEL, Julia a FARID, Hany. *The accuracy, fairness, and limits of predicting recidivism*. Online. Science Advances, Vol. 4, No. 1, 2018. ISSN 2375-2548. Dostupné z: https://doi.org/10.1126/sciadv.aao5580

DVOŘÁK, Marek. *Bezpilotní letadla (drony) a oprávnění policistů k zamezení jejich provozu*. In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. Vliv nových technologií na trestní právo. Praha: Auditorium, 2022. s. 280-293. ISBN 9788087284957.

ELSAYED, Gamaleldin F; GOODFELLOW, Ian; SOHL-DICKSTEIN, Jascha. *Adversarial Reprogramming of Neural Networks*. Online. Cornell University, 2018. Dostupné z: https://doi.org/10.48550/arXiv.1806.11146

FAQIR, Raed S. A. *Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview*. Online. International Journal of Cyber Criminology, Vol. 17, No. 2, 2023. Dostupné z: https://doi.org/10.5281/zenodo.4766706

FERGUSON, Andrew Guthrie. *Predictive Policing Theory*. Online. In: LAVE, Tamara Rice a MILLER, Eric J. The Cambridge Handbook of Policing in the United States. Cambridge University Press, 2019. s. 491-510. ISBN 9781108354721. Dostupné z: https://doi.org/10.1017/9781108354721.025

FIALOVÁ, Eva. *Využití algoritmů při profilování v trestním řízení a důsledky pro lidská práva*. Online. Časopis pro právní vědu a praxi, roč. 26, č. 2, 2018. ISSN 1805-2789. Dostupné z: https://doi.org/10.5817/CPVP2018-2-3

FIALOVÁ, Eva; MATEJKA, Ján a GÜTTLER, Vojen. *Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod*. Praha: Ústav státu a práva AV ČR, 2020. ISBN 9788087439425. Dostupné z: https://www.ilaw.cas.cz/casopisy-a-knihy/knihy-a-e-knihy/profilovani-a-automatizovane-rozhodovani-(nejen)-ve-svetle-lidskych-prav-a-zakladnich-svobod.html

FOREJTOVÁ, Monika a ZÁRUBA, Viktor. *Kontury evropského Aktu o umělé inteligenci*. Online. Právní prostor, 2024. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/kontury-evropskeho-aktu-o-umele-inteligenci

GALANTE, Nicola; COTRONEO, Rosy; FURCI, Domenico; LODETTI, Giorgia a CASALI, Michelangelo Bruno. *Applications of artificial intelligence in forensic sciences: Current potential benefits, limitations and perspectives*. Online. International Journal of Legal Medicine, Vol. 137, No. 2, 2023. ISSN 0937-9827. Dostupné z: https://doi.org/10.1007/s00414-022-02928-5

GARRETT, Brandon L. a RUDIN, Cynthia. *Interpretable algorithmic forensics*. Online. Proceedings of the National Academy of Sciences, Vol. 120, No. 41, 2023. ISSN 0027-8424. Dostupné z: https://doi.org/10.1073/pnas.2301842120

GIKAY, Asress Adimi. *REGULATING USE BY LAW ENFORCEMENT AUTHORITIES OF LIVE FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SPACES: AN INCREMENTAL*

APPROACH. Online. The Cambridge Law Journal, Vol. 82, No. 3, 2023. ISSN 0008-1973. Dostupné z: https://doi.org/10.1017/S0008197323000454

GUO, Gabe; RAY, Aniv; IZYDORCZAK, Miles; GOLDFEDER, Judah; LIPSON, Hod et al. *Unveiling intra-person fingerprint similarity via deep contrastive learning*. Online. Science Advances, Vol. 10, No. 2, 2024. ISSN 2375-2548. Dostupné z: https://doi.org/10.1126/sciadv.adi0329

HALLEVY, Gabriel. *The Criminal Liability of Artificial Intelligence Entities*. Online. SSRN Electronic Journal, 2010. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.1564096

HALLEVY, Gabriel. *When Robots Kill: Artificial Intelligence Under Criminal Law*. Boston: Northeastern University Press, 2013. ISBN 9781555538019.

HANNAH-MOFFAT, Kelly. *Actuarial Sentencing: An "Unsettled" Proposition*. Online. Justice Quarterly Vol. 30, No. 2, 2013. ISSN 0741-8825. Dostupné z: https://doi.org/10.1080/07418825.2012.682603

HARCOURT, Bernard E. *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age*. Online. SSRN Electronic Journal, 2005. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.756945

HOELZ, Bruno W. P.; RALHA, Célia Ghedini a GEEVERGHESE, Rajiv. *Artificial intelligence applied to computer forensics*. Online. In: Proceedings of the 2009 ACM symposium on Applied Computing. New York: ACM, 2009. s. 883-888. ISBN 9781605581668. Dostupné z: https://doi.org/10.1145/1529282.1529471

HOFFMANN, Christian Hugo. *Is AI intelligent? An assessment of artificial intelligence, 70 years after Turing*. Online. Technology in Society, 2022. Dostupné z: https://doi.org/10.1016/j.techsoc.2022.101893

HOLČÍK, Jiří a KOMENDA, Martin. *Matematická biologie: e-learningová učebnice*. Online. Brno: Masarykova univerzita, 2015. ISBN 9788021080959. Dostupné z: https://portal.matematickabiologie.cz/

HUTSON, Matthew. *AI can now defend itself against malicious messages hidden in speech*. Online. Nature, 2019. ISSN 0028-0836. Dostupné z: https://doi.org/10.1038/d41586-019-01510-1

JADHAV, Ekta; SANKHLA, M. Singh a KUMAR Rajeev. *Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation*. Online. Journal of Seybold Report, Vol. 15, No. 8, 2020. ISSN 1533-9211. Dostupné z: https://www.researchgate.net/publication/343826071_Artificial_Intelligence_Advancing_Automation_in_Forensic_Science_Criminal_Investigation

JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část.* 8. aktualizované vydání. Praha: Leges, 2022. ISBN 9788075025760

JOEL M. Caplan a LESLIE W. Kennedy. *Risk Terrain Modeling: Crime Prediction and Risk Reduction*. Oakland: University of California Press, 2016. ISBN 9780520282933

KARAFILLIDIS, Athanasios a WEIDNER, Robert (ed.). *Developing Support Technologies. Biosystems & Biorobotics*. Online. Springer International Publishing, 2018. Dostupné z: https://doi.org/10.1007/978-3-030-01836-8_26

KHAN, Zubair Ahmed a RIZVI, Asma. *AI BASED FACIAL RECOGNITION TECHNOLOGY AND CRIMINAL JUSTICE: ISSUES AND CHALLENGES*. Online. Turkish Journal of Computer and Mathematics Education, Vol. 12, No. 14, 2021. ISSN 1309-4653. Dostupné z: https://www.proquest.com/docview/2623929941/abstract/86DEF3AAEA4342F3PQ/1?sourcetype=Scholarly%20Journals

KNUTH, Donald E. *Umění programování. 1. díl, Základní algoritmy.* Brno: Computer Press, 2008. ISBN 9788025120255

KOLAŘÍKOVÁ, Linda a HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. ISBN 9788075987839

KOMKOV, Stepan a PETIUSHKO, Aleksandr. *AdvHat: Real-World Adversarial Attack on ArcFace Face ID System*. Online. In: 2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021. s. 819-826. ISBN 9781728188089. Dostupné z: https://doi.org/10.1109/ICPR48806.2021.9412236

KUPPALA, Jishitha; SRINIVAS, K. Kalyana; ANUDEEP, P.; KUMAR, R. Sravanth a VARDHINI, P. A Harsha. *Benefits of Artificial Intelligence in the Legal System and Law Enforcement*. Online. In: 2022 International Mobile and Embedded Technology Conference (MECON). IEEE, 2022. s. 221-225. ISBN 9781665420204. Dostupné z: https://doi.org/10.1109/MECON53876.2022.9752352

KWONG, Katherine. *The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence*. Online. Harvard Journal of Law & Technology, 2017. Dostupné z: https://www.semanticscholar.org/paper/The-Algorithm-Says-You-Did-It%3A-The-Use-of-Black-Box-Kwong/60aada8e8d409702c3243668ffe5a47a341a83ba

MCCARTHY, John; MINSKY, Marvin L; ROCHESTER, Nathaniel a SHANNON, Claude E. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Online. AI Magazine, 1955. Dostupné z: https://doi.org/10.1609/aimag.v27i4.1904

MIKEŠ, Stanislav. *Právo ve věku inteligentních strojů*. Online. Bulletin advokacie, 2018. Dostupné z: http://www.bulletin-advokacie.cz/pravo-ve-veku-inteligentnich-stroju

MIRON, Marius; TOLAN, Songül; GÓMEZ, Emilia a CASTILLO, Carlos. *Evaluating causes of algorithmic bias in juvenile criminal recidivism*. Online. Artificial Intelligence and Law, Vol. 29, 2021. ISSN 0924-8463. Dostupné z: https://doi.org/10.1007/s10506-020-09268-y

MIRSKY, Yisroel; MAHLER, Tom; SHELEF, Ilan a ELOVICI Yuval. *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. Online. 28th USENIX Security Symposium, 2019. ISBN 9781939133069 Dostupné z: https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky

OSMANI, Nora. *The Complexity of Criminal Liability of AI Systems*. Online. Masaryk University Journal of Law and Technology, Vol. 14, No. 1, 2020. ISSN 1802-5951. Dostupné z: https://doi.org/10.5817/MUJLT2020-1-3

PIRAIANU, Alin-Ionut; FULGA, Ana; MUSAT, Carmina Liana; CIOBOTARU, Oana-Roxana; POALELUNGI, Diana Gina et al. *Enhancing the Evidence with Algorithms: How Artificial Intelligence Is Transforming Forensic Medicine*. Online. Diagnostics, Vol. 13, No. 18, 2023. ISSN 2075-4418. Dostupné z: https://doi.org/10.3390/diagnostics13182992

POLČÁK, Radim. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti*. Online. Bulletin advokacie, 2018. Dostupné z: http://www.bulletin-advokacie.cz/odpovednost-umele-inteligence-a-informacni-utvary-bez-pravni-osobnosti

PROVAZNÍK, Jan a MULÁK, Jiří. *Roboti za mřížemi - je české trestní právo připraveno na rozvoj umělé inteligence?* In: GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana. Vliv nových technologií na trestní právo. Praha: Auditorium, 2022. s. 256-279. ISBN 9788087284957.

RAAIJMAKERS, Stephan. *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*. Online. IEEE Security & Privacy, Vol. 17, No. 5, 2019. ISSN 1540-7993. Dostupné z: https://doi.org/10.1109/MSEC.2019.2925649

SHARKEY, Noel; GOODMAN, Marc a ROS, Nick. *The Coming Robot Crime Wave*. Online. Computer. 2010, Vol. 43, No. 8. ISSN 0018-9162. Dostupné z: https://doi.org/10.1109/MC.2010.242

SHCHITOVA, A.A. *Definition of Artificial Intelligence for Legal Regulation*. Online. In: Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020). Paris: Atlantis Press, 2020. s. 616-620. ISBN 9789462392915. Dostupné z: https://doi.org/10.2991/aebmr.k.201205.104

SCHERMER, Bart; GEORGIEVA, Ilina; VAN DER HOF, Simone a KOOPS, Bert-Jaap. *Legal Aspects of Sweetie 2.0*. Online. In: VAN DER HOF, Simone; GEORGIEVA, Ilina; SCHERMER, Bart a KOOPS, Bert-Jaap (ed.). Sweetie 2.0. Information Technology and Law Series. The Hague: T.M.C. Asser Press, 2019. s. 1-94. ISBN 9789462652873. Dostupné z: https://doi.org/10.1007/978-94-6265-288-0_1

SCHRAAGEN M. P.; BEX F. J.; ODEKERKEN D a TESTERINK B. J. G. *Argumentation-driven information extraction for online crime reports*. Online. In: International Workshop on Legal Data Analysis and Mining: CEUR workshop proceedings, 2018. Dostupné z: https://research.tilburguniversity.edu/en/publications/argumentation-driven-information-extraction-for-online-crime-repo

SCHUETZ, Peter N. K. *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework*. Online. Law and Inequality: A Journal of Theory and Practice, Vol. 39, No. 1, 2021. Dostupné z: https://heinonline-org.ezproxy.is.cuni.cz/HOL/P?h=hein.journals/lieq39&i=221

SMITH, Marcus a MILLER, Seumas. *Biometric Identification, Law and Ethics*. Online. Springer International Publishing, 2021. ISBN 9783030902551. Dostupné z: https://doi.org/10.1007/978-3-030-90256-8

SPIRIDONOV, M. S. *Artificial Intelligence Technologies in Criminal Procedural Proving*. Online. Journal of Digital Technologies and Law, Vol. 1, No. 2, 2023. ISSN 2949-2483. Dostupné z: https://doi.org/10.21202/jdtl.2023.20

STANILA, Laura. *Living in the Future: New Actors in the Field of Criminal Law – Artificial Intelligence*. Online. In: Legal Science: Functions, Significance and Future in Legal Systems II. University of Latvia, 2020. ISBN 9789934185304. Dostupné z: https://doi.org/10.22364/iscflul.7.2.24

ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020. ISBN 9788073808037.

TERZIDO, Kalliopi. *The Use of Artificial Intelligence in the Judiciary and its Compliance with the Right to a Fair Trial*. Online. 31 Journal of Judicial Administration 154, 2022. Dostupné z: https://ssrn.com/abstract=4495715

TURING, Alan. M. *I.-COMPUTING MACHINERY AND INTELLIGENCE*. Online. Mind, Vol. LIX, No. 236, 1950. ISSN 1460-2113. Dostupné z: https://doi.org/10.1093/mind/LIX.236.433

WEISBURD, David; WYCKOFF, Laura A.; READY, Justin; ECK, John E.; HINKLE, Joshua C. et al. *Does Crime Just Move Around The Corner? A Controlled Study of Spatial Displacement and Diffusion of Crime Control Benefits*. Online. Criminology, Vol. 44, No. 3, 2006. ISSN 0011-1384. Dostupné z: https://doi.org/10.1111/j.1745-9125.2006.00057.x

2. Seznam použitých internetových zdrojů

"Break Their Lineage, Break Their Roots". China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims. Online. Human Rights Watch, 2021. Dostupné z: https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting

A compendium of research and analysis on the Offender Assessment Systém (OASys) 2009-2013. Online. Ministry of Justice Analytical Series (National Offender Management Service), 2015. Dostupné z: https://www.gov.uk/government/publications/research-and-analysis-on-the-offender-assessment-system

A Definition of AI: Main Capabilities and Scientific Disciplines. Online. Brussels: European Commission, 2018. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

ALLEN-EBRAHIMIAN, Bethany. *Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm*. Online. International Consortium of Investigative Journalists, 2019. Dostupné z: https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/

An Overview of the Federal Post Conviction Risk Assessment. Online. Administrative Office of the United States Courts (Office of Probation and Pretrial Services), 2011. Dostupné z: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2014/PCRA_2011.pdf

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya a KIRCHNER, Lauren Lauren Kirchner. *Machine Bias: There's software used across the country to predict future criminals. And it's*

biased against blacks. Online. ProPublica, 2016. Dostupné z: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Artificial Intelligence | Chapters. Online. Legal 500, 2023. Dostupné z: https://www.legal500.com/guides/guide/artificial-intelligence/

Automating Banishment part 5: Racial Terror and White Wealth in South Central. Online. Stop LAPD Spying Coalition, 2021. Dostupné z: https://automatingbanishment.org/section/5-racial-terror-and-white-wealth-in-south-central/

Backup driver for self-driving Uber that killed Arizona pedestrian pleads guilty. Online. The Guardian, 2023. Dostupné z: https://www.theguardian.com/technology/2023/aug/01/uber-self-driving-arizona-deadly-crash

BARNES, Geoffrey C. a M. HYATT, Jordan. *Classifying Adult Probationers by Forecasting Future Offending*. Online. Office of Justice Programs, 2012. Dostupné z: https://www.ojp.gov/ncjrs/virtual-library/abstracts/classifying-adult-probationers-forecasting-future-offending

BERNARDI, Dan. *Forensic Scientists Design the First Machine Learning Approach to Forensic DNA Analysis*. Online. Syracuse University News, 2021. Dostupné z: https://news.syr.edu/blog/2021/07/28/forensic-scientists-design-the-first-machine-learning-approach-to-forensic-dna-analysis/

BETZ, Sunny a WHITFIELD, Brennan. *7 Types of Artificial Intelligence: From chatbots to super-robots, here's the types of AI to know and where the tech's headed next*. Online. Built In, 2024. Dostupné z: https://builtin.com/artificial-intelligence/types-of-artificial-intelligence

BHUIYAN, Johana. *LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws*. Online. The Guardian, 2021. Dostupné z: https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform

BLATNÝ, Jiří. *Nvidia má nový superčip. Jmenuje se po slavném vědci a umělá inteligence s ním zařadí vyšší rychlost*. Online. CzechCrunch, 2024. Dostupné z: https://cc.cz/nvidia-ma-novy-supercip-jmenuje-se-po-slavnem-vedci-a-umela-inteligence-s-nim-zaradi-vyssi-rychlost/

Bletchley Declaration. Online. Department for Science, Innovation and Technology, 2023. Dostupné z: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

BOCÁN, Josef. *AKTUALIZACE: Vyjádření k provozování informačního systému Digitálních podob osob*. Online. Policie ČR, 2023. Dostupné z: https://www.policie.cz/clanek/vyjadreni-k-provozovani-informacniho-systemu-digitalnich-podob-osob.aspx

BOGLE, Ariel. *Australian Federal Police officers trialled controversial facial recognition tool Clearview AI*. Online. ABC News, 2020. Dostupné z: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

BRAVENEC, Vojtěch. *Predikce kriminality v práci Policie ČR – ukázka prediktivních map a možnosti využití predikce při plánování služeb, neuronové sítě*. Online. Ministerstvo vnitra, 2022. Dostupné z: https://www.mvcr.cz/clanek/prezentace-z-konference-projektu-mapy-budoucnosti-ii-v-narodni-technicke-knihovne-9-cervna-2022.aspx

BRAVO, Maria V. *What U.S. Regulators can Learn from the EU AI Act*. EPIC, 2024. Online. Dostupné z: https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/

BRITTAIN, Blake. *How copyright law could threaten the AI industry in 2024*. Reuters, 2024. Dostupné z: https://www.reuters.com/legal/litigation/how-copyright-law-could-threaten-ai-industry-2024-2024-01-02/

Canada Tesla driver charged over 'napping while speeding'. Online. BBC News, 2020. Dostupné z: https://www.bbc.com/news/world-us-canada-54197344

CIDLINA, Václav a PROKŮPEK, Jan. *Legalita zavedení technologie rozpoznávání obličeje*. Online. Advokátní deník, 2020. Dostupné z: https://advokatnidenik.cz/2020/09/14/legalita-zavedeni-technologie-rozpoznavani-obliceje/

Clearview AI data use deemed illegal in Austria, however no fine issued. Online. noyb, 2023. Dostupné z: https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued

COLLINS, Dave. *Should police use computers to predict crimes and criminals?* Online. Associated Press, 2018. Dostupné z: https://apnews.com/article/14bb35110b644edc8798365ade767bd2

COONEY, Christy. *Creating sexually explicit deepfakes to become a criminal offence*. Online. BBC News, 2024. Dostupné z: https://www.bbc.com/news/uk-68823042

Crime map. Online. Police UK (Metropolitan Police Service). Dostupné z: https://www.police.uk/pu/your-area/metropolitan-police-service/junction/?tab=crimemap

DOLEJŠÍ, Milan. *Přístroje stále nefungují, benešovská nemocnice kvůli kryptoviru omezí provoz i v pondělí*. Online. ČT24, 2019. Dostupné z: https://ct24.ceskatelevize.cz/clanek/regiony/pristroje-stale-nefunguji-benesovska-nemocnice-kvuli-kryptoviru-omezi-provoz-i-v-pondeli-56462

Drony Nemesis. Online. Skupina D z.s., 2024. Dostupné z: https://www.dronynemesis.cz/

DUTTON, Tim. *An Overview of National AI Strategies*. Online. Medium, 2018. Dostupné z: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

EU schválila akt o umělé inteligenci. Je první svého druhu na světě. Online. Aktuálně.cz, 2024. Dostupné z: https://zpravy.aktualne.cz/zahranici/staty-eu-definitivne-potvrdily-drive-odsouhlaseny-akt-o-umel/r~45068598174d11efb589ac1f6b220ee8/

European Data Protection Supervisor. *EDPS orders Europol to erase data concerning individuals with no established link to a criminal aktivity*. Online. The Office of the EDPS, 2022. Dostupné z: https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en

Evropský přístup k umělé inteligenci. Online. Evropská komise, 2024. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/european-approach-artificial-intelligence

Experimental Security Research of Tesla Autopilot. Online. Ars Electronica, 2019. Dostupné z: https://ars.electronica.art/center/en/experimental-security-research-of-tesla-autopilot/

Facial Recognition. Online. Interpol, 2020. Dostupné z: https://www.interpol.int/How-we-work/Forensics/Facial-Recognition

Facing reality? Law enforcement and the challenge of deepfakes. *An Observatory Report from the Europol Innovation Lab*. Online. Luxembourg: Publications Office of the European Union, 2022. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/06099c52-dc33-11ee-b9d9-01aa75ed71a1/language-en

FAŤUN, Martin; KUČERA, Zdeněk; KRÁL, Luboš; PĚCHOUČEK, Michal; KRAUSOVÁ, Alžběta; MATEJKA, Ján et al. *Výzkum potenciálu rozvoje umělé inteligence v České republice. Souhrnná zpráva.* Online. Úřad vlády ČR, 2018. Dostupné z: https://vlada.gov.cz/assets/evropske-zalezitosti/aktualne/AI-souhrnna-zprava-2018.pdf

FISHER, Miloslav. *Kybernetická kriminalita je v Česku na vzestupu. Pomohl tomu i covid*. Online. Novinky, 2023. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-kyberneticka-kriminalita-je-v-cesku-na-vzestupu-pomohl-tomu-i-covid-40446871

Global Freedom of Expression. *Catt v. the United Kingdom*. Online. Columbia University. Dostupné z: https://globalfreedomofexpression.columbia.edu/cases/catt-v-the-united-kingdom/

GLOVER, Ellen a KOSS, Hal. *What Is Sentient AI?: Some experts believe it's only a matter of time before artificial intelligence systems can think and feel like humans.* Online. Built In, 2024. Dostupné z: https://builtin.com/artificial-intelligence/sentient-ai

GORNER, Jeremy. *With violence up, Chicago police focus on a list of likeliest to kill, be killed*. Online. Chicago Tribune, 2019. Dostupné z: https://www.chicagotribune.com/2016/07/22/with-violence-up-chicago-police-focus-on-a-list-of-likeliest-to-kill-be-killed/

Governments race to regulate AI tools. Online. Reuters, 2024. Dostupné z: https://www.reuters.com/technology/governments-race-regulate-ai-tools-2023-10-13/

Hansken. Online. Netherlands Forensic Institute. Dostupné z: https://www.forensicinstitute.nl/products-and-services/forensic-products/hansken

HANŽL, Pavel a SOCHŮREK, Adam. *Městský soud v Praze o umělé inteligenci a autorském právu*. EPRAVO.CZ, 2023. Dostupné z: https://www.epravo.cz/top/clanky/mestsky-soud-v-praze-o-umele-inteligenci-a-autorskem-pravu-117318.html

HASKINS, Caroline. *Oakland Becomes Third U.S. City to Ban Facial Recognition*. Online. Vice Media Group, 2019. Dostupné z: https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz

HILL, Kashmir. *The Secretive Company That Might End Privacy as We Know It*. Online. The New York Times, 2020. Dostupné z: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

HIROSAWA, Mayumi. *Japan to assign bandwidth for Level 4 self-driving vehicles*. Online. NikkeiAsia, 2023. Dostupné z: https://asia.nikkei.com/Business/Technology/Japan-to-assign-bandwidth-for-Level-4-self-driving-vehicles

How the Ministry of Justice used AI to compare prison reports. Online. Ministry of Justice, 2019. Dostupné z: https://www.gov.uk/government/case-studies/how-the-ministry-of-justice-used-ai-to-compare-prison-reports--2

CHANDRAN, Rina. *Activists say China's new Silk Road equips autocrats with spy tech*. Online. Context, 2022. Dostupné z: https://www.context.news/surveillance/activists-say-chinas-new-silk-road-equips-autocrats-with-spy-tech

ChatGPT 3.5 version. Online. OpenAI, 2024. Dostupné z: https://chat.openai.com/share/bfd3b8a6-7b67-4d67-9d9c-5f847b462b10

CHATURVEDI, Amit. *Navinder Singh Sarao: How This Indian Trader Wiped Off $1 Trillion From US Market*. Online. NDTV, 2024. Dostupné z: https://www.ndtv.com/feature/navinder-singh-sarao-how-this-indian-trader-wiped-off-1-trillion-from-us-market-5062729

CHAWLA, Mallika. *COMPAS Case Study: Investigating Algorithmic Fairness of Predictive Policing*. Online. Medium, 2022. Dostupné z: https://mallika-chawla.medium.com/compas-case-study-investigating-algorithmic-fairness-of-predictive-policing-339fe6e5dd72

Internet Organised Crime Threat Assessment (IOCTA). Online. Publications Office of the European Union, 2023. Dostupné z: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

JODKA, Sara H. *Manipulating reality: the intersection of deepfakes and the law*. Online. Reuters, 2024. Dostupné z: https://www.reuters.com/legal/legalindustry/manipulating-reality-intersection-deepfakes-law-2024-02-01/

JOHN, Camila. *Theory of Mind AI: The Next Frontier in Artificial Intelligence*. Online. Medium, 2023. Dostupné z: https://medium.com/bestai/theory-of-mind-ai-the-next-frontier-in-artificial-intelligence-92cb1963ab5d

KARLÍK, Tomáš. *Neuralink funguje, oznámil Musk. První pacient dokáže myšlenkami ovládat kurzor*. Online. ČT24, 2024. Dostupné z: https://ct24.ceskatelevize.cz/clanek/veda/neuralink-funguje-oznamil-musk-prvni-pacient-dokaze-myslenkami-ovladat-kurzor-346261

KARLÍK, Tomáš. *Obecná umělá inteligence tu bude do pěti let, věří šéf společnosti Nvidia*. Online. ČT24, 2024. Dostupné z: https://ct24.ceskatelevize.cz/clanek/veda/obecna-umela-inteligence-tu-bude-do-peti-let-veri-sef-spolecnosti-nvidia-346726

KELION, Leo. *Crime prediction software 'adopted by 14 UK police forces'*. Online. BBC news, 2019. Dostupné z: https://www.bbc.com/news/technology-47118229

KILEEN, Molly. *German Constitutional Court strikes down predictive algorithms for policing*. Online. Euractiv, 2023. Dostupné z: https://www.euractiv.com/section/artificial-

intelligence/news/german-constitutional-court-strikes-down-predictive-algorithms-for-policing/

KLEINMAN, Zoe. *Our fingerprints may not be unique, claims AI*. BBC, 2024. Dostupné z: https://www.bbc.com/news/technology-67944537

KOFROŇOVÁ, Johana; VOJÍŘ, Aleš a JANKO, Michal. *Recepční, programátoři, makléři. Experti sestavili seznam, koho AI připraví o práci*. Online. Aktuálně.cz, 2024. Dostupné z: https://zpravy.aktualne.cz/datavize/kdo-muze-prijit-o-praci-kvuli-ai/r~33182af0d4b111eeabbe0cc47ab5f122/

Koncepce rozvoje Policie ČR do roku 2027. Policie ČR. Online. Dostupné z: https://www.policie.cz/clanek/dokumenty-policie-ceske-republiky.aspx

KRÁL, Petr. *Dopad deepfake pornografie má řešit soud. Satira a vtip ale nemají za cíl poškodit, upozorňuje náměstek*. iROZHLAS, 2024. Dostupné z: https://www.irozhlas.cz/zpravy-domov/dopad-deepfake-pornografie-ma-resit-soud-satira-a-vtip-ale-nemaji-za-cil_2404082223_tkz

KUDLÁČKOVÁ, Barbora. *Interpol doporučil databázi Reliéf*. Online. Policie ČR, 2016. Dostupné z: https://www.policie.cz/clanek/interpol-doporucil-databazi-relief.aspx

KUO, Lily. *China bans 23m from buying travel tickets as part of 'social credit' system*. Online. The Guardian, 2019. Dostupné z: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system

Less traditional crime, more cybercrime. Online. Statistics Netherlands (CBS), 2020. Dostupné z: https://www.cbs.nl/en-gb/news/2020/10/less-traditional-crime-more-cybercrime

LESSNER, Dan; LÁNA, Martin; PODRÁZKOVÁ TOMKOVÁ Michala a HAUT Jiří. *Základy informatiky pro střední školy*. Online. Jihočeská univerzita v Českých Budějovicích, 2020. ISBN 9788073947859. Dostupné z: https://popelka.ms.mff.cuni.cz/~lessner/mw/index.php/Hlavn%C3%AD_strana

LOKAJ, Zdeněk; ZELINKA, Tomáš; FIALOVÁ, Eva; MATEJKA, Ján; ŠČERBA, Tomáš; STEHLÍK, Vít et al. *Návrh úpravy jednotlivých právních institutů a aspektů platných v České republice relevantních pro zavádění vozidel od stupně automatizace SAE 3 a výše do provozu a zajištění jejich provozu*. Online. Ministerstvo dopravy, 2022. Dostupné z: https://www.mdcr.cz/Uzitecne-odkazy/Autonomni-mobilita

LUND, Jesper. *Danish DPA approves Automated Facial Recognition*. Online. European Digital Rights, 2019. Dostupné z: https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/

MACH, Václav. *Český Minority Report: Využití umělé inteligence Policií České republiky*. Online. Iuridicum Remedium, 2023. Dostupné z: https://digitalnisvobody.cz/blog/2023/12/30/cesky-minority-report-zmapovali-jsme-jak-policie-ceske-republiky-pracuje-s-umelou-inteligenci/

MANSFIELD, Tony. *Facial Recognition Technology in Law Enforcement, Equitability Study, Final Report*. Online. National Physical Laboratory, 2023. ISSN 1754-2960. Dostupné z: https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

Mapa kriminality. Online. Policie ČR. Dostupné z: https://kriminalita.policie.cz/

Mapy budoucnosti II. Online. Ministerstvo vnitra, 2019. Dostupné z: https://www.mvcr.cz/clanek/mapy-budoucnosti-ii.aspx

MCCARTHY, Odhran J. *AI & Global Governance: Turning the Tide on Crime with Predictive Policing*. Online. UNU-CPR, 2019. Dostupné z: https://unu.edu/cpr/blog-post/ai-global-governance-turning-tide-crime-predictive-policing

METZ, Rachel. *San Francisco just banned facial-recognition technology*. Online. CNN Business, 2019. Dostupné z: https://edition.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html

Národní strategie umělé inteligence v České republice. Online. Ministerstvo průmyslu a obchodu, 2019. Dostupné z: https://www.mpo.gov.cz/cz/podnikani/digitalni-ekonomika/umela-inteligence/

Obrana práv uprchlíků a migrantů v digitálním věku. Online. Amnesy International, 2024. Dostupné z: https://www.amnesty.cz/zprava/5889/obrana-prav-uprchliku-a-migrantu-v-digitalnim-veku

PASEKOVÁ, Eva. *ČR v justici málo využívá umělou inteligenci či práci z domova, říká zpráva EK*. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/06/cr-v-justici-malo-vyuziva-umelou-inteligenci-ci-praci-z-domova-rika-zprava-ek/

Policie chce v Praze testovat technologii automatického rozpoznávání obličejů. Online. Advokátní deník, 2019. Dostupné z: https://advokatnidenik.cz/2019/11/20/policie-chce-v-praze-testovat-technologii-automatickeho-rozpoznavani-obliceju/

Policie využívá nástroj na rozpoznávání tváří k objasňování trestných činů. Online. Advokátní deník, 2023. Dostupné z: https://advokatnidenik.cz/2023/07/24/policie-vyuziva-nastroj-na-rozpoznavani-tvari-k-objasnovani-trestnych-cinu/

Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Online. U.S. Department of State, 2023. Dostupné z: https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/

POULTNEY, Leon. *BMW matches Mercedes-Benz with huge autonomous driving upgrade for 7 Series*. Online. TechRadar, 2023. Dostupné z: https://www.techradar.com/vehicle-tech/hybrid-electric-vehicles/bmw-matches-mercedes-benz-with-huge-autonomous-driving-upgrade-for-7-series

Procedure file 2021/0106(COD) Artificial Intelligence Act. Online. European Parliament. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/0106(COD)

Předsedové nejvyšších soudů řešili umělou inteligenci. V justici se uplatní třeba při anonymizaci. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/11/predsedove-nejvyssich-soudu-resili-umelou-inteligenci-v-justici-se-uplatni-treba-pri-anonymizaci/

Report: Facial recognition market to reach $24 billion by 2033, driven by law enforcement and security needs. Online. Police1, 2024. Dostupné z: https://www.police1.com/police-products/police-technology/police-software/facial-recognition/report-facial-recognition-market-to-reach-24-billion-by-2033-driven-by-law-enforcement-and-security-needs

RIEHLE, Cornelia. *Europol Report Criminal Use of Deepfake Technology*. Online. eucrim, 2022. Dostupné z: https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/

RODELLI, Caterina. *The EU AI Act: a failure for human rights, a victory for industry and law enforcement*. Online. Acces Now, 2024. Dostupné z: https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/

ROURK, Chris. *The Turing Test is so Last Century: Introducing the Barista Test for Artificial General Intelligence*. Online. Medium, 2023. Dostupné z: https://medium.com/predict/the-turing-test-is-so-last-century-the-barista-test-for-artificial-general-intelligence-faf91034fa8c

SAE International. *SAE Levels of Driving Automation™ Refined for Clarity and International Audience*. Online. SAE Blog, 2021. Dostupné z: https://www.sae.org/site/blog/sae-j3016-update

SANKIN, Aaron a MATTU, Surya. *Predictive Policing Software Terrible At Predicting Crimes*. Online. The Markup, 2023. Dostupné z: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

SARPO. Online. Vězeňská služba České republiky. Dostupné z: https://www.vscr.cz/sekce/sarpo

SCOTT, Daniella. *Deepfake Porn Nearly Ruined My Life*. Online. ELLE, 2020. Dostupné z: https://www.elle.com/uk/life-and-culture/a30748079/deepfake-porn/

SCHWEIZER, Kristen. *Avatar Sweetie exposes sex predators*. Online. The Age, 2014. Dostupné z: https://www.theage.com.au/world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html

SKOUPILOVÁ, Ivana. *Umělá inteligence už okrádá důvěřivce*. Online. Policie České republiky – KŘP Olomouckého kraje, 2024. Dostupné z: https://www.policie.cz/clanek/umela-inteligence-uz-okrada-duverivce.aspx

SRNKOVÁ, Petra. *RELIÉF převzal Interpol*. Online. Policie ČR, 2019. Dostupné z: https://www.policie.cz/clanek/relief-prevzal-interpol.aspx

SWEENEY, Annie a GORNER, Jeremy. *For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended.* Online. Chicago Tribune, 2020. Dostupné z: https://www.chicagotribune.com/2020/01/24/for-years-chicago-police-rated-the-risk-of-tens-of-thousands-being-caught-up-in-violence-that-controversial-effort-has-quietly-been-ended/

Sweetie. Online. Terre des Hommes, 2022. Dostupné z: https://www.terredeshommes.nl/en/projects/sweetie

Sweetie: 'Girl' chatbot targets thousands of paedophiles. Online. BBC, 2017. Dostupné z: https://www.bbc.com/news/av/technology-42461065

TALMAGE-ROSTRON, Mark. *How Will Artificial Intelligence Affect Jobs 2024-2030*. Online. Nexford University, 2024. Dostupné z: https://www.nexford.edu/insights/how-will-ai-affect-jobs

TAUBER, Alejandro. *How the Dutch police are using AI to unravel cold cases*. Online. TNW, 2018. Dostupné z: https://thenextweb.com/news/how-the-dutch-police-is-using-ai-to-unravel-cold-cases

The Facial Recognition World Map. Online. Surfshark. Dostupné z: https://surfshark.com/facial-recognition-map

TRAN, Dominic. *Supreme Court of Canada rules use of psychological risk assessment tools on Indigenous offenders illegal*. Online. Human Rights Law Centre, 2018. Dostupné z: https://www.hrlc.org.au/human-rights-case-summaries/2018/12/17/supreme-court-of-canada-rules-use-of-psychological-risk-assessment-tools-on-indigenous-offenders-illegal

TROJÁNEK, Hynek. *Jednou nohou v dystopii. Systém rozpoznávání obličejů používá i česká policie*. Online. Deník Referendum, 2023. Dostupné z: https://denikreferendum.cz/clanek/35457-jednou-nohou-v-dystopii-system-rozpoznavani-obliceju-pouziva-i-ceska-policie

ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. Online. Úřad pro ochranu osobních údajů, 2019. Dostupné z: https://uoou.gov.cz/uoou-k-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech

VÁLOVÁ, Irena. *Policie našla muže technologií rozpoznávání obličeje. Jde o porušení práv, uvedl Štrasburk*. Online. Česká justice, 2023. Dostupné z: https://www.ceska-justice.cz/2023/07/policie-nasla-muze-technologii-rozpoznavani-obliceje-jde-o-poruseni-prav-uvedl-strasburk/

VOUNG, Zen. *Alhambra police chief says predictive policing has been successful*. Online. Pasadena Star-News, 2017. Dotupné z: https://www.pasadenastarnews.com/government-and-politics/20140211/alhambra-police-chief-says-predictive-policing-has-been-successful/

VRANKEN, Bram. *Big Tech lobbying is derailing the AI Act*. Online. Corporate Europe Observatory, 2023. Dostupné z: https://corporateeurope.org/en/2023/11/big-tech-lobbying-derailing-ai-act

What is artificial intelligence and how is it used? European Parliament, 2023. Dostupné z: https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

WINSTON, Ali. *Palantir has secretly been using New Orleans to test its predictive policing technology*. Online. The Verge. 2018. Dostupné z: https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

WRIGHT, Finley. *Bridges V CCSWP: A Landmark Case In The Era Of Automated Facial Recognition*. Online. Human Rights Pulse, 2020. Dostupné z:

https://www.humanrightspulse.com/mastercontentblog/bridges-v-ccswp-a-landmark-case-in-the-era-of-automated-facial-recognition

YONG, Ed. *A Popular Algorithm Is No Better at Predicting Crimes Than Random People*. Online. The Atlantic, 2018. Dostupné z: https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/

3. Seznam použitých právních předpisů

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 140/1961 Sb., trestní řád

Zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích

Zákon č. 273/2008 Sb., o Policii České republiky

Důvodová zpráva k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, č. 111/2019 Dz

Nařízení Komise v přenesené pravomoci (EU) 2017/589 ze dne 19. července 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/65/EU, pokud jde o regulační technické normy upřesňující organizační požadavky na investiční podniky zabývající se algoritmickým obchodováním

Nařízení Evropského parlamentu a Rady (EU) 2024/982 ze dne 13. března 2024 o automatizovaném vyhledávání a výměně údajů pro policejní spolupráci a o změně rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nařízení Evropského parlamentu a Rady (EU) 2018/1726, (EU) 2019/817 a (EU) 2019/818 (nařízení Prüm II)

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SV

Code de la route (Version en vigueur depuis le 16 avril 2021)

Code des transports (Version en vigueur au 06 mai 2024)

4. Seznam použité judikatury

Commonwealth v. Foley [PA. Super. Ct. 2012] 38 A.3d 882

People v. Collins [N.Y. Sup. Ct. 2015] 15 N.Y.S.3d 564

State Wisconsin v. Loomis [Wis. 2017] 881 N.W.2d 749

Ewert v. Canada [2018] 2 S.C.R. 165

R (Bridges) v. CCSWP and SSHD [2019] EWHC 2341

Rozsudek Evropského soudu pro lidská práva ze dne 24. ledna 2019, *Catt v. United Kingdom,* stížnost č. 43514/15

Rozsudek Evropského soudu pro lidská práva ze dne 4. července 2023, *Glukhin v. Russia*, stížnost č. 11519/20

5. Seznam ostatních zdrojů

Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku

Sdělení Komise Evropskému Parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru Regionů ze dne 25. dubna 2018 (Umělá inteligence pro Evropu)

Usnesení Evropského parlamentu ze dne 13. června 2018 o kybernetické obraně

Sdělení Komise Evropskému Parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru Regionů ze dne 7. prosince 2018 (Koordinovaný plán v oblasti umělé inteligence)

Bílá kniha o umělé inteligenci - evropský přístup k excelenci a důvěře ze dne 19. února 2020

Usnesení Evropského parlamentu ze dne 6. října 2021 o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech

Umělá inteligence v trestním právu
(se zaměřením na použití při vyšetřování trestných činů)

Abstrakt

Umělá inteligence je fenomén, který postupně proniká do všech oblastí našeho života, s čímž úzce souvisí i její praktické využití v různých právních odvětvích. V mezích českého trestního práva je umělá inteligence tématem poměrně neprobádaným. Zato v zahraničí se můžeme setkat s mnoha případy jejího začlenění do trestněprávní praxe, odkud je možné čerpat zkušenosti s touto technologií pro její efektivní využití u nás.

Tato práce se věnuje vybraným trestněprávním hlediskům spojených s umělou inteligencí. Nejprve obecně definuje ústřední pojem spolu s dalšími souvisejícími pojmy a shrnuje dosavadní snahy o trestněprávní úpravu umělé inteligence. Představuje též nejaktuálnější znění nového evropského nařízení, tzv. Aktu o umělé inteligenci. Dále práce prozkoumává otázky trestní odpovědnosti umělé inteligence, představuje nové podoby trestné činnosti s využitím této technologie a zjišťuje potenciální vliv umělé inteligence na rozhodování v trestním řízení. Dílčím tématem je potom praktické použití v oblasti vymáhání práva. Podrobněji se práce zaměřuje na umělou inteligenci, kterou využívá policie při vyšetřování trestných činů jako jsou systémy predikce trestné činnosti, shromažďování a analýzy důkazů a biometrické identifikace. Práce v závěru nabízí vhled do budoucnosti, rozvijí otázky k diskuzi a navrhuje konkrétní doporučení.

Hlavním přínosem práce je odhalení zásadních problematických aspektů využití umělé inteligence v trestním právu, kvůli kterým nepřímo dochází k porušování základních práv a svobod dotčených osob. Jedná se o zvýšenou chybovost systémů biometrické identifikace, která se projevila zejména u lidí s tmavší barvou pleti; diskriminační tendence algoritmů používaných v rámci trestního řízení vůči příslušníkům etnické nebo národnostní menšiny kvůli jejich nedostatečné reprezentaci v souborech dat, které jsou určené k trénování těchto algoritmů; a netransparentnost forenzních softwarů používaných u soudu jako důkaz, jejichž zdrojový kód je nepřístupný pro účastníky, kteří potom nemohou naplno uplatňovat své právo na obhajobu a právo na spravedlivý proces. Významným faktorem na poli trestního práva se také ukázala být absence právní úpravy umělé inteligence.

Klíčová slova: umělá inteligence, trestní právo, vyšetřování

Artificial Intelligence in Criminal Law
(focusing on use in criminal investigation)

Abstract

Artificial intelligence is a phenomenon that is gradually infiltrating all areas of our lives, which is closely related to its practical application in various legal sectors. Within the boundaries of Czech criminal law, artificial intelligence is a relatively unexplored topic. However, we can encounter many cases of its integration in criminal law practice abroad, from where it is possible to draw experience with this technology for its effective use in our country.

This thesis focuses on selected criminal law aspects related to artificial intelligence. Firstly, it defines the central concept along other related terms and summarizes the most up-to-date efforts of criminal legislation on artificial intelligence. It also presents the most recent version of the new European regulation, the so-called Artificial Intelligence Act. Later, the thesis explores the issues of criminal liability of artificial intelligence, introduces new methods of criminal activity using this technology and examines the potential impact of artificial intelligence on decision-making in criminal procedure. The subtopic of the thesis is the practical application in law enforcement. In more detail, the thesis focuses on artificial intelligence used by the police in criminal investigations such as crime prediction systems, evidence collection and analysis, and biometric identification. The thesis concludes by offering insight into the future, introducing questions for discussion and proposing specific recommendations.

The main contribution of the thesis is the discovery of essential problematic aspects of the use of artificial intelligence in criminal law, which indirectly lead to the violation of fundamental rights and freedoms of the people involved. These include the increased error rate in biometric identification systems, which is mostly evident in identifying people with darker skin color; the discriminatory tendencies of algorithms used in criminal proceedings towards members of ethnic or national minorities due to their insufficient representation in the datasets used to train these algorithms; and non-transparency of forensic software used as evidence in court, the source code of which is inaccessible to the parties, who are then unable to fully exercise their right of defence and right to a fair trial. The absence of legal regulation on artificial intelligence in the field of criminal law has also proved to be a significant factor.

Key words: artificial intelligence, criminal law, investigation