Eva Fialová
Ján Matejka
Vojen Güttler

ÚSTAV STÁTU A PRÁVA
Akademie věd ČR

Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod

Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod

Eva Fialová, Ján Matejka, Vojen Güttler

Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod

Vzor citace:
FIALOVÁ, E. – MATEJKA, J. – GÜTTLER, V. *Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod*. Praha: Ústav státu a práva AV ČR, 2020, 78 s. ISBN: 978-80-87439-42-5

Odborní recenzenti:
prof. JUDr. Věra Štangová, CSc.
JUDr. Ing. Libor Kyncl, Ph.D.

Technická a jazyková korektura:
Mgr. Jitka Pourová a Mgr. Iveta Bůžková

Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-26910S s názvem Biometrické údaje a jejich zvláštní právní ochrana (Biometric Data and Their Specific Legal Protection).

Vydavatel:
Ústav státu a práva AV ČR, v. v. i.
Národní 18, 116 00 Praha 1
Česká republika
www.ilaw.cas.cz

ÚSTAV STÁTU A PRÁVA
Akademie věd ČR

ISBN: 978-80-87439-42-5 (e-pub)

Obsah

Vlčí rozhodování

Kde potůček si bystře tek', tam stálo jehně, žíznilo.
Tu kousek výš si stoupne vlk; a když se jehně napilo,
vlk přijde blíž a chmuří se a hledá „slušné" důvody,
jak s neviňátkem začít spor. Ač pilo níž tam u vody,
hned zhurta na ně vyjede: „Mně kalíš vodu před nosem!"
A jehně: „Právě od tebe ta voda běží přímo sem."
Tak pádnou pravdou umlčen, vlk zosnuje si novou lež:
„A před rokem mě tupilos, což popírat snad nebudeš."
Tu vyděšené jehňátko: „Já tebe že jsem tupilo?
A jak bych mohlo, prosím tě, když před rokem jsem nežilo?"
„Tvůj otec – ten mě pohaněl," – a vlk zuří po straně;
a ještě dřív, než úžasem se zmohlo k nové obraně,
je popad' za krk, zadávil a už je vleče od vody…
„Můj hlad," si mručí,
„přemůže i nejpádnější důvody."[1]

[1] *Svět ezopských bajek*. Edice Antická knihovna sv. 35. Svoboda: Praha, 1976. Překlad Václav Bahník, Rudolf Kuthan, Jiří Valeš. 1. souborné vydání, 594 s.

Část I. Obecný úvod do problematiky

Ve veřejném prostoru, ve kterém současný člověk žije, jsou stále častěji přítomny informační a komunikační technologie. Někteří autoři hovoří o digitalizaci veřejného prostoru jako o životě v síti,[2] ze které je ovšem obtížné, ne-li nemožné se odhlásit.[3] Orgány veřejné moci informační a komunikační technologie využívají v čím dále větší míře nejen k tomu, aby zlepšily své služby poskytované občanům, ale i z toho důvodu, aby ochránily společnost před jednotlivci, kteří mohou znamenat riziko pro bezpečnost ostatních.[4] Jednotlivci jsou v určitém prostoru, např. na letišti či v jiném místě, podrobeni dohledu a automatizovanému vyhodnocování chování na základě algoritmu.

Již v roce 1995 Clive Norris zaznamenal, že nasazování kamerových systémů CCTV (*Closed Circuit Television*, dále jen: „CCTV“) ve veřejném prostoru změnilo dohled orgánů veřejné moci nad jednotlivci. Zatímco před nástupem kamer CCTV byl rozsah dohledu určen omezeným počtem policistů v ulicích, s častějším využíváním kamerových systémů CCTV lze tento dohled vykonávat nepřetržitě. Operátoři systému kamer se nacházeli v místnostech obklopeni obrazovkami, na nichž byl přenášen obraz snímaný kamerou. Pokud operátor zpozoroval neobvyklou nebo podezřelou aktivitu, zaměřil se na ni přiblížením obrazu. Jestliže bylo podle vyhodnocení operátora nutné přijmout další opatření nebo na místě zasáhnout, spojil se tento operátor s policejní hlídkou a poslal ji na místo. Další změna dle Norrise nastala, když i činnost operátora byla nahrazena automatizovaným vyhodnocováním aktivit jednotlivců a událostí ve veřejném prostoru. Systém nahradil činnost člověka. Úsudek o tom, zda dochází k určité aktivitě nebo chování, si vytváří systém sám na základě algoritmu. Vyhodnocení je tedy prováděno matematickým vzorcem.[5] Není ponecháno na operátorovi, zda se na situaci ve veřejném prostoru detailněji zaměří, nebo dokonce vyšle na místo hlídku. Tyto typy rozhodování činí systém sám právě na podkladě algoritmu. Operátor již nerozhoduje, zda v konkrétním případě zasáhnout, či nikoliv. Tato rozhodnutí algoritmus činí, stejně jako v předchozím případě, na základě profilů událostí a chování jednotlivců, kteří se na události podílejí.

---

2 VAN´T HOF, Ch. – VAN EST, R. – DAEMEN, F. *Check In / Check Out. The Public Space as an Internet of Things.* Rotterdam: NAi Publishers, 2011, s. 13.

3 Ibid., s. 147.

4 Např. ZARSKY, T. Governmental Data Mining and its Alternatives. *Penn State Law Review* [online]. 2011, Vol. 116, No. 2, s. 287 [cit. 2016-05-04]. Dostupné z: <http://www.pennstatelawreview.org/116/2/116 Penn St. L. Rev. 285.pdf>.

5 NORRIS, C. Video Charts: Algorithmic Surveillance. *Criminal Justice Matters* [online]. 1995, Vol. 20, No. 1, s. 8 [cit. 2016-05-06]. Dostupné z: <http://www.popcenter.org/library/crimeprevention/volume_10/06-Norris-Armstrong.pdf>.

Pokud je systémem detekována určitá aktivita nebo situace, může být na základě tohoto vyhodnocení přímo algoritmem rozhodnuto o dalším postupu. Systém se může na konkrétního jednotlivce dále zaměřit, snažit se ho identifikovat nebo upozornit odpovědné osoby. Pokud systém na základě předem vytvořených profilů vyhodnotí chování jednotlivce jako potenciálně nebezpečné, mohou být na tohoto jednotlivce upozorněny policejní orgány nebo zaměstnanci ostrahy, popřípadě může být chování jednotlivce ovlivněno přímo systémem. Jednotlivec může být na základě svého chování vpuštěn do určitého prostoru nebo mu může být přístup odepřen či s ním bude zacházeno jiným způsobem ve srovnání s osobami, které nebyly systémem vyhodnoceny jako rizikové. Jednotlivec může být rovněž na základě automatizovaného vyhodnocení svého chování omezen na osobní svobodě nebo může být podroben jiným opatřením nebo omezením,[6] např. osobní prohlídce.

Systémy pro hodnocení rizikovosti využívají k rozhodování analýzu chování jednotlivce, aby rozlišily tzv. normální chování od chování, které není v daném čase a místě obvyklé.[7] Standardním chováním na letišti je trasa cestujících od východu k odbavení, informační tabuli a bezpečnostní kontrole. Pokud se osoba od této standardní trasy odchýlí, systém toto jednání zaznamená.[8] Algoritmus může sice na základě chování jednotlivce rozpoznat neobvyklé chování v určitém prostoru a čase, nicméně již nedokáže vyhodnotit, proč k němu dochází.[9]

Při vyhodnocování chování a dalších tělesných charakteristik dochází ke zpracování osobních údajů. Analýza chování jednotlivce je biometrickým údajem tzv. druhé generace. Účelem biometrických údajů druhé generace není identifikovat jednotlivce, nýbrž číst jeho mysl.[10] Některé systémy mohou být nadto spojeny i s technologií na rozpoznávání obličejů a jiných biometrických údajů dané osoby.[11] K identifikaci jednotlivce dochází právě v okamžiku užití technologie na rozpoznávání obličejů, chůze či skenování duhovky. Z výše uvedeného vyplývá, že systémy pro vyhodnocování chování využívají biometriku a biometrické údaje. Na základě biometrických behaviorálních biometrických profilů vyhodnocují chování osob v určitém místě a čase. Biometrické údaje slouží i k identifikaci. K ní může dojít po vyhodnocení chování osoby jako potenciálně rizikového. Identifikovat lze rovněž každého jednotlivce v předem vymezeném prostoru. Poté, co k identifikaci dojde, mohou být vůči této osobě uplatněna opatření spojená s rizikem konkrétní osoby pro veřejný pořádek nebo

---

6 Srov. ROUVROY, A. *„Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data* [online]. 2011, s. 31 [cit. 2016-05-04]. Dostupné z: <http://works.bepress.com/antoinette_rouvroy/64/>.

7 WACHS, M. – FINK, C. N. Y. – LOUKAITOU-SIDERIS, A. – TAYLOR, B. D. Securing Public Transit Systems. In: HAKIM, S. – ALBERT, G. – SHIFTAM, Y. *Securing Transporation Systems*. Hoboken: Wiley, 2016, s. 158.

8 SCHULZ, D. M. – GILBERT, S. *Video Surveillance Uses by Rail Transit Agencies. A Synthesis of Transit Practice* [online]. Washington, 2011, s. 40 [cit. 2018-03-05]. Dostupné z: <http://www.safetyvision.com/sites/safetyvision.com/files/rail_1.pdf>.

9 HOSPEDALES, T. – GONG S. – XIANGS, T. *A Markov Clustering Topic Model for Mining Behaviour in Video* [online]. 2009, s. 7 [cit. 2018-02-01]. Dostupné z: <http://www.eecs.qmul.ac.uk/~sgg/papers/HospedalesGongXiang_ICCV09.pdf>.

10 DE HERT, P. Biometrics and the Challenge to Human Rights in Europe. In: CAMPISI, P. *Security and Privacy in Biometrics*. Dordrecht: Springer, 2013, s. 406.

11 WACHS, M. – FINK, C. N. Y. – LOUKAITOU-SIDERIS, A. – TAYLOR, B. D. *Securing Public Transit Systems*. op. cit.

národní bezpečnost. Příkladem může být identifikace pasažérů a jejich případný zápis v seznamu osob, kterým není dovoleno z bezpečnostních důvodů létat (tzv. *No Fly List*).

S rozhodováním na základě algoritmu vyvstává otázka, zda jsou zachovávána práva jednotlivce, nad nímž je ve veřejném prostoru vykonáván dohled a o němž je na podkladě algoritmického vyhodnocení dat rozhodnuto. Požadavek zachovávání lidských práv obsahuje tzv. *human-centric artificial intelligence*[12] neboli umělá inteligence zaměřená na člověka. Tento přístup k umělé inteligenci akcentuje dodržování lidských práv, lidské důstojnosti při vývoji a využívání systémů na bázi algoritmů s funkcí strojového učení.[13] V souvislosti s algoritmickým rozhodováním se nabízejí obavy z možného zásahu do tří základních práv garantovaných lidsko-právními dokumenty. Základním právem, které může být při algoritmickém rozhodování porušeno z důvodu charakterizování jednotlivce na základě profilu sestaveného z biometrických charakteristik jednotlivců, je právo nebýt diskriminován neboli zákaz diskriminace. Algoritmické rozhodování, které vyhodnocuje nestandardní vzorce chování jako podezřelé, aniž by dokázalo samo vyhodnotit příčinu tohoto chování, může vyústit v zásah proti jednotlivci. Jednotlivec bude na základě svého chování vyhodnocen jako *a priori* podezřelý z potenciálního budoucího spáchání trestného činu, přestože k žádnému takovému jednání nedošlo. Základní právo, které může být zásahem proti tomuto jednotlivci porušeno, je právo na spravedlivý proces. Dalším právem, kterým se budeme v souvislosti s algoritmickým rozhodováním zabývat, je právo na soukromí a právo ona ochranu osobních údajů. Rozhodování na podkladě algoritmu v reálném čase může ve svém důsledku narušit právo na soukromí při výkonu masového dohledu a následném zásahu orgánů veřejném moci proti osobě, nad níž je dohled vykonáván.

Cílem této publikace je analyzovat využití nových technologií, které fungují na základě algoritmů na bázi strojového učení z pohledu práva. Jelikož systémy využívající výše zmíněné algoritmy rozhodují automatizovaně, bez lidského zásahu, zaměřuje se publikace na samotnou právní úpravu automatizovaného rozhodování a na některé dílčí aspekty, které s automatizovaným rozhodováním souvisí, jako je využití algoritmů, profilování a big data. Poté publikace zanalyzuje právní regulaci biometrických údajů. Právě biometrika je využívána v systémech, které sledují a vyhodnocují chování jednotlivců, aby o nich mohly automatizovaně rozhodnout, nebo ovlivnit jejich chování.

Téma automatizovaného rozhodování a profilování na podkladě biometrických údajů je vysoce aktuální s ohledem na využité těchto nástrojů pro sledování jednotlivců, nebo lépe

[12] Podle sdělení Evropské komise se za umělou inteligenci „*považují systémy vykazující inteligentní chování v podobě vyhodnocování svého okolí a následného rozhodování či vykonávání kroků – s určitou mírou autonomie – k dosažení konkrétních cílů.*“ EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a Sociálnímu výboru a Výboru regionů. Umělá inteligence pro Evropu. 2018 [cit. 2019-12-03]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0237&from=CS>.

[13] Srov. EVROPSKÁ KOMISE, Odborná skupina na vysoké úrovni pro umělou inteligenci (AI HLEG). Etické pokyny pro zajištění důvěryhodnosti UI. 2019. [online] [cit. 2019-12-03]. Dostupné z: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

řečeno jejich plošnému monitorování a hodnocení jejich chování v reálném čase za účelem přijetí omezujícího opatření nebo vyvození jiných důsledků. Technologie, které tyto nástroje využívají, jsou nasazovány ve stále větší míře, a to z důvodu tvrzeného zajištění veřejné a národní bezpečnosti. Tato publikace upozorňuje na některá rizika s použitím těchto technologií spojená, zejména pak rizika pro základní práva a svobody člověka.

Část II. Automatizované rozhodovací procedury, jejich význam a druhy

2.1 Datová stopa člověka a její současný význam

Průměrná datová stopa člověka se během posledních desetiletí rozrostla v míře, která je v historii naší společnosti dosud nevídaná. Lidstvo o sobě generuje neuvěřitelné množství dat, mnohdy navíc zcela bez jakékoliv přímé aktivity dotčených osob. Jedinec zpravidla bývá automaticky omezen v možnosti ovlivňovat okruh informací, které jsou o něm zpracovávány, mnohdy ani nemá šanci zjistit jejich rozsah či strukturu, čímž ztrácí reálnou možnost jakkoliv ovlivnit další nakládání s těmito údaji nebo rozhodovat o jejich dalším osudu.

Na tento stav reagovala relativně dynamicky a nekompromisně EU vytvořením veřejnoprávního systému ochrany osobních údajů. Tento institut byl nejprve koncipován v polovině devadesátých let na základě Směrnice Evropského parlamentu a Rady č. 95/46/ES o ochraně osobních údajů, která až do *25. května 2018* představovala základní referenční normu pro oblasti ochrany osobních údajů v celé EU. Tato směrnice stanovila velmi přísná pravidla a omezení pro shromažďování a využívání osobních údajů a zároveň stanovila povinnost všem členským státům vytvořit nezávislý vnitrostátní orgán pověřený ochranou těchto údajů. Důvody pro přijetí tohoto režimu ochrany jinak spíše soukromoprávního statku měly své kořeny v rozhodovací praxi evropských soudů, a to zejména Ústavního soudu Německa,[14] jež jako první na světě uznaly základní lidské právo na „*informační sebeurčení*“. Tato regulace byla postupně implementována do práva všech členských států EU, jakož i některých nečlenských[15] zemí EU, a měla výrazný vliv na formování nových regulací

[14] Bundesverfassungsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.
[15] Jako např. Island, Lichtenštejnsko, Norsko aj.

ochrany osobních údajů v právních řádech států, jako je Argentina, Kanada, Hongkong, Rusko či dubajské zóny volného obchodu (DIFC).[16]

Koncepce této směrnice spočívala především v relativně široké veřejnoprávní regulaci do dosud typicky soukromoprávních vztahů; směrnice dopadala na všechny údaje zpracovávané automaticky (např. databáze zákazníků či zaměstnanců), jakož i na údaje, které jsou obsaženy v neautomatizovaném rejstříku nebo do něj mají být zařazeny (tradiční lístkové rejstříky či kartotéky), a to s tím, že je lhostejno, jakým způsobem či v jaké formě je samotné zpracovávání prováděno.[17] Hlavním cílem směrnice byla přirozená ochrana práv a svobod člověka v souvislosti se zpracováním jeho osobních údajů, přičemž za účelem naplnění tohoto cíle stanovila relativně jasné zásady, práva i povinnosti; k naplnění těchto zásad bylo zřízeno široké portfolio práv, přičemž v případě jejich porušení musela mít každá dotčená osoba garantované právo předložit věc soudu.

Jakkoliv tento evropský systém ochrany osobních údajů představoval přístup v mnoha ohledech revoluční, v mezinárodním prostředí se jednalo navíc o dosud nevídaný koncept, relativně brzo se začaly ukazovat jeho vnitřní slabiny; šlo zejména o vysokou míru obecnosti této úpravy, s tím související nejednotný přístup k implementaci směrnice i jejímu odlišnému naplňování členskými státy, včetně sporných otázek týkajících se osobní i věcné působnosti navazujících národních legislativ, jakož i absence některých pravidel (např. předávání údajů do zahraničí apod.).[18]

Navzdory opakované kritice tohoto evropského pojetí systému ochrany však směrnice bezesporu položila široké základní schéma zásad zpracování osobních údajů a měla velký vliv na zákony v ostatních zeměpisných oblastech. Její nedostatky však vedly k přijetí nové evropské úpravy ve formě přímo použitelného nařízení Evropského parlamentu a Rady Evropy 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu údajů (dále jen „nařízení“, nebo též „GDPR“), které vstoupilo v účinnost dne 25. května 2018, čímž souběžně nepřímo nahradilo převážnou část související zákonné úpravy.

Oblast, která stojí na relativně nových principech, představuje zpracování velkých objemů dat (k problematice Big Data viz část VI.), včetně možnosti jejich automatizované analýzy, sdílení a navazujícího profilování, tj. především těch oblastí, které přinášejí současné komunikační a informační technologie, zejména pak neuronové sítě a související možnosti umělé inteligence či automatizovaného algoritmizovaného učení či rozhodování; právě tato oblast si jako jedna z mála zaslouží označení nová, byť nikoliv revoluční, navíc s možností širokého uplatnění v rámci téměř neomezeného spektra právních i společenských vztahů napříč většinou právních oborů.

---

[16] K tomu více viz KUNER, Ch. *The ‘Internal Morality’ of European Data Protection Law.* November 24, 2008. [online] [cit. 2019-12-08]. Dostupné z: <http://ssrn.com/abstract=1443797>.

[17] Z věcné působnosti této Směrnice bylo vyjmuto v zásadě pouze zpracování prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností a zpracování prováděné pro výkon činností, které nespadají do oblasti působnosti práva Unie (např. veřejná bezpečnost, obrana či bezpečnost státu).

[18] K tomu více viz např. KUNER, Ch. *The ‘Internal Morality’ of European Data Protection Law.* op. cit.

2.2 Formální podstata automatizovaného rozhodování ve světle ochrany subjektivních práv

Každé rozhodnutí realizované na základě algoritmů vyvolává ze své podstaty otázku, zda byla zachovávána subjektivní práva jednotlivce, případně zda byly při aplikaci zachovány také hodnoty, jež příslušná právní norma chrání. Nutno však nejprve určit, co se v tomto kontextu vlastně rozumí automatizovaným rozhodnutím. Ze své podstaty totiž jde o rozhodnutí, jež realizuje specifický software určitého výpočetního systému (tj. program a počítač), a to na základě zpravidla předem naprogramovaného autonomního programu a jemu přístupných dat; člověk a jeho vůle se tak na takovém rozhodnutí nepodílí,[19] a to z podstatné části. Nutno se tak zabývat možností, zda automatizace rozhodovacích procesů tohoto typu bude přinášet určité problémy v hodnocení konkrétních skutkových stavů, včetně samotné právní argumentace a kvalitního odůvodnění podstaty svých rozhodnutí. Klíčovým rozdílem je zde skutečnost, že samotnou rozhodovací autoritou je zde autonomní systém, jenž nemůže být z pohledu své (neexistující) právní osobnosti odpovědný, zatímco po osobě, která by odpovědnost nést (teoreticky) mohla, nelze toto spravedlivě požadovat, neboť nad konkrétní rozhodovací procedurou či samotnou podstatou věci nemá jakoukoliv přímou kontrolu.

Základním stavebním kamenem jakéhokoliv rozhodování ve výše uvedeném významu je především přesvědčivý a kvalitní výklad právních norem realizovaný ve formě důsledného odůvodnění svých rozhodnutí.[20] V rámci procesu rozhodování tak musí ten, kdo rozhoduje, aplikovat jak určité teoretické i praktické poznatky, tak i ve smyslu svých důsledků domýšlet reálný dopad svých rozhodnutí, včetně určitého preventivního působení takového rozhodnutí do budoucnosti. Samotný text právní normy je zcela jistě zásadním faktorem a klíčovým indikátorem směru interpretace, ale jistě nesmí být toliko jediným faktorem rozhodování.

U rozhodnutí realizovaných výlučně na základě algoritmů může existovat obava z určitého „předprogramovaného" formalismu, tj. stavu, kdy formální podstata rozhodnutí ve většině podstatných aspektů převáží nad věcnou správností rozhodnutí samotného. V tomto ohledu nutno připomenout, že i český Ústavní soud ve své judikatuře[21] opakovaně dovozuje, že netoleruje orgánům veřejné moci a především obecným soudům v řešení sporných případů příliš formalistický postup; zdůraznil přitom mj., že obecný soud není absolutně vázán doslovným zněním zákona, nýbrž se od něj smí a musí odchýlit, pokud to vyžaduje účel

[19] K tomu viz SVOBODA, P. et al. *Právní a daňové aspekty e-obchodu*. Praha: Linde Praha, 2001, 464 s.

[20] Ústavní soud konstatuje, že porušením práva na spravedlivý proces podle čl. 36 odst. 1 Listiny základních práv a svobod může být i situace, kdy v hodnocení skutkových zjištění absentuje určitá část skutečností, která vyšla v řízení najevo, event. nebo tím spíše – pokud ji účastník řízení namítal, nicméně obecný soud ji náležitým způsobem v celém souhrnu posuzovaných skutečností nezhodnotil, aniž by např. dostatečným způsobem odůvodnil jejich irelevantnost. Pokud obecný soud postupuje takto, dopouští se mj. i libovůle, zakázané v článku 2 odst. 2 Listiny základních práv a svobod. (Z nálezu Ústavního soudu sp. zn. I.ÚS 2232/07 ze dne 2. 6. 2010.)

[21] Např. nález sp. zn. Pl. ÚS 21/96, Sbírka nálezů a usnesení Ústavního soudu, svazek 7, nález č. 13, nebo nález sp. zn. 19/98, Sbírka nálezů a usnesení Ústavního soudu, svazek 13, nález č. 19.

zákona, historie jeho vzniku, systematická souvislost nebo některý z principů, jež mají svůj základ v ústavně konformním právním řádu jako významovém celku, a že povinnost soudů nalézat právo neznamená pouze vyhledávat přímé a výslovné pokyny v zákonném textu, ale též povinnost zjišťovat a formulovat, co je konkrétním právem i tam, kde jde o interpretaci abstraktních norem a ústavních zásad.

2.3 Rostoucí význam automatizovaného rozhodování, jeho praktické aspekty a možná rizika

Úvahy o automatizovaném právním rozhodování nepředstavují nic nového.[22] Odpovědné a efektivní rozhodování o subjektivních právech představuje jeden z důležitých úkolů vrchnostenské části veřejné správy. Tyto jednotlivé typy rozhodování se z celé řady důvodů odlišují svojí důležitostí, předvídatelností či časovým hlediskem, případně množstvím kritérií, jež je třeba odpovědně zvažovat. Všechny tyto atributy rozhodování mají vliv na to, zda dané rozhodování je svou podstatou způsobilé k automatizaci či nikoliv; ostatně i v současné době dochází k automatizovaným rozhodnutím v celém spektru společenského či průmyslového života, zejména pak v oblasti železniční či letecké dopravy, případně také autonomně řízených vozidel.

Automatizované rozhodování se tak používá ve stále větším počtu odvětví, lhostejno zda v oblasti soukromé, či veřejné. Bankovnictví a finance, zdravotní péče, zdanění, pojištění, marketing a reklama jsou jenom některé příklady oblastí, kde se profilování provádí pravidelněji s cílem pomoci při rozhodování. Technologický pokrok a schopnost analýzy dat velkého objemu, umělá inteligence a strojové učení usnadňují vytváření profilů a provádění automatizovaného rozhodování, přičemž mohou významně ovlivnit práva a svobody jednotlivců. Široká dostupnost osobních údajů na internetu a ze zařízení internetu věcí a schopnost nacházet vzájemné souvislosti a vytvářet vazby může vést k určení, analýze a odhadu aspektů týkajících se osobnosti, chování, zájmů a zvyklostí jednotlivců.

Kromě nesporně pozitivních dopadů na efektivitu celé řady právních rozhodovacích procesů, jež byly dosud především doménou lidské práce, lze očekávat i vytváření vysoce efektivních nástrojů směřujících k odosobněným (avšak o to více efektivním) sporným či dokonce negativním dopadům do práv a svobod jednotlivců. V důsledku automatizace těchto právních procesů se totiž rozhodování přesune o něco dále od člověka, dojde tak k určitému útěku od jeho odpovědnosti za rozhodnutí v konkrétních „živých“ věcech.

Všechny tyto aspekty tak ve svém souhrnu logicky povedou ke stále častějšímu využívání právně-rozhodovacích procedur realizovaných na základě algoritmizace, a to jak v oblasti

[22] Připomenout lze například i více než 50 let staré úvahy Knappovy, viz např. KNAPP, V. *O možnosti použití kybernetických metod v právu*. Praha: Nakladatelství Československé akademie věd, 1963, případně též úvahy pozdější, např. KNAPP, V. *Právo a informace*. Praha: Academia, 1988, 289 s.

práva procesního i hmotného, veřejného či soukromého, resp. smluvního.[23] Důsledkem bude tedy jak zrychlení samotné realizace práva, tak i vytvoření řady dalších nespecifických právních nástrojů, jež svými charakteristickými rysy mohou svádět k patologickému zneužití. Rozsah těchto možných využití či zneužití pak bude vyplývat z konkrétních zájmů, resp. hodnotových základů jednotlivých odvětví, v rámci kterých bude rozhodováno. Klíčovým kritériem pro jejich aplikaci bude rozměr lidskoprávní, neboť jejich extenzivní využívání může vést k tomu, že se používané algoritmy dostanou mimo možnost faktické kontroly ze strany člověka či společnosti (ve smyslu faktické regulace); v takovém případě mohou do určité míry začít žít svým vlastním životem. Jak k tomuto uvádí Bejček, byly již zdokumentovány případy, kdy se algoritmus výrazně odchýlil od původně zamýšlené role; výsledky pak překvapily i jeho samotné autory.[24]

Z oblasti práva soukromého lze dále uvést rozsáhle možnosti využití automatizovaného rozhodování v oblasti tzv. chytrých smluv, případně elektronické kontraktace založené např. na softwarových možnostech technologie blockchainu, jež se již v současnosti začínají prosazovat jak ke zvýšení rychlosti i celkové efektivity realizace zejména smluvní agendy. Nemalé možnosti automatizace rozhodování se rýsují rovněž v právu pracovním, a to zejména při zajištění požadavku na objektivitu a rovnost při odměňování, ochraně majetku zaměstnavatele, ochraně zdraví zaměstnanců, případně při kontrole pracovní výkonnosti zaměstnance; u posledního jmenovaného je však nutno pamatovat na rozdílný přístup literatury i judikatury,[25] jež sledování pracovní výkonnosti zaměstnance (a tedy i navazující automatizované rozhodování) silně limitují.[26] Obdobné využití může mít automatizované využití v právu veřejném, ať již podpůrně (viz dále) v právu deliktním, případně v právu hospodářské soutěže, kde, jak trefně uvádí např. Bejček,[27] je však na místě obezřetný právně politický přístup, a to tak, aby se nezhatil kladný potenciál této nové technologie.

Jedním z významných aspektů automatizovaného rozhodování je tak především požadavek zajistit efektivní a především transparentní možnost kontroly odpovědného provozovatele systému automatizovaného rozhodování nad jeho činností, stejně tak jako předvídatelnost a zpětnou verifikovatelnost jeho jednání; takové úvahy však výrazně přesahují zamýšlený rámec této publikace.

---

[23] K tomu viz též např. LESSIG, L. *Code V.2.* New York: Basic Books, 2006, 426 s.

[24] Např. automatizovaně počítaná cena vstupenek do lyžařského resortu Colorado se odvíjí od automaticky hlášeného množství sněhu, nebo že nápojové automaty mění ceny za nápoje podle vnější teploty. To může např. ve spojení s analýzou „Big Data" vést k vysoce sofistikované a individualizované cenové diskriminaci. Nedostatek lidské kontroly vedl i excesům, jako že učebnice o ovocných muškách kvůli interaktivním cenovým automatům používaným Amazonem stála až 23,7 mil. USD, nebo kdy naopak v důsledku chyby prodávaly United Airlines letenky za 5 USD. K tomu více viz BEJČEK, J. Chytré smlouvy jakožto smlouvy „chytře" protiprávní. In: SUCHOŽA, J. – HUSÁR, J. – HUČKOVÁ, R. *Právo Obchod Ekonomika IX*. Košice: UPJŠ v Košiciach, Právnická fakulta, 2019, s. 361–381.

[25] Viz BĚLINA, M. – DRÁPAL, L. a kol. *Zákoník práce: komentář.* Praha: C. H. Beck, 2012, 1616 s. Autorem příslušné části komentáře k § 316 je M. Štefko.

[26] K tomu více viz MATEJKA, J. Zaměstnanec jako objekt profilování a automatizovaného rozhodování dle obecného nařízení o ochraně osobních údajů. In: HROMADA, M. *Pocta Jarmile Pavlátové k 85. narozeninám*. Plzeň: Západočeská univerzita v Plzni, 2018, s. 87–104.

[27] K tomu více viz BEJČEK, J. *Chytré smlouvy jakožto smlouvy „chytře" protiprávní*. op. cit.

Část III. Biometrika a biometrické údaje

3.1 Biometrika první a druhé generace

Güttler a Matejka definují biometriku jako techniku nebo systém, který umožňuje strojovou identifikaci jednotlivce či umožňuje potvrdit jeho totožnost.[28] Podle nich se biometrika vztahuje k pojmu měřitelnosti, neboť se soustředí na měřitelné fyzické vlastnosti.[29] Biometrika se dělí na silnou, slabou a jemnou. Silná biometrika (*strong biometrics*) jsou rysy, které můžeme považovat za unikátní a v čase neměnné, jako jsou otisky prstů, otisk duhovky, struktura žil apod. Slabá biometrika (*weak biometrics*) nemá tak silný identifikační charakter jako silná biometrika a musí být vždy hodnocena podle kontextu, času nebo místa, kde se jednotlivec nachází. Do slabé biometriky řadíme znaky jako gesta, způsob chůze či dynamika obličeje. Za jemnou biometriku (*soft biometrics*) jsou označovány znaky, které nemohou být přiřazeny pouze určitému jedinci (barva očí, kůže, rasa nebo pohlaví).[30]

Literatura rozlišuje biometriku na biometriku první a druhé generace. Zatím co první generace biometriky si pokládala otázku, kdo jste, biometrie druhé generace si klade otázku, jak jste. Druhá generace biometriky se méně zabývá údaji, které se vztahují k identitě jednotlivce. Biometrika druhé generace se zaměřuje na vztah jednotlivce a prostředí tím, že se zaměřuje na úmysly jednotlivce a jejich projevy.[31]

„Druhá generace biometriky odkazuje na novou vlnu biometrických technologií, které mají za cíl přiblížit se k tomu, aby mohly napodobovat způsob, jakým se lidé identifikují a jak se sobě prokazují. To jest, prostřednictvím rozpoznání jednotlivých rysů a průběžné *analýzy jedinečné dynamiky těla, která může být zachycena v „reálném čase" a nenápadně ve smyslu, že nutně nevyžaduje, aby se jednotlivec zastavil u stroje, který umožňuje proces skenování. Tyto biometrie mají tendenci soustředit se na méně persistentní (slabší) rysy než standardní biometrie (jako jsou otisky prstů nebo skenování duhovky) a často mají sklony se měnit* v průběhu času. Ačkoli druhá generace *biometrie směřuje na rysy, které jsou*

[28] GÜTTLER, V. – MATEJKA, J. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*. 2016, roč. 155, č. 12, s. 1036.
[29] MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The Ethical, Legal and Social Context.* Dordrecht: Springer, 2011, s. 7.
[30] Ibid., s. 9.
[31] Ibid., s. 11.

nestabilní a méně rozlišující, mohou být úspěšně využity k jakémukoli druhu rozpoznávání, od autentizace, identifikace až po screening, zvláště v případě, že několik biometrických prvků je spojeno do multimodálního systému, který zohledňuje najednou několik různých biometrických prvků."[32]

Biometrika, která se vztahuje k vyhodnocování a měření charakteristik člověka souvisejících s jeho vědomým či nevědomým chováním nebo jednáním, se nazývá behaviorální biometrikou. Na jejím základě lze osobu nejen identifikovat nebo ověřit její totožnost, ale také určit její rozpoložení a úmysly. Profily vytvořené s pomocí behaviorální biometriky se nazývají behaviorální biometrické profily.[33]

Na podkladě biometriky první a druhé generace můžeme rozlišit biometrické údaje na biometrické údaje v širším a užším smyslu. Biometrickými údaji v širším smyslu jsou údaje, které jsou výstupem systému využívajícího technologii založenou na biometrice. Tyto údaje nemusí nutně identifikovat jednotlivce, ale vypovídají o jeho chování a možných úmyslech. Biometrickými údaji v užším smyslu jsou údaje, jež umožňují identifikaci osoby. Takto biometrické údaje definuje GDPR. Podle čl. 4 bodu 14 jsou biometrickými údaji osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje. Biometrické údaje za účelem jedinečné identifikace fyzické osoby jsou dle čl. 9 GDPR citlivými údaji neboli podle terminologie GDPR zvláštními kategoriemi údajů. Stejně definuje biometrický údaj i čl. 3 bod 13 směrnice 2016/680 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.

3.2 Identifikace biometrickými systémy

Pokud údaj (např. kamerový záznam, který je v reálném čase vyhodnocen algoritmem) neumožňuje nebo nepotvrzuje jedinečnou identifikaci osoby, bude se v případě takového údaje jednat o osobní údaj, nicméně již ne o údaj biometrický v užším smyslu, tedy o biometrický údaj ve smyslu GDPR. I když se však v takovém případě nebude jednat o biometrický údaj podle GDPR, jedná se o osobní údaj podle čl. 4 bodu 1 tohoto nařízení, neboť osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat. Soudní dvůr Evropské unie (dále jen: „SDEU") v případu *Breyer*[34] dovodil, že pro určení, zda

[32] MORDINI, E. – ASHTONS, H. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The ethical, Legal and Social Context*. Dordrecht: Springer, 2011, s. 262.

[33] YANNOPOULOS, A. – ANDRONIKOU, V. – VARVARIGOU, T. Behavioural Biometric Profiling and Ambient Intelligence. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008, s. 90.

[34] Rozsudek SDEU ze dne 19. října 2016, věc C-582/2014 (*Breyer*).

je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. SDEU cituje ve svém rozsudku stanovisko generálního advokáta k výše uvedenému případu, který uvedl, že se nejedná o situace, kdy by identifikace subjektu údajů byla zakázána zákonem nebo by byla prakticky neproveditelná, například z důvodu skutečnosti, že by vyžadovala nepřiměřené úsilí z časového hlediska a z hlediska ekonomických a lidských zdrojů.

Argumentem *a contrario* lze dovodit, že osoba je identifikovatelná, pokud je identifikace zákonem dovolená či prakticky proveditelná, tedy že nevyžaduje ze strany správce nepřiměřené úsilí. Osoba, jejíž chování je na základě vyhodnocení algoritmem shledáno jako možné riziko pro majetek, život nebo zdraví jiných osob, může být odpovědnými osobami oslovena a identifikována. O biometrický údaj v užším smyslu by se jednalo za situace, kdy chování jednotlivce by bylo tak charakteristické, že by se přímo z tohoto chování, nebo zároveň ve spojení s fyziognomickými rysy, dala určit identita této osoby. K určení osoby by mohly sloužit i fotografie uložené v databázi přístupné správci osobních údajů. Recitál 51 GDPR stanoví, že na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby. Vztahuje-li se na zpracování biometrických údajů GDRP, je správce povinen tyto údaje zpracovávat v souladu s GDPR.

Nařízení se dle čl. 2 nevztahuje na zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Unie nebo které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU. První výjimka se vztahuje na zpracování osobních údajů v souvislosti se zajištěním bezpečnosti členských států, druhá na výkon společné zahraniční a bezpečnostní politiky Unie. Čl. 23 GDPR stanoví, že právo Unie nebo členského státu může prostřednictvím legislativního opatření omezit rozsah povinností správce nebo zpracovatele a práv subjektů údajů s cílem zajistit mimo jiné národní a veřejnou bezpečnost či prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti. Možnost takového omezení využila České republika formou adaptačního zákona k GDPR, a to konkrétně v ustanovení § 5 zákona č. 110/2019 Sb., o zpracování osobních údajů.

V oblasti ochrany národní a veřejné bezpečnosti se biometrika využívá ve stále větší míře. V tomto smyslu se mluví o *biometric-enabled intelligence* čili o zpravodajství umožněném biometrikou. Tento druh zpravodajství je zaměřen na identifikaci podezřelé osoby na základě jeho fyziologických charakteristik.[35] Biometrii využívá řada nadnárodních organizací jako INTERPOL, EUROPOL nebo NATO.[36] Ve spojení s biometrií se hovoří i o konceptu

[35] HU, M. Biometric Cyberintelligence and the Posse Comitatus Act. *Emory Law Journal*. 2017, Vol. 66, No. 4, s. 704.

[36] MORRIS, V. R. Identity and Biometrics Enabled Intelligence (BEI) Sharing for Transnational Threat Actors. *Small Wars Journal* [online]. 22. 3. 2016 [cit. 2018-02-01]. Dostupné z: <http://smallwarsjournal.com/jrnl/art/identity-and-biometrics-enabled-intelligence-bei-sharing-for-transnational-threat-actors>.

zpravodajství založeném na identitě (*Identity Intelligence*). Toto zpravodajství je založené na atributech identity, jako jsou atributy biologické, biografické, behaviorální, jakož i informace o pověsti a další informace shromážděné ve všech zpravodajských disciplínách. Jako u každé zpravodajské činnosti je cílem odhalení neznámých potenciálních hrozeb spojením jednotlivců s jinými osobami, místy, událostmi nebo materiály, analyzováním způsobu života a charakterizováním úrovně potenciálních hrozeb.[37]

[37] Ibid.

Část IV. Algoritmy a jejich využití

4.1 Pojem algoritmizace

Systémy pro vyhodnocování biometrických údajů využívají zpravidla algoritmů.[38] Slovo algoritmus pochází odvozením ze jména perského matematika Al-Chorezmího a znamená metodu systematického a automatizovaného výpočtu. Algoritmus je soubor příkazů, které musí být provedeny, aby se dosáhlo požadovaného výsledku nebo řešení. Algoritmus funguje pouze tehdy, pokud přesně známe faktory, které chceme algoritmem řešit.[39] Pro tvorbu algoritmu, který určuje hodnotu opce akcií, je třeba vědět, že cena závisí na proměnlivosti ceny akcií, úrokové míře a na realizační ceně opce, tedy na ceně, za kterou může vlastník opce tuto opci uplatnit.[40] Základními vlastnostmi algoritmu jsou konečnost, určitost, vstup, výstup a efektivita. Konečnost znamená, že algoritmus končí po vykonání konečného počtu kroků. Určitostí neboli též jednoznačností se rozumí skutečnost, že každá operace musí být přesně určena. Každý algoritmus musí mít na začátku určitý počet vstupů, které jsou zadány před jeho započetím nebo v průběhu. Výstupem se pak rozumí veličina mající vztah ke vstupům. Poslední vlastností je efektivita, jež znamená jednoduchost prováděných operací, aby je bylo možno provést přesně a za konečnou dobu.[41]

V současné době bývá analytická práce nejrůznějšího charakteru vykonávána pomocí algoritmů, které automatizují nejrůznější činnosti dříve vykonávané člověkem.[42] Zakladatel kybernetiky Norbert Wiener mluví o tomto typu mechanizace jako o typu nahrazujícím lidské rozhodování. Přestože Wiener nepředpokládal, že je možné nahradit složité rozhodování člověka s mnoha proměnnými rozhodováním mechanizovaným,[43] ukázalo se, že opak je pravdou, neboť mechanizované rozhodování je přítomno ve všech oblastech běžného života.[44]

---

38 Např. REVETT, K. *Behavioral Biometrics. A Remote Access Aproach*. Hoboken: Wiley, 2008, s. 1.
39 STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*. London: Penguin Books, 2012, s. 50.
40 Ibid., s. 57.
41 KNUTH, D, E. *Umění programování. 1. díl. Základní algoritmy*. Brno: Computer press, 2008, s. 5.
42 STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World.* op. cit., s. 15.
43 WIENER, N. *The Human Use of Human Beings: cybernetics and society*. London: Free Association Books, 1989, s. 159.
44 STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World.* op. cit., s. 41.

Podle Kate Crawford se algoritmy často rozumí výpočetní nástroj, který autokraticky rozhoduje mezi proměnnými a vytváří jeden výstup. Tento pohled, jenž se zaměřuje výhradně na okamžik, kdy algoritmus vytváří výsledek, opomíjí komplexnější chápání toho, jak algoritmy fungují. Důsledkem toho je, že výstupy jsou považovány za racionální, oproštěné od subjektivních představ a požadavků.[45]

„Algoritmy mohou být mechanismy založené na pravidlech, které plní úkoly, ale jsou také řídícími mechanismy, které vybírají mezi konkurenčními a někdy i konfliktními daty. To, co vidíme, je jediný výsledek, nebo pečlivě uspořádaný výběr, který odpovídá našim preferencím a předchozímu chování. Velká část z toho, jak algoritmus funguje, spočívající v určení vítěze informační soutěže, nám zůstává skryta. Kritéria, podle nichž algoritmy provádějí hodnocení, jsou neznámá, přestože tyto přijímají politická rozhodnutí o vhodném a legitimním poznání.“[46]

4.2 Gillespieho šest dimenzí algoritmů

Tarleton Gillespie hovoří o algoritmech s veřejným významem (*public relevance algorithms*). Tyto algoritmy vybírají z dat o preferencích, aktivitách a výrocích ty nejvhodnější informace, které jsou poté uživateli ve formě výsledku prezentovány. Výsledky představují vědění, které je pro uživatele srovnatelné s vědeckými výsledky, názory expertů nebo s vlastním rozumem.[47] Přestože se Gillespieho algoritmy týkají hlavně algoritmů využívaných vyhledávači a sociálními sítěmi, lze některé z vlastností těchto algoritmů vztáhnout i na algoritmy, které vyhodnocují biometrické údaje, přiřazují je k behaviorálním biometrickým profilům a prezentují výsledky odpovědným osobám nebo systému, aby spustily odpověď na detekovanou situaci. Gillespie rozeznává šest dimenzí algoritmů s veřejným významem. Těmito dimenzemi jsou vzorce pro začlenění (*patterns of inclusion*), koloběh očekávání (*cycles of anticipation*), zhodnocení důležitosti (*evaluation of relevance*), příslib objektivity algoritmu (*promise of algorithmic objectivity*), začlenění do praxe (*entanglement with practice*) a publikum vytvořené výpočtem (*production of calculated publics*).[48] Pro algoritmy hodnotící chování jednotlivce a další biometrické údaje je relevantní dimenze spočívající ve zhodnocení důležitosti příslibem objektivity a začleněním do praxe, tedy třetí, čtvrtá a pátá dimenze algoritmu.

Zhodnocení důležitosti spočívá v kritériích, podle nichž algoritmy určují, co je přesně pro danou situaci, kontext, prostředí a čas relevantní. Tvůrce algoritmu musí zjistit, které proměnné jsou z hlediska požadovaného výsledku důležitější než jiné a jaká data jsou bezvýznamná. Aby prediktivní algoritmy správně fungovaly, je třeba, aby bezvýznamná data

[45] CRAWFORD, K. *Can An Algorithm be Agonistic? Scenes of Contest in Calculated Publics* [online]. 2016, s. 2 [cit. 2016-04-30]. Dostupné z: <http://www.katecrawford.net/docs/CanAnAlgorithmBeAgonistic-Ap>.

[46] Ibid., s. 5.

[47] GILLESPIE, T. *The relevance of algorithms* [online]. 2012, s. 2 [cit. 2016-04-30]. Dostupné z: <http://www.tarletongillespie.org/essays/Gillespie%20-%20The%20Relevance%20of%20Algorithms.pdf>.

[48] Ibid., s. 2.

ignorovaly, a naopak aby se koncentrovaly pouze na relevantní skutečnosti. Hodnocení toho, jaké skutečnosti jsou relevantní, se provádí pomocí analýzy dat. Nejběžnější způsob analýzy dat se nazývá regresní analýza. Díky této technice lze činit předpovědi na základě údajů získaných v minulosti.[49]

Po zadání dotazu musí algoritmus vyhodnotit data tak, aby naplnil kritéria požadavku zadaného uživatelem algoritmu. *„Protože neexistuje nezávislý vzorec pro to, co jsou ve skutečnosti relevantní výsledky pro každý jednotlivý dotaz, musí inženýři rozhodnout, jak výsledky vypadají, že jsou ty ‚správné', a vyladit svůj algoritmus tak, aby tohoto výsledku dosáhly, nebo provést změny založené na důkazech od uživatelů a nakládat s rychlým kliknutím a s absencí následného vyhledávání jako s přiblížením se ne přímo relevantnosti, nýbrž uspokojení."*[50]

Čtvrtou dimenzí algoritmů s veřejným významem je příslib objektivity algoritmu čili způsob, jak je zajištěna nestrannost algoritmu a jak je tento požadavek zaručen. U algoritmů bývá zdůrazňována objektivita a nestrannost výsledků. Objektivita výsledků nabídnutých uživateli na základě algoritmu je však v přímém rozporu se zhodnocením pro uživatele relevantních informací, jak bylo popsáno výše. Tento rozpor Gillespie nazývá zásadním paradoxem ve formulaci algoritmu. Poskytovatelé poukazují na technickou podstatu výstupů, která je automatizovaná, a tudíž objektivní, zatímco postupem, jenž není veřejnosti znám, anticipují relevanci těchto výstupů pro uživatele a rozhodují tak o tom, jaké výstupy jsou uživatelům algoritmu zobrazeny.[51] V případě prediktivního algoritmu bude na základě výstupů poté s uživatelem nebo systémem jednáno.

Pátou dimenzí je dle Gillespieho začlenění do praxe, jímž se rozumí to, jak uživatelé mění své chování, tak aby vyhovovalo algoritmu, na kterém závisí. Uživatelé výsledků algoritmu nebo třetí osoby, jež mohou výstupy algoritmu ovlivnit, mají povědomí o tom, že jejich chování může ovlivnit informace, které se na základě algoritmu jeho uživatelům zobrazí. *„Protože jsou tyto algoritmy zakořeněny v každodenním životě lidí a jejich běžných informačních praktikách, uživatelé utvářejí a přetvářejí algoritmy, s nimiž se setkávají. Algoritmy mají dopad na to, jak lidé hledají informace, jak vnímají a přemýšlí o vědomostech a o tom, jak chápou sami sebe ve veřejném diskursu a skrze něho."*[52] Změna chování se v případě prediktivních algoritmů nebude týkat uživatelů, ale osob, jejichž chování je systémem sledováno a vyhodnocováno.

[49] STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World.* op. cit., s. 57.
[50] GILLESPIE, T. *The relevance of algorithms.* op. cit., s. 9.
[51] Ibid., s. 16.
[52] Ibid., s. 17.

4.3 Informační asymetrie v oblasti algoritmického rozhodování

Přestože kritéria, na jejichž základě algoritmus generuje výsledky, jsou často neznámá, jednotlivci s algoritmy při svém jednání mohou počítat, např. na základě informací o přítomnosti takových systémů v určitém prostoru, a své chování optimalizovat tak, aby pro ně byl výsledek co možná nejpřijatelnější nebo nejvhodnější. Existují zde dva typy informační asymetrie.

Za první typ asymetrie lze považovat asymetrii mezi poskytovateli algoritmu a případně dalšími osobami, které se na vývoji a fungování algoritmu podílejí, a třetími osobami, ať již uživateli nebo jednotlivci, vůči nimž tito uživatelé na základě výsledků generovaných algoritmem určitým způsobem jednají. Druhým typem asymetrie je asymetrie mezi uživateli algoritmu nebo výše uvedenými jednotlivci, kteří dokáží své jednání přizpůsobit kritériím pro fungování algoritmu daným poskytovatelem, a těmi, kteří přizpůsobit své jednání nedokáží, neboť nedisponují potřebnými znalostmi či informacemi, nebo přizpůsobit své jednání nechtějí nebo nemohou. Brunton a Nissenbaum hovoří spíše než o přizpůsobení se o obejití systému (doslova mlžení – *obfuscation*), protože jiná řešení jako vyhnutí se nebo skrytí se nejsou k dispozici (nelze využít tzv. možnosti *opt-out*).[53]

Obejití systému podle Bruntona a Nissenbaum představuje strategie pro zmírnění dohledu, analýzu dat a jejich profilování. Obejití systému má za cíl učinit dohled, analýzu nebo profilování méně jednoznačné, matoucí, a tudíž z hlediska použitelnosti méně hodnotné. Algoritmus vyhodnocuje údaje o chování jednotlivce. Některé výstupy, které se na základě výsledku zobrazí, nemusí být zobrazeny pouze na základě vstupních dat detekovaných systémem v určitém kontextu, ale i výsledkem profilování, jehož podkladem je nejen výsledek týkající se určitého jednotlivce, ale celé skupiny osob, jež byly poskytovatelem zařazeny do stejné kategorie, kupříkladu podle pohlaví nebo barvy pleti.

[53] BRUNTON, F. – NISSENBAUM, H. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* [online]. 2011, Vol. 16, No. 5. [cit. 2016-05-08]. Dostupné z: <http://firstmonday.org/article/view/3493/2955>.

Část V. Algoritmický dohled a rozhodování

5.1 Pojem a význam algoritmického dohledu

Policie a bezpečnostní složky, které střeží letiště, nádraží, jiné dopravní uzly, hraniční a jiná místa, mohou díky technologiím v reálném čase hodnotit chování jednotlivců a odhadnout, zda se v místě nenachází osoba, která má v plánu spáchat teroristický útok nebo jiný trestný čin proti životu a zdraví, proti majetku nebo jiným chráněným hodnotám. Jedná se o dohled, při kterém algoritmus vyhodnocuje jednotlivce potenciálně rizikové pro veřejnou a národní bezpečnost.

Dohled je systematické monitorování jednání a komunikace jedné nebo více osob.[54] Dohled slouží k monitorování jednotlivce, k dohledu nad jeho chováním. Dohled, především dohled státu nad svými občany, není novým fenoménem, který by vznikl až s rozvojem informačních a komunikačních technologií. Tyto technologie dohled usnadnily a rozšířily. Zároveň se kvůli technologiím stal dohled pro jednotlivce méně viditelným.[55] Poté, co Edward Snowden zveřejnil rozsah dohledu americké Národní bezpečnostní agentury, který zahrnoval sběr a analýzu telefonních hovorů a internetového provozu ve Spojených státech a mezi Spojenými státy a zahraničím,[56] je většinová společnost informována o existenci dohledu ze strany státu.[57] Přesto stále sofistikovanější formy dohledu znemožňují jednotlivcům předvídat, kdy a jakým způsobem bude nad nimi dohled vykonáván.

Koops nazývá současnou společnost společností kriminální. Znakem této společnosti je její senzitivita ve vztahu k riziku, jež doba přináší.[58] *„Přestože většina lidí by racionálně souhlasila s tím, že ne všechna rizika mohou být eliminována, a to ani tehdy, pokud by k tomu*

---

54 CLARKE, R. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* [online]. 1997 [cit. 2014-06-15]. Dostupné z: <http://www.rogerclarke.com/DV/Intro.html#InfoPriv>.

55 LYON, D. *The Electronic Eye: the Rise of Surveillance Society*. Minneapolis: University of Minneapolis Press, 1994, s. 40.

56 Např. MORNIN, J. D. NSA Metadata Collection And The Fourth Amendment. *Berkeley Technology Law Journal* [online]. 2014, Vol. 29, s. 985 [cit. 2016-03-15]. Dostupné z: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2042&context=btlj>.

57 Public Perceptions of Privacy and Security in the Post-Snowden Era, *Pew Research Center* [online]. 12. 11. 2014 [cit. 2014-05-14]. Dostupné z: <http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf>.

58 KOOPS, B.-J. Technology and the Crime Society: Rethinking Legal Protection. *Selected Works* [online]. 2009, s. 16 [cit. 2014-05-14]. Dostupné z: <http://works.bepress.com/bert_jaap_koops>.

byly dostupné neomezené prostředky, noviny a parlamentní debaty mají tendenci zveličovat nehody, katastrofy a útoky a následně požadovat všechny možné kroky, aby se těmto škodám v budoucnosti zabránilo [...]. Formovat společenský vývoj z hlediska rizika a touhy a eliminovat nebezpečí tak, jak to jen lze, téměř nezbytně vede ke kultuře kontroly.“[59]

Dohled reaktivní je nahrazován dohledem proaktivním. Jednotlivec je na základě profilování, které může mít i podobu biometrického behaviorálního profilování, zařazen do skupiny osob představující potenciální riziko pro bezpečnost nebo veřejný pořádek. Na podkladě profilu je pak tento jednotlivec vystaven dohledu ze strany státu. Tento jev nazývají Mayer-Schönberger a Curkier vinou na základě asociace.[60]

Ideální model dohledu popsal francouzský filozof Michel Foucault ve svém díle Dohlížet a trestat. Foucault převzal Bethamův model vězení s transparentními celami. Vězni v takových celách mohou, ale nemusí být pozorováni dozorcem. Vězeň sám dozorce nevidí. Podstatný rys panoptika je nevědomost vězně o tom, zda je v konkrétním okamžiku pozorován, či nikoliv. Strach z dohledu vězně nutí chovat se podle pravidel. Foucault na základě výše popsaného modelu popisuje mechanismus fungování společnosti založené na disciplíně a poslušnosti. Cílem není trestat, ale normalizovat.

Podle Lyona je panoptikum jedním z modelů dohledu. *„Díky architektuře elektronických technologií, jejichž prostřednictvím se dnes moc rozděluje v proměnlivých a mobilních organizacích, je architektura zdí a oken do značné míry nadbytečná [...]. Tato architektura umožňuje kontrolu s jinou tváří. Nejenže nepřipomíná vězení; často má rysy flexibility a rozmary, jak je známe z oblasti zábavního průmyslu a spotřeby.“*[61]

Zatímco tvrdá podoba panoptika vyvolává mezi sledovanými pocity odporu a ofenzívy, dohled beze zdí tyto pocity nevyvolává. Tato forma dohledu implikuje větší míru poslušnosti.[62] Podle Zygmunda Baumana je dnešní svět post-panoptický. V post-panoptickém světě se stírají rozdíly mezi dohlížiteli a těmi, nad nimiž je dohled vykonáván.[63]

Podle Marxe se podstata moderního dohledu změnila v tom, že namísto sledování specifického subjektu dochází ke sledování celé kategorie subjektů, neboť celá kategorie je podezřelá.[64] Data získaná sledováním chování mohou být analyzována a spojována dlouhou dobu poté, co byla o jednotlivcích pořízena.[65]

---

59 Ibid., s. 7.

60 MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big Data: a revolution that will transform how we live, work and think*. London: John Murray, 2013, s. 160.

61 BAUMAN, Z – LYON, D. *Tekutý dohled*. Olomouc: Broken Books, 2013, s. 16.

62 Ibid., s. 60.

63 BAUMAN, Z. *Liquid Modernity*. Cambridge: Polity Press, 2002, s. 11.

64 MARX, G. T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988, s. 218.

65 Ibid., s. 217.

Pro současný typ dohledu se někdy namísto pojmu *surveillance* používá pojem überveillance.[66] *Überveillance* je všudypřítomný a trvalý dohled osob a objektů. Überveillance je umožněn datafikací čili převodem lidského chování, emocí, fyziologických procesů a dalších biometrických i nebiometrických aspektů lidské existence na data, jež jsou uložena v databázích a následně analyzována.[67]

5.2 Systémy dohledu

Algoritmickým dohledem je podle Lucase Introneho a Davida Wooda takový dohled, který postupuje automaticky dle přesně daných instrukcí. Algoritmický dohled může být vyjádřen i tak, že se jedná o technologie dohledu, jež využívají počítačové systémy, které poskytují odpovědným osobám již pomocí algoritmu zpracovaná data. Výsledkem je zobrazení shody mezi zaznamenanými daty a daty uloženými v databázi. Jiné systémy jsou schopné předvídat na základě zaznamenaných dat budoucí události.[68]

Tyto systémy dohledu jsou využívány policií a jinými bezpečnostními složkami ke třem základním účelům. Prvním z nich je účel prevence a bezpečnosti na určitých místech nebo při určitých událostech. Dalším účelem je shromažďování informací. Shromažďování informací se děje nejen prostřednictvím stabilních CCTV kamer, které monitorují lidské chování, ale i kamer dočasných nebo mobilních. Třetím základním účelem je vyšetřování, ke kterému většinou nedochází v reálném čase, ale až analýzou shromážděných dat.[69] Překážkou rozvoje a sdílení dat je ovšem v současné době nedostatečná standardizace těchto systémů. Kupříkladu u kamer CCTV by se standardizace měla týkat formátu, v němž jsou data shromážděna, podmínek, za kterých je záznam proveden (nastavení polohy kamer, jejich úhel, standardní přiblížení zaznamenávaného objektu, lokalizace kamery pomocí GPS apod.), synchronizace dat, která jsou zaznamenána s případnými varovnými signály při vyhodnocení rizika, formátu a protokolu přenosu obsahu záznamu a pravidel pro zabezpečení a ověření pravosti obsahu, která by mimo jiné umožňovala použití dat jako důkazu v soudním řízení.[70]

Systémy dohledu pomocí kamer CCTV se v současné době neomezují pouze na monitorování osob a událostí třeba i v reálném čase. Tyto systémy jsou propojeny se softwarem,

---

66 MICHAEL, MG – MICHAEL, K. A Note on "Überveillance". In: MICHAEL, MG. *The Second Workshop on the Social Implications of National Security. From Dataveillance to* Überveillance *and the Realpolitik of the Transparent Society* [online]. 2007, s. 10 [cit. 2014-08-14]. Dostupné z: <http://works.bepress.com/cgi/viewcontent.cgi?article=1050&context=kmichael>.

67 MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big data: a revolution that will transform how we live, work and think*. op. cit., s. 78.

68 INTRONA, L. D. – WOOD, D. Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance & Society* [online]. 2004, Vol. 2, No. 2/3, s. 181 [cit. 2016-05-13]. Dostupné z: <http://www.surveillance-and-society.org/cctv.htm\nhttp://eprints.lancs.ac.uk/28931/>.

69 MARRAUD, D. – CÉPAS, B. – SULZER, J.-F. – MULAT, Ch. – SÈDESA, F. Posteriori Analysis for Investigative Purposes. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, s. 34.

70 Ibid., s. 37.

který analyzuje shromážděná data na základě algoritmu. Na podkladě nasnímaných obrazů algoritmus porovná databázi fotografií za účelem rozpoznání obličeje nebo celé postavy, a to i ve 3D technologii.[71] Zobrazení postavy ve 3D včetně jejího postoje v reálném čase poskytuje přesné informace o aktivitě jednotlivce a jeho případných sociálních interakcích s okolím.[72] Pomocí algoritmu je hodnoceno i chování osoby v reálném čase, které je snímáno kamerovým systémem. Systém dokáže předvídat budoucí pravděpodobné jednání osoby.[73] Pokud systém vyhodnotí chování jako podezřelé, jelikož je schopen rozlišit „běžné" a „neběžné" chování osoby na určitém místě, jsou ihned uvědoměny osoby odpovědné za bezpečnost sledovaného prostoru.[74]

Algoritmus dokáže vyhodnotit, kdo je potenciální terorista, nicméně není vyloučena ani falešně pozitivní identifikace osoby jako domnělého teroristy.[75] Systém může dokonce vyhodnotit, který algoritmus je v dané situaci nejvhodnější, a pomocí něho monitorovat danou situaci. Pokud je takový systém použit kupříkladu na letišti, může identifikovat a monitorovat konkrétní jednotlivce či rozpoznat předměty, které nevypadají obvykle nebo se nacházejí na neobvyklých místech. Systém může detekovat určité osoby a předměty, když se objeví na monitorovaném místě, jakož i umí vyhodnotit situace, kdy se osoby nebo předměty pohybují nebo jsou přemisťovány určitým způsobem, jenž může být pro bezpečnost daného místa potenciálně rizikový.[76]

Výhodou těchto systémů je kromě zvýšení bezpečnosti osob nacházejících se na monitorovaných místech a rychlejšího zásahu bezpečnostních složek i rychlejší odbavení cestujících, jelikož systém rozpozná jejich obličeje,[77] v důsledku čehož nebudou cestující nuceni předkládat při různých fázích odbavování cestovní doklad. Namísto fyzické kontroly cestovních dokladů by byly např. u příchodu k letadlům, tzv. gatům, kontrolovány pouze obličeje cestujících a následně srovnávány s fotografiemi z cestovního dokladu uloženého

---

71 Srov. MILLER, M. I. —VAILLANT, M. – HOFFMAN, W. – SCHUEPP, P. 2D-to-3D Systems Face Recognition. In: VOELLER, J. G. *Detection and Intelligent Systems for Homeland Security (1)*. Somerset, US: Wiley, 2014, s. 1.

72 LIEM, M. – GAVRILA, D. M. Person Appearance Modeling and Orientation Estimation using Spherical Harmonics. *Proc. of the IEEE International Conference on Automatic Face & Gesture*, Shanghai [online], China, 2013, s. 1 [cit. 2016-05-27]. Dostupné z: <https://www.informationsystems.foi.se/main.php/Person-Appearance-Modeling-and-Orientation-Estimation-using-Spherical-Harmonics.pdf?fileitem=7340161>.

73 KOOIJ, J. F. P. – ENGLEBIENNE, G. – GAVRILA, D. A Non-parametric Hierarchical Model to Discover Behavior Dynamics from Tracks. *Proc. of the European Conference on Computer Vision* [online], Vol. 6, Florence, Italy, 2012, s. 270 [cit. 2016-05-27]. Dostupné z: <https://www.informationsystems.foi.se/main.php/A-Non-parametric-Hierarchical-Model-to-Discover-Behavior-Dynamics-from-Tracks.pdf?fileitem=7340168>.

74 WACHS, M. – FINK C. N. Y. – LOUKAITOU-SIDERIS A. – TAYLOR B. D. *Securing Public Transit Systems.* op. cit, s. 158.

75 KOOIJ, J. F. P. – ENGLEBIENNE, G. – GAVRILA, D. *Non-parametric Hierarchical Model to Discover Behavior Dynamics from Tracks*. op. cit., s. 279.

76 KNIGH, H. System improves automated monitoring of security cameras. New approach uses mathematics to reach a compromise between accuracy, speed. *MIT News* [online]. 5. 6. 2012 [cit. 2016-06-01]. Dostupné z: <http://news.mit.edu/2012/auto-video-surveillance-algorithm-0605>.

77 RAGHAVENDRA, R. – BUSCH, Ch. Improved Face Recognition by Combining Information from Multiple Cameras in Automatic Border Control System. *12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* [online], 2015, s. 1 [cit. 2016-06-01]. Dostupné z: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7301748&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F7295687%2F7301715%2F07301748.pdf%3Farnumber%3D7301748>.

v databázi.[78] Systém, kde cestující projde tunelem, v němž budou snímány jeho biometrické údaje za účelem jeho identifikace a rychlejšího odbavení nebo naopak detailnější kontroly, se připravuje kupříkladu na mezinárodním letišti v Dubaji.[79] Postoj osob podrobených dohledu v určité lokalitě je ambivalentní. Těmto osobám vadí, že jsou předmětem dohledu. Zároveň se však cítí bezpečněji, jelikož si uvědomují možnost teroristického útoku nebo jiné kriminální aktivity, obzvlášť v místech, kde je vysoká koncentrace osob.[80] Systém nemusí upozornit odpovědné osoby pouze ve výše uvedených případech. Upozornění může systém odeslat, i pokud detekuje žebrající osobu nebo chování jednotlivce, u něhož je podezření, že má v plánu spáchat sebevraždu.[81]

Požadavkem na přesné zobrazení požadovaných výstupů je znalost vstupních dat. Těmi jsou informace o objektu zájmu, o možných scénářích událostí a o operátorech. Informací o objektu zájmu jsou informace o zóně, kde se dohled vykonává, o osobách a předmětech, jež se v této zóně nacházejí nebo mohou nacházet, případně o jejich umístění nebo aktivitách.[82] Pokud systém vyhodnotí určitou osobu jako rizikovou, může být taková osoba z místa výkonu dohledu vykázána, může být u ní provedena bezpečnostní prohlídka či důkladnější bezpečnostní prohlídka, než je tomu u jiných osob, nebo může být dokonce omezena na osobní svobodě.

Dalšími informacemi na vstupu jsou informace o aktivitách, které mají být předmětem dohledu. Pokud je v místě dohledu detekována určitá předem definovaná aktivita, systém se může sám na danou aktivitu detailněji zaměřit, např. jejím přiblížením, nebo spustí alarm.[83] Pokud není možné dostatečně definovat aktivity, které jsou předmětem dohledu, je třeba definovat alespoň operátory, které zaznamenají atributy sledovaného místa, např. skutečnost, že se objekt nachází ve sledované zóně, či mimo ni, že se překrývá s jiným objektem nebo že se v zóně nachází jeden objekt ve spojení s dalším objektem.[84]

Předmětem dohledu nemusí být všechny osoby ve stejné míře. Zvýšený dohled je vykonáván nad těmi osobami, u kterých algoritmus na základě vstupních dat může předpokládat zvýšené riziko pro jejich příslušnost k určité národnosti nebo sociální či etnické skupině.[85]

---

[78] SPREEUWERS, L. J. – HENDRIKSE, J. A. – GERRITSEN, K. J. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport. *Biometrics Special Interest Group (BIOSIG) – Proceedings of the International Conference* [online]. 2012, s. 99 [cit. 2016-06-01]. Dostupné z: <http://cs.emis.de/LNI/Proceedings/Proceedings196/99.pdf>.

[79] THUY, O. Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints. *The Verge* [online]. 10. 10. 2017 [cit. 2018-02-24]. Dostupné z: <https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium>.

[80] WACHS, M. – FINK, C. N. Y. – LOUKAITOU-SIDERIS, A. – TAYLOR, B. D. *Securing Public Transit Systems*. op. cit., s. 158.

[81] VELASTIN, S. A. – BOGHOSSIAN, B. A. – PING LAI LO, B. – SUN, J. – VICENCIO-SILVA, M. A. PRISMATICA: Toward Ambient Intelligence in Public Transport Environments. *IEEE Transactions On Systems, Man, and Cybernetics—Part A: Systems and Humans* [online]. 2005, Vol. 35, No. 1, s. 179 [cit. 2016-06-01]. Dostupné z: <http://ids.snu.ac.kr/w/images/9/9e/AmI04.pdf>.

[82] BOULAY, B. – BRÉMOND, F. Activity Recognition. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, s. 207.

[83] Ibid., s. 209.

[84] Ibid., s. 210.

[85] TOPAK, Ö. E. – BRACKEN-ROCHE, C. – SAULNIER, A. – LYON, D. From Smart Borders to Perimeter Security: The Expansion of Digital Surveillance at the Canadian Borders. *Geopolitics*. 2015, Vol. 20, č. 4, s. 890.

Ke sledování však nemusí docházet pouze na místech, kde hrozí vyšší riziko teroristického útoku nebo jiného kriminálního jednání, např. na letištích, vlakových nádražích a jiných dopravních uzlech. Jednotlivci mohou být sledováni kupříkladu i po překročení státní hranice a v případě podezření z nelegální aktivity, včetně překročení platnosti pobytového oprávnění, mohou být vyhledáni a zadrženi. V tomto smyslu se mluví o tzv. mobilních hranicích.[86] Zatímco na hraničních přechodech jednotlivci o dohledu státu nad tím, kdo vstupuje na jejich území, vědí, neboť předkládají ke kontrole svoje cestovní doklady, o dohledu nad sebou mimo hraniční přechod tito jednotlivci informováni nejsou.

5.3 Efektivita systémů dohledu ve vazbě na jejich účel

Systémy dohledu na místech s vysokým počtem osob nebo předmětů vykazují chyby. Kromě případů, kdy systém osobu nebo objekt vůbec nezaznamená, se může stát, že osoba nebo předmět jsou nesprávně označeny jako potenciálně rizikové, přestože tomu podle hodnot zadaných v systému takto není. V takovém případě hovoříme o falešně pozitivní detekci. Pokud jsou objekty dohledu v krátké vzdálenosti od sebe nebo se částečně překrývají, může systém tyto objekty spojit v jeden nebo je zaměnit. Pokud bude jeden z objektů vyhodnocen jako rizikový a dojde-li k záměně, bude tento objekt opět označen jako falešně pozitivní.[87]

Cílem výše uvedených systémů je vyhodnotit chování jednotlivců a vyvolat intervenci odpovědných osob ještě předtím, než vůbec k trestnému činu dojde. Lyon toto nazývá předzločinem (*pre-crime*). Masivním nasazením systému dohledu je skutečnost, že se stírá rozdíl mezi národní bezpečností a veřejnou bezpečností. Systémy dohledu nejsou využívány pouze k detekování možného teroristického útoku, ale i jiných aktivit, byť se nemusí jednat ani o aktivity kriminálního charakteru. Příkladem může být výše uvedený příklad, kdy jsou systémy ve veřejné dopravě schopné vyhodnotit, zda se osoba pokusí v nejbližší době o sebevraždu. Systémy dohledu se nezaměřují pouze na osoby, které páchají trestnou činnost, ale na všechny jednotlivce ve sledované lokalitě. S podezřelými z předzločinu se pak zachází jako s pachateli.[88]

Změnou v systému dohledu, kterou lze podle Lyona pozorovat, je posun od prověřování osob k jejich vyloučení.[89] Příkladem je vyloučení ze sledovaného místa na základě určitého chování, které je vyhodnoceno jako rizikové, nebo již výše zmíněný *No Fly List*. *„Tento*

[86] Ibid., s. 888.
[87] MAGGIO, S. – HAUGEARD, J.-E. – MEDEN, B. – LUVISON, B. – AUDIGIER, R. – BURGER, B. – PHAM, Q. C. Tracking of Objects of Interest in a Sequence of Images. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, s. 135.
[88] LYON, D. – HAGGERTY, K. D. The Surveillance Legacies of 9/11: Recalling, Reflecting on, and Rethinking Surveillance in the Security Era. *Canadian Journal of Law and Society*. 2012, Vol. 27, No. 2, s. 293.
[89] Ibid., s. 295.

proces sociálního třídění ukazuje, že hranice se stávají ve zvýšené míře *biopolitickými, cílem je řídit jednotlivce pouze jako biologická těla, nikoli jako politické subjekty s politickými právy. To se děje prostřednictvím využití výjimky v tom smyslu, že z osob překračujících hranice byly učiněny objekty biopolitické intervence. Přechod těchto osob přes hranice je povolen do té míry, že tyto osoby mohou být v každém okamžiku vyloučeny. Je to právě diverzifikace a rozšíření digitálních technologií dohledu, které učinily to, že se taková výjimečná praxe stala normou. Digitální systémy umožňují nepřetržité a automatické sdílení informací mezi státními orgány, když se z každého místa stává hranice nebo vyhrazený prostor*.“[90]

Dohled slouží ke klasifikaci jednotlivců pomocí biometrického profilování a jejich možné následné identifikaci. Důvodem je vyhodnocení rizika, které by mohli představovat pro veřejnou bezpečnost.[91] Toto kategorizování jednotlivců vede podle Lyona k jejich diskriminaci právě na základě rizika, jež by mohli představovat. *„Každodenní dohled závisí stále více na vyhledávacích databázích. I tam, kde tomu ještě tak není, nebo ne zcela – jako například u kamerových systémů CCTV převážně obsluhovaných* člověkem *– hlavním cílem je sociální třídění. Dohledový systém získává údaje osob i skupin pro to, aby klasifikoval osoby a obyvatelstvo podle různých kritérií, aby se určilo, na koho se zaměřit z důvodu zvláštního zacházení, podezření, oprávnění dle určitých požadavků, začlenění, přístupu, a tak dále*.“[92]

Příčinou sociálního třídění v rámci dohledu je tendence k mapování populace, jež je již od počátku zatížena předsudky a stereotypy mapujících osob, které vykonávají pravomoc orgánů veřejné moci. Obyvatelstvo je pro účely dohledu tříděno na základě jemných biometrických údajů, jako je rasa nebo pohlaví.[93]

Clive Norris uvádí na příkladu sledování kamerovým systémem CCTV, jak se toto třídění prakticky uplatňuje v tomto typu dohledu. Personál obsluhující kamerový systém je doslova zahlcen daty získanými prostřednictvím kamer. Tato data musí být vyhodnocena s ohledem na potenciální riziko snímaných osob pro veřejnou bezpečnost. Jelikož není možné, aby obsluha kamerového systému vyhodnotila veškerá data z výše uvedeného hlediska, je nutné, aby provedla výběr situací a osob náhodně, nebo aby zvolila k bližšímu zkoumání osoby a situace, které jsou v jejím pohledu nejrizikovější.[94] Výběr takových osob a situací může být ovlivněn předsudky a nepodloženými podezřeními obsluhy kamerového systému. Toto potvrdil i výzkum, který Norris s Garym Armstrongem provedli mezi obsluhou kamerového systému CCTV. Závěrem tohoto průzkumu byla vysoká diferenciace sledovaných osob. Sledování bylo nepřiměřeně zaměřeno na mladé muže, zejména pokud byli tmavé pleti nebo mohli být viditelně přiřazeni k určité subkulturní skupině na podkladě oblečení nebo

[90] TOPAK, Ö. E. – BRACKEN-ROCHE, C. – SAULNIER, A. – LYON, D. *From Smart Borders to Perimeter Security: The Expansion of Digital Surveillance at the Canadian Borders*. op. cit., s. 892.

[91] LYON, D. Surveillance as social sorting. Computer codes and mobile bodies. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003, s. 13.

[92] Ibid., s. 13.

[93] Ibid., s. 16.

[94] NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003, s. 263.

účesu. Tuto selekci vyhodnotili Norris a Armstrong jako diskriminační, neboť z průzkumu vyplynulo, že rozlišování na základě výše uvedené příslušnosti sledovaných osob nemusí být založeno na jejich chování ani na jiných individuálních kritériích, nýbrž na jejich příslušnosti ke společenské skupině, popř. na jejich rase.[95]

[95] NORRIS, C. – ARMSTRONG, G. CCTV and the Social Structuring of Surveillance. Crime Prevention Studies [online]. 1999, Vol. 10, s. 175 [cit. 2016-04-30]. Dostupné z: <http://www.popcenter.org/library/crimeprevention/volume_10/06-NorrisArmstrong.pdf>.

Část VI. Profilování jako nedílný základ algoritmického rozhodování

6.1 Pojem Big Data a jejich význam pro oblast profilování

Orgány veřejné správy a soukromé subjekty, které využívají ve svých systémech algoritmy pro hodnocení chování a automatizované rozhodování, potřebují k tréningu těchto systémů a k jejich provozu velké množství dat. Tato data mohou být osobními údaji či se o osobní údaje jednat nemusí, ať již proto, že byly anonymizovány, nebo se jednalo od počátku o neosobní údaje.

Pojmem Big Data se rozumí nové způsoby, jimiž organizace, ať již orgány veřejné správy, nebo soukromé subjekty, kombinují data a pomocí statistiky a data miningu v nich nalézají skryté informace a korelace[96] které mohou být mimo jiné použity k provozu systémů sledování a automatizovaného rozhodování. Big Data slouží rovněž k profilování jednotlivců. Profilování je činnost, kdy je soubor znaků charakterizujících určité osoby vyvozován z informací získaných v minulosti, a soubory údajů jsou pak prohledávány s cílem najít osoby, které těmto znakům odpovídají.[97] GDPR definuje profilování jako jakoukoli formu 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 (čl. 4 bod 4 GDPR). Výsledkem profilování mohou být i biometrické behaviorální profily typizovaného

[96] RUBINSTEIN, I. S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* [online]. 2013, Vol. 3, No. 2, s. 1 [cit. 2014-05-10]. Dostupné z: <http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.full>.

[97] CLARKE, R. *Profiling: A Hidden Challenge to the Regulation of Data Surveillance* [online]. 1993 [cit. 2012-03-15]. Dostupné z: <http://www.rogerclarke.com/DV/PaperProfiling.html>.

chování v určitém prostoru a čase. GDPR stanoví zvláštní podmínky, pokud je na základě profilování učiněno automatizované individuální rozhodnutí (viz níže).

Profily neboli modely mohou být získávány pomocí techniky data miningu. Podstatou data miningu je prohledání databází s daty s cílem najít hodnotné informace, na jejichž základě jsou profily vystavěny. Technikou data miningu lze nalézt i souvislosti mezi daty, např. přiřadit jméno k fotografii nebo videozáznamu.

Jelikož smyslem Big Data je generování nových informací a hledání korelací mezi nimi, jsou Big Data prostředkem pro profilování jednotlivců a dohled nad nimi. Profilování a dohled spolu úzce souvisí. Profilování umožňuje neinvazivní dohled v reálném čase. K přijetí opatření invazivního charakteru může ovšem dojít, pokud chování osoby neodpovídá biometrickému behaviorálnímu profilu. Prostřednictvím dohledu dále orgány veřejné moci získávají informace, které jsou opět použity pro účely profilování a algoritmického rozhodování.

Rouvroy rozeznává tzv. měkká a tvrdá data (*soft data* a *hard data*).[98] Tvrdá data jsou konsolidované údaje, které o jednotlivci produkují orgány veřejné správy, např. fotografie jednotlivce spolu s jeho identifikačními údaji. Měkká data jsou data získaná prostřednictvím sociálních sítí, pozice zařízení s technologií GPS apod. Spíše než skutečnost, kdo je původcem dat a jejich správcem podle právních norem na ochranu osobních údajů, je možné vnímat rozdělení na měkká a tvrdá data podle toho, zda jsou tato data již od počátku jako data zaznamenána a zpracovávána, nebo zda se jedná o data vytvořená z něčeho, co původně jako data vnímáno nebylo, ale vzniklo digitalizací určitého objektu nebo biometrických charakteristik (např. obličeje, tělesného postoje či chování). V době Big Data je totiž zaznamenáváno, digitalizováno a ukládáno vše, co bylo předtím triviální a pomíjivé, jako například zvuky, pohyby nebo gesta. Toto vše bylo pochopitelně zaznamenáváno i před touto dobou, nicméně díky všudypřítomnosti informačních a komunikačních technologií a kapacitě datových úložišť je objem těchto dat ve srovnání s érou před Big Data neporovnatelný. Měkká data mohou být přitom generována jak soukromými subjekty, tak i orgány veřejné správy, které disponují potřebnou technologií, nebo mohou být veřejným orgánům předána soukromým subjektem v rámci takzvaného partnerství soukromého a veřejného sektoru.

Big Data jsou tradičně definována třemi *V*: *volume*, *variety* a *velocity*, tedy objemem, různorodostí a rychlostí. V době Big Data využívají analytici všechna data, která mají k dispozici, a ne pouze vzorek dat z určitého celku údajů. Tím se zvyšuje schopnost predikce budoucího vývoje a možnost získat informace, které by bez využití všech dat zůstaly skryté,[99] např. identita jednotlivce získaná porovnáním fotografie s připojenými identifikačními údaji a videozáznamu, na němž se tato osoba nachází. Různorodost dat je dána typem zpracovávaných dat. Data mohou mít podobu textu, audio nebo video nahrávky, obrázku, ale také

[98] ROUVROY, A. – STIEGLER, B. Le régime de vérité numérique. De la gouvernementalité algorithmique à un nouvel État de droit. *Scio* [online]. 2015, Vol. 4, s. 116 [cit. 2016-04-30]. Dostupné z: <https://pure.fundp.ac.be/ws/files/13160335/socio_1251_4_le_regime_de_verite_numerique.pdf>.

[99] MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big Data: a revolution that will transform how we live, work and think*. op. cit., s. 12.

logů, lokačních dat apod. Některá data jsou strukturována, tj. jsou zařazena do databáze dle svého druhu, jiná jsou v podobě nestrukturovaných dat. Nestrukturovaná data jsou se strukturovanými daty propojována. Poslední tradiční charakteristikou Big Data je rychlost. Shromážděná data mohou být zpracovávána v reálném čase.[100]

Ke třem *V* jako k základní charakteristice Big Data jsou aktuálně doplňována další dvě, a sice *veracity* a *value*, tedy pravdivost a hodnota.[101] Pravdivost není charakteristikou pro Big Data na vstupu, nýbrž na výstupu neboli ve výsledcích, které jsou prostřednictvím Big Data dosahovány. Na vstupu je naopak znakem Big Data chaotičnost.

„Když je množství dat mnohem větší a nového typu, přesnost již v některých případech není cílem, pokud můžeme vytušit obecné trendy. Posuneme-li se do vyššího měřítka, nezmění se jen očekávání přesnosti, ale i praktická možnost dosáhnout exaktnosti. Přestože se to může zdát na první pohled jako protimluv, pokud budeme zacházet s daty jako s něčím nedokonalým a nepřesným, umožňuje nám to činit kvalitnější předpovědi a tím rozumět lépe světu."[102] Dosažení větší přesnosti by ani z ekonomického hlediska nemělo smysl, jelikož by třídění dat na vstupu bylo nákladnější než hodnota, kterou mají informace, jež jsou prostřednictvím analýzy dat získány.[103]

Dalším znakem Big Data je jejich hodnota. V éře Big Data mají hodnotu všechna data. Nezáleží na tom, zda jsou data použitelná pro konkrétní účel v přítomnosti. Hodnota dat spočívá ve všech potenciálních způsobech využití v budoucnu. Mayer-Schönberger a Cukier toto nazývají nejasnou hodnotou dat.[104] Hodnota dat se nesnižuje jejich prvotním použitím. Data mohou být využívána opakovaně. Využití dat jedním subjektem nebrání jejich užití dalšími.[105] Data nemají hodnotu pouze pro prvotní účel, pro nějž byla shromážděna. Budoucí využití dat však nemusí být v době, kdy jsou data shromažďována, ještě známo.[106] V době Big Data shromažďují orgány veřejné moci údaje za účelem ochrany veřejné a národní bezpečnosti a snižování nákladů, i nákladů na lidské zdroje.[107] Rovněž orgány veřejné moci využívají techniky data miningu k vyhledávání skrytých informací a korelací v datových souborech. Tyto informace a korelace mohou být použity právě pro účely algoritmického rozhodování v reálném čase uskutečňovaného v rámci dohledu. Pokud je systémem zaznamenáno neobvyklé chování, systém se na takovou osobu zaměří a prostřednictvím prohledávání databází se pokusí osobu identifikovat, popř. o ní získat další

[100] MINELLI, M. – CHAMBERS, M. – DHIRAJ, A. B*ig Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*. Hoboken: John Wiley & Sons, Inc., 2012, s. 9.

[101] Srov. HITZLER, P. – JANOWICZ, K. *Linked Data, Big Data, and the 4th Paradigm* [online]. 2013, s. 1 [cit. 2014-06-15]. Dostupné z: <http://www.semantic-web-journal.net/system/files/swj488.pdf>.

[102] MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big Data: a revolution that will transform how we live, work and think*. op. cit., s. 40.

[103] Ibid., s. 41.

[104] Ibid., s. 104.

[105] Ibid., s. 101.

[106] Ibid., s. 103.

[107] ROUVROY, A. – BERNS, T. Gouvernementalité algorithmique et perspectives d'émancipation: le disparate comme condition d'individualisation par la relation? *Réseaux* [online]. 2013, Vol. 177, No. 1, s. 3 [cit. 2016-05-18]. Dostupné z: <http://works.bepress.com/antoinette_rouvroy/47/>.

informace, na jejichž základě by vyhodnotil její riziko pro veřejný pořádek nebo národní bezpečnost. Využívání techniky data miningu a algoritmického rozhodování mohou státy odůvodňovat přesnějším a objektivnějším rozhodováním v kratším čase, jakož i sníženými náklady na lidské zdroje, které by musely data vyhodnocovat, což v době Big Data není u všech dat, která jsou orgánům veřejné moci dostupná, ani možné.

6.2 Rizika v oblasti data miningu

Podle Crawforda a Schultze je možné prostřednictvím Big Data porušovat antidiskriminační právní normy.[108] Jestliže s jednotlivcem bude zacházeno méně příznivě než s jinými osobami ve stejné situaci pouze na základě příslušnosti k určité etnické skupině nebo chování, jedná se o diskriminaci. Nepříznivé zacházení může mít formu vyloučení těchto osob k detailnější kontrole nebo dokonce aktivní zásah proti nim, který je způsobilý těmto osobám přivodit újmu.

Paul Rosenberg navrhuje záruky ochrany práv jednotlivce při využití techniky data miningu a techniky získávání informací. První zárukou by mělo být povolení pro použití určité techniky data miningu a získávání informací zákonodárcem. Dále by k získávání informací o jednotlivci měla být dodržována pravidla stanovená vnitřními směrnicemi a měly by být použity pouze údaje získané v souladu s právními předpisy. Pro automatizovanou analýzu vzorců by měly být použity předem schválené vzorce a modely. Ochrana jednotlivce by měla být zajištěna tím, že jeho osobní údaje mohou být předány orgánům veřejné moci pouze s předchozím souhlasem soudu.

Zákon by měl stanovit, že výsledek automatizované analýzy bude použit pouze pro další vyšetřování. Zákon by měl dále obsahovat proces nápravy falešně pozitivních výsledků. Používání techniky data miningu a získávání informací by mělo být podrobeno dohledu a kontrole. Odpovědné osoby by měly procházet školeními a pro případ zneužití informací by měla být upravena občanskoprávní a trestněprávní odpovědnost. Jako poslední záruku Rosenzweig uvádí absolutní zákonný zákaz využívání techniky pro získávání informací prostřednictvím data miningu pro vyšetřování, které není spojeno s ohrožením terorismem.[109]

Rosenzweig se dále zabývá ochranou jednotlivce při zpracování jeho osobních údajů pro účely data miningu a získávání informací. Systém musí být nastaven tak, aby bylo zajištěno, že data, která jsou zaznamenána a analyzována z důvodu možné shody se vzorcem či modelem, nejsou dále zpracovávána, pokud není tato shoda nalezena. Poté, co algoritmus prohledá databáze za účelem nalezení informací odpovídajících hledanému vzorci nebo

[108] CRAWFORD, K. – SCHULTZ, J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Review* [online]. 2014, Vol. 55, No. 1, s. 99 [cit. 2016-04-30]. Dostupné z: <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr>.

[109] ROSENZWEIG, P. Proposals for Implementing the Terrorism Information Awareness System. *Heritage.org* [online]. 7. 8. 2003 [cit. 2016-04-30]. Dostupné z: <http://www.heritage.org/research/reports/2003/08/proposals-for-implementing-the-terrorism-information-awareness-system>.

modelu, nesmí být údaje, které se neshodují se vzorcem, dále zpracovávány, tj. zejména uchovávány v databázích orgánů státní správy. Dále musí být zajištěno, aby údaje, které neodpovídají požadovanému vzorci nebo modelu, nebyly předmětem dalšího analyzování. Tento postup musí být automatizován, aby se zabránilo výše zmíněnému analyzování.

Právní předpisy by měly upravovat parametry technologie získávání informací. Právními předpisy by měl být zejména regulován postup, v jakém budou databáze prohledávány. Jako první by měly být použity databáze orgánů veřejné moci. Pokud není v těchto databázích nalezena shoda se vzorcem, teprve poté mohou být využity databáze dat, v nichž jsou zpracovávána data soukromými subjekty. Právní předpisy by měly rovněž zaručit, že na počátku nebude jednotlivec spojován se vzory, jež jsou předmětem dotazu. Vyhodnocení dotazu by mělo obsahovat pouze informace o určité aktivitě, která se shoduje se vzorci údajné teroristické činnosti. Na počátku by neměly být systémem poskytovány informace, které mohou jednotlivce identifikovat.

Část VII. Automatizované rozhodování dle GDPR

7.1 Právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování

Při algoritmickém dohledu v reálném čase dochází z povahy věci k algoritmickému rozhodování. GDPR nazývá takové rozhodování rozhodováním automatizovaným. Vodítka Pracovní skupiny 29 k automatizovanému individuálnímu rozhodování a profilování uvádí, že automatizované rozhodování znamená schopnost dělat rozhodnutí čistě technologickými prostředky bez lidského zásahu.[110] Věcná působnost GDPR je vymezena v čl. 2 tohoto nařízení. Podle druhého odstavce se toto nařízení nevztahuje na zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Pokud je dohled a algoritmické rozhodování v určitém prostoru prováděn bezpečnostními složkami, GDPR se na algoritmické rozhodování vztahovat nebude. Do působnosti GDPR ovšem spadá algoritmické rozhodování v rámci dohledu prováděného jinými subjekty než bezpečnostními složkami. Takovými subjekty bude provozovatel letiště, nádraží nebo jiného prostoru, kde k dohledu dochází.

Subjekt údajů má dle čl. 22 odst. 1 GDPR právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Právním účinkem podle výše uvedených Vodítek je zamezení přechodu přes hranice, podrobení zvýšené úrovni bezpečnostních opatření nebo sledování příslušnými úřady. Podrobení zvýšené úrovni bezpečnostních opaření bude mít analogicky pro subjekt údajů právní účinky, bude-li prováděno soukromými subjekty, pokud účinky pro subjekt údajů budou stejné nebo srovnatelné

[110] PRACOVNÍ SKUPINA 29. Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679. *Úřad pro ochranu osobních údajů* [online], s. 8. [2019-10-30] Dostupné z: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893>.

s prováděním těchto činností orgány veřejné moci. Právním účinkem zde bude zásah do práva na soukromí či práva na ochranu tělesné integrity.

7.2 Zákaz automatizovaného rozhodování

Ustanovení čl. 22 přináší výkladové problémy, zda se jedná o zákaz automatizovaného rozhodování, nebo o námitku subjektu údajů, který může po poskytnuté informaci o takovém druhu rozhodování, která je pro správce povinná, vyjádřit svůj nesouhlas.

Argumentem pro námitku je právě existence povinnosti správce subjekt údajů informovat o existenci automatizovaného rozhodování (čl. 13 odst. 2 písm. f) a čl. 14 odst. 2 písm. g)). Automatizované individuální rozhodování je rovněž v nařízení zařazeno spolu s námitkou do samostatného oddílu. Znění tohoto článku je také odlišné od směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která ve svém článku 15 stanovila, že přiznají všem osobám právo nestát se subjektem rozhodnutí, které vůči nim zakládá právní účinky nebo které se jich významně dotýká, přijatého výlučně na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jejich osobnosti.

Skutečnost, že se jedná o zákaz automatizovaného rozhodování, podporuje znění ostatních článků GDPR, které jsou vyjádřeny pozitivně (subjekt údajů má podle čl. 15 GDPR právo na přístup k údajům, podle čl. 17 právo na výmaz atd.), zatímco znění čl. 22 GDPR je negativní. Podle výše zmiňovaných Vodítek k automatizovanému individuálnímu rozhodování čl. 22 odst. 1 toto rozhodování zakazuje.[111] Přestože tento výklad nemá jednoznačný podklad v textu nařízení, dá se předpokládat, že se jím budou orgány aplikující právo řídit a každé automatizované rozhodování, které není založeno na jedné z výjimek uvedených v ustanovení čl. 22, sankcionovat.

7.3 Přípustnost automatizovaných individuálních rozhodování

Automatizované individuální rozhodování je přípustné, pokud je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů, je

– povoleno právem Unie nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo
– pokud je založeno na výslovném souhlasu subjektu údajů. Tyto výjimky se neuplatní, je-li automatizované rozhodování založeno na zvláštních kategoriích údajů, kromě

[111] Ibid., s. 9.

případů, že subjekt údajů dal ke zpracování těchto údajů výslovný souhlas nebo zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Pokud právo členského státu nebo unijní právo nepovolí provozovateli příslušných prostor automatizované rozhodování o chování za účelem předcházení bezpečnostním hrozbám, musí mít provozovatelé prostor, kde dochází k dohledu a následnému automatizovanému rozhodování, ke zpracování osobních údajů o chování jednotlivců na základě jejich sledování a vyhodnocování jejich chování podle biometrických behaviorálních profilů bez identifikace, souhlas subjektu. Souhlas oznámením o zpracování osobních údajů a prostým vyvěšením upozornění o tom, že vstupem do prostoru subjekt údajů uděluje svůj souhlas s automatizovaným rozhodováním, při vstupu do prostor by byl pravděpodobně shledán v rozporu s GDPR. Pracovní skupina 29 ve svých Vodítkách k souhlasu uvádí, že *„jednoznačný projev vůle souhlasu vyžaduje prohlášení subjektu údajů nebo jednoznačné potvrzení, což znamená, že tak vždy musí být učiněno aktivním úkonem nebo prohlášením. Musí být zřejmé, že subjekt údajů s daným konkrétním zpracováním souhlasil“*.[112] Souhlas se zpracováváním osobních údajů pro účely automatizovaného rozhodování musí být navíc výslovný, to znamená, že *„[s]ubjekt údajů musí učinit výslovné prohlášení o souhlasu“*.[113] Pokud nebude existovat český nebo unijní právní předpis, nelze podle našeho názoru automatizované individuální rozhodování při výkonu dohledu pro účely ochrany bezpečnosti privátními subjekty použít, neboť si v praxi lze pouze stěží představit, že každý, kdo vstupuje do prostor, kde je vykonáván dohled, učiní výslovné prohlášení o souhlasu.

Pokud by byl dohled spojený s automatizovaným individuálním rozhodováním českým nebo unijním právním předpisem povolen, musel by takový předpis stanovit vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů. Jako vhodné opatření se jeví právo na soudní přezkum. I v případě povolení automatizovaného rozhodování právním předpisem by správce měl mít povinnost o tomto dohledu subjekt údajů informovat podle čl. 13 a 14 GDPR. Informace o automatizovaném zpracování by měla být poskytnuta subjektu údajů i po uplatnění jeho práva na přístup dle čl. 15 GDPR. Při poskytování informací o automatizovaném rozhodování musí správce subjekt údajů informovat o tom, že k tomuto rozhodování dochází, a zároveň poskytnout smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů. Zvláštní právní předpis by pravděpodobně rozsah informací o automatizovaném rozhodování s ohledem na zajištění ochrany práv a svobod ještě rozšířil, minimálně o právo podat návrh na soudní přezkum rozhodnutí. Problematickou se v případě zajištění bezpečnosti jeví informace o použitém postupu. Tyto informace bývají nazývány právem na vysvětlení („*right to explanation*“). Wachter, Mittelstadt a Floridi rozlišují dva aspekty práva na vysvětlení automatizovaného rozhodnutí, a sice aspekt týkající se povahy informací a časový aspekt, tedy dobu, kdy je formace poskytnuta. Právo na vysvětlení se může, za

[112] PRACOVNÍ SKUPINA 29. Vodítka k souhlasu podle Nařízení 2016/679. *Úřad pro ochranu osobních údajů* [online], s. 15. [2019-10-30] Dostupné z: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896>.

[113] Ibid., s. 17.

prvé, vztahovat k fungování systému, včetně kritérií a předdefinovaných modelů, nebo, za druhé, k rozhodnutím, jejich odůvodněním, k referenční skupině nebo profilům a k individuálním okolnostem, na jejichž základě bylo rozhodnutí vydáno. Právo na vysvětlení může být realizováno *ex ante*, tedy před učiněním rozhodnutí. V takovém případě se informace budou moci vztahovat pouze k fungování systému. Může se jednat i o vysvětlení *ex post*, po přijetí rozhodnutí. Subjekt údajů může být v této době informován jak o fungování systému, tak i o rozhodnutí samotném.[114]

Právo na vysvětlení zmiňuje recitál 71 nařízení. Na automatizované individuální rozhodnutí by se měly podle něj vztahovat vhodné záruky, které by měly zahrnovat konkrétní informování subjektu údajů a právo na lidský zásah, na vyjádření svého názoru, na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a na napadení tohoto rozhodnutí. Články 13 a 14 ani článek 15 GDPR ovšem právo na vysvětlení neobsahují. Recitály unijních právních předpisů nejsou právně závazné a slouží jen jako interpretační vodítko právnímu předpisu, kterému předchází. Podle Wachtera, Mittelstadta a Floridiho se právo na vysvětlení nedá ze závazného textu nařízení dovodit. Spíše se jedná o zvláštní případ práva na informace o postupu, významu a důsledcích automatizovaného individuálního rozhodování.[115]

Pokud by byl požadavek na informace o použitém postupu příliš široký, mohl by znamenat, že jednotlivci, kteří mohou znamenat bezpečnostní hrozbu, budou schopni systém obejít. Vodítka k automatizovanému rozhodování ani detailní informace o algoritmu nevyžadují. *„Správce by měl nalézt jednoduchý způsob, jak subjektu údajů sdělit podstatu nebo kritéria, na nichž rozhodování spočívá, aniž by se vždy musel snažit o úplné vysvětlení použitých algoritmů nebo o odhalení celého algoritmu.“*[116] V případě algoritmu s funkcí strojového učení nejsou postup a kritéria rozhodnutí známy ani samotnému správci osobních údajů.

Automatizované individuální rozhodování je možné i v případě, že by byl v určitém prostoru vykonáván dohled s následným algoritmickým rozhodováním pro účely prevence trestných činů příslušnými orgány. Podle čl. 11 směrnice 2016/680 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 (dále jen: „směrnice 2016/680“) členské státy stanoví, že rozhodování založené výhradně na automatizovaném zpracování včetně profilování, které má pro subjekt údajů nepříznivé právní účinky nebo se ho významně dotýká, je zakázáno, není-li povoleno právem Unie nebo členského státu, kterému správce podléhá a jež poskytuje vhodné záruky práv a svobod subjektu údajů, alespoň práva na lidský zásah ze strany správce. Taková rozhodnutí se nesmějí opírat o zvláštní kategorie osobních údajů, pokud nejsou k dispozici vhodná opatření zajišťující ochranu

[114] WACHTER, S. – MITTELSTADT, B. – FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, Vol. 7, No. 2, s. 78.

[115] Ibid., s. 77.

[116] PRACOVNÍ SKUPINA 29. Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679. op. cit., s. 14.

práv a svobod a oprávněných zájmů subjektu údajů. Příslušným orgánem je podle čl. 3 bod 7 směrnice 2016/680 jakýkoliv orgán veřejné moci příslušný k prevenci, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, nebo jakýkoliv jiný orgán nebo subjekt pověřený právem členského státu plnit veřejnou funkci a vykonávat veřejnou moc pro účely prevence, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

Směrnice 2016/680 nestanoví zvláštní povinnost informovat subjekt údajů o tom, že dochází k automatizovanému individuálnímu rozhodování, a to ani v rámci práva na informace podle čl. 13 a 14 této směrnice. Nadto má členský stát možnost přijmout legislativní opatření, aby výkon těchto práv omezil či od něho upustil v takovém rozsahu a na takovou dobu, jak je to v demokratické společnosti s náležitým přihlédnutím k základním právům a oprávněným zájmům dotčené fyzické osoby nutné a přiměřené, s cílem mj. zabránit nepříznivému ovlivňování prevence a chránit veřejnou nebo národní bezpečnost (čl. 13 odst. 3 a čl. 15 směrnice 2016/680).

Zákon o zpracování osobních údajů, který směrnici 2016/680 implementuje do českého právního řádu, hovoří v § 39 o zásahu na základě automatizovaného zpracování. Spravující orgán může prostřednictvím výhradně automatizovaného zpracování osobních údajů zasáhnout do práv a právem chráněných zájmů subjektu údajů, nebo způsobit jiný obdobně závažný následek pro subjekt údajů, jen pokud to výslovně stanoví jiný zákon. Tento zákon na rozdíl od směrnice nestanoví, že zákon musí stanovit nezbytné záruky práv a svobod subjektu údajů, alespoň právo na lidský zásah ze strany správce. Zákon, který by automatizované (individuálním) rozhodování povoloval, zatím český právní řád nezná. Rovněž důvodová zpráva k zákonu o zpracování osobních údajů mluví o budoucím zákonu. Zákon o zpracování osobních údajů rovněž nepřevzal zákaz rozhodnutí, která by se opírala o zvláštní kategorie osobních údajů za předpokladu, že nejsou k dispozici vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů (čl. 11 odst. 2 směrnice 2016/680).

Spravujícím orgánem je podle § 24 zákona o zpracovávání osobních údajů orgán veřejné moci příslušný k plnění úkolu předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Na zpravodajské služby se zákon o zpracování osobních údajů nevztahuje.

Část VIII. Algoritmické rozhodování a základní lidská práva

8.1 Zákaz diskriminace

Přestože by rozhodování na základě algoritmu mělo být objektivní, to znamená nejen nezávislé a nestranné, ale rovněž prosté jakéhokoliv nelegitimního rozlišování osob a diskriminace, vyvstává při použití algoritmu k rozhodování obava z různého zacházení s osobami na základě jejich skutečného nebo domnělého atributu. Tímto atributem může být údaj v podobě biometrického údaje v širším smyslu (pohlaví, věk, národnost, etnická příslušnost), příslušnost k určité sociální skupině či jakýkoliv jiný znak. Podle Christophera Slobogina jsou atributy, jako je pohlaví nebo věk, součástí metodologie pro predikci trestné činnosti.[117]

Dohled v reálném čase vyvolává obavy z odlišného zacházení mezi jednotlivci na základě výše zmíněných kritérií. S jednotlivci určité rasy, etnicity, národnosti, pohlaví, věku nebo jako s příslušníky určité sociální skupiny může být zacházeno jinak než s osobami, které do těchto kategorií nespadají. Tito jednotlivci mohou být pouze na podkladě svojí příslušnosti klasifikováni jako rizikoví či rizikovější pro veřejnou nebo národní bezpečnost ve srovnání s osobami, které do jedné z výše uvedených kategorií nespadají, přestože svým chováním nezavdali příčinu ke zvýšenému dohledu. Jednotlivci, kteří jsou klasifikováni jako rizikoví, ať již pro svoji příslušnost, nebo chování, jsou podrobeni zvýšenému nebo cílenému dohledu a následně mohou být i omezeni na svých právech orgány veřejné moci. I toto rozhodnutí může být prezentováno jako objektivní, neboť o rizikovosti jednotlivce bylo rozhodnuto na základě algoritmu.

Rozpor mezi objektivitou automatizovaného rozhodování a obavou z odlišného zacházení a diskriminace vysvětluje Rouvroy vlastností algoritmu spočívající v učení se z předchozích operací. Algoritmus tak podle Rouvroye převezme pohled na svět svých uživatelů

[117] SLOBOGIN, Ch. *Proving the Unprovable. The Role of Law, Science, and Speculation in Adjudicating Culpability and Dangerousness.* Oxford: Oxford University Press, 2007, s. 112.

a použitím jím generovaných výsledků je ve správnosti svých výsledků dále utvrzován. Diskriminaci je velmi obtížné prokázat kvůli argumentu objektivity rozhodování na základě algoritmu.[118]

Rozhodování na základě biometrických údajů v širším smyslu a dalších údajů může být do systému přímo zaneseno. Algoritmus pak s těmito hodnotami pracuje od začátku. V případě algoritmu se schopností učení generuje algoritmus výstupy v průběhu fungování systému v důsledku učení z předchozích operací. Oba tyto modely mohou být při rozhodování v reálném čase použity.

Na rozdíl od lidského dohledu není diskriminace zřejmá, jelikož konkrétní zásah se děje na základě vyhodnocení algoritmem. Námitka osoby, proti níž byl zásah veden, že došlo k diskriminaci na základě příslušnosti k určité rase, národnosti, pohlaví, věkové či sociální skupině, by byla s největší pravděpodobností zamítnuta s odkazem na objektivitu algoritmického rozhodování.

Rozlišujeme dva druhy diskriminace, a to diskriminaci přímou a diskriminaci nepřímou. Přímou diskriminací rozumíme jednání, kdy se s jednou osobou zachází méně příznivě než s jinou osobou ve srovnatelné situaci na základě nepřípustného kritéria.[119] Nepřímá diskriminace vyvolává rozdílné zacházení v aplikační rovině, která je zapříčiněna diskriminační interpelací normy nebo její vadnou konstrukcí.[120]

Podstatu diskriminace ve svém odlišném stanovisku k rozsudku Evropského soudu pro lidská práva (dále jen: „ESLP“) *Chassagnou a ostatní proti Francii*[121] výstižně shrnul soudce tohoto soudu Boštjan Zupančič. *„[J]e třeba samozřejmě chápat, že účel prakticky každé právní normy* – ať už se jedná o příkaz, zákaz*, či zmocnění – je rozlišovat mezi různými kategoriemi (třídami) právních subjektů. Dokonce i trestní zákony jsou v tomto smyslu „diskriminační“ mezi těmi, kteří se nadále považují za nevinné, a těmi, kteří byli shledáni vinnými. Každý právní systém funguje na principu koncepčních rozdílů s právními důsledky – v ústavním, občanském, trestním, správním, mezinárodním aj. právu. Význam latinského slovesa „discriminare“ je rozlišit, vnímat významné rozdíly atd. Nicméně i v běžném jazyce slovo „diskriminace“ nabývá pejorativních konotací, pokud neexistuje rozumný důvod pro rozdílné zacházení s jednotlivci (nebo třídou jednotlivců). Tam, kde takové rozdílné zacházení, plynoucí z předsudků nebo z nedostatku racionální úvahy, je spojeno s užitím moci, hovoříme o libovůli, vrtošivosti, nekonzistentnosti, neregulérnosti, nepředvídatelnosti [...] Intuitivně chápeme, že tyto atributy jsou zcela neslučitelné s ideálem právního státu*.“

Evropská úmluva o lidských právech a základních svobodách (dále jen: „EÚLP“) diskriminaci při užívání práv a svobod garantovaných touto úmluvou zakazuje v čl. 14. Užívání práv

[118] ROUVROY, A. *„Of Data and Men“. Fundamental Rights and Freedoms in a World of Big Data*. op. cit., s. 33.
[119] BOBEK, M. – BOUČKOVÁ, P. – KÜHN, Z. (eds). *Rovnost a diskriminace*. Praha: C. H. Beck, 2007, s. 43.
[120] Ibid., s. 53.
[121] Rozsudek ESLP ze dne 29. dubna 1999, stíž. č. 25088/94, 28331/95 a 28443/95 ve věci *Chassagnou a ostatní proti Francii.*

a svobod musí být zajištěno bez diskriminace založené na jakémkoli důvodu, jako je pohlaví, rasa, barva pleti, jazyk, náboženství, politické nebo jiné smýšlení, národnostní nebo sociální původ, příslušnost k národnostní menšině, majetek, rod nebo jiné postavení. Toto ustanovení nestanoví, že by stát mohl toto právo nebýt diskriminován z legitimních důvodů omezit, tak jako je tomu např. v případě práva na ochranu soukromého a rodinného života nebo práva na svobodu projevu.

Podle čl. 1 odst. 1 Protokolu č. 12 k EÚLP[122] užívání každého práva přiznaného zákonem musí být zajištěno bez jakékoli diskriminace z důvodu pohlaví, rasy, barvy pleti, jazyka a náboženství, politického či jiného smýšlení, národnostního či sociálního původu, příslušnosti k národnostní menšině, majetku, rodu či jiného postavení. Druhý odstavec tohoto ustanovení stanoví, že nikdo nesmí být diskriminován žádným orgánem veřejné moci z jakéhokoli důvodu, zejména z důvodů uvedených v prvním odstavci.

Literatura rozděluje na základě judikatury ESLP tak zvaná *a priori* podezřelá kritéria a kritéria, která *a priori* podezřelá nejsou.[123] Rozdíl mezi výše uvedenými kritérii je v míře uvážení ESLP. Zatímco u kritérií, která podezřelá nejsou, může stát uplatnit širší míru uvážení, u kritérií podezřelých je třeba, aby stát odůvodnil rozdílné zacházení objektivními a závažnými důvody, přičemž musí být zachována proporcionalita mezi užitými prostředky a požadovaným účelem rozdílného zacházení.[124] *A priori* podezřelými důvody jsou pohlaví, sexuální orientace, národnost, rasa nebo etnický původ, manželský či nemanželský původ dítěte a zdravotní stav nebo postižení.[125]

Ve věci, již řešil ESLP, *Turan Cakir proti Belgii*[126] se stěžovatel tureckého původu domáhal prošetření zacházení policie při zatýkání, jelikož se domníval, že způsob jednání policie byl nepřiměřený právě z důvodu etnické příslušnosti stěžovatele. Postup policie nebyl belgickými státními orgány dostatečně prošetřen. ESLP judikoval, že při vyšetřování násilných incidentů mají státní orgány přijmout veškerá opatření, aby odhalily jakýkoli rasistický motiv, a určit, zda událost nebyla ovlivněna předsudky, které by měly svůj základ v etnickém původu dotčené osoby. Stát musí přijmout za daných okolností přiměřená opatření, shromažďovat a zajišťovat důkazy, prošetřit všechny skutečnosti pro to, aby byla zjištěna pravda a bylo vyneseno odůvodněné nestranné a objektivní rozhodnutí, bez vynechání podezřelých skutečností svědčících o aktu násilí motivovaného rasovými důvody. Kromě toho je prověřování souvislostí mezi rasistickými postoji a násilím ze strany státních orgánů jeden z aspektů procesních povinností, které pro státy vyplývají z čl. 3 EÚLP upravující zákaz mučení a jiného nelidského zacházení nebo trestu. Toto prověřování může být vnímáno jako implicitní součást odpovědnosti státu podle čl. 14 EÚLP, neboť je třeba zajistit respektování čl. 3 EÚLP bez jakékoliv diskriminace.

[122] Protokol č. 12 k Úmluvě o ochraně lidských práv a základních svobod.
[123] Srov. KABELOVÁ DOLEJŠOVÁ, K. *Zákaz diskriminace jako právní problém v judikatuře Evropského soudu pro lidská práva*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012, s. 114.
[124] Rozsudek ESLP ze dne 24. července 2003, stíž. č. 40016/98 ve věci *Karner proti Rakousku*.
[125] Srov. WÁGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer ČR, 2012, s. 104.
[126] Rozsudek ESLP ze dne 10. března 2009, stíž. č. 44256/06 ve věci *Turan Cakir proti Belgii*.

Stejný názor ESLP vyslovil i v rozsudku ve věci *B. H. proti Španělsku*[127] na základě stížnosti nigerijské prostitutky, která se při čtvrtém zatčení v roce 2005 domáhala prošetření možné diskriminace na základě rasy, neboť její kolegyně, které nebyly afrického původu, zatýkány nebyly. Stěžovatelka nadto dále tvrdila, že bylo proti ní ze strany policie použito násilí. Španělské orgány však její tvrzení stejně jako v případě Turana Cakira neprošetřily.

V případě Fredin se ESLP zabýval důkazním břemenem na straně stěžovatele, který o sobě tvrdí, že je obětí diskriminace. Soud ve svém rozsudku *Fredin proti Švédsku* připomněl, že čl. 14 EÚLP garantuje ochranu proti diskriminaci, která spočívá v rozdílném zacházení s osobami ve srovnatelných situacích bez objektivního a rozumného zdůvodnění. Aby byla stížnost k ESLP týkající se porušení tohoto článku úspěšná, musí být založena mimo jiné na tvrzení, že situace údajné oběti diskriminace může být považována za podobnou situaci osob, s nimiž bylo zacházeno lépe.[128]

Obdobně zákaz diskriminace obsahuje i Listina základních lidských práv Evropské unie (dále jen: „Listina EU“). Podle čl. 21 Listiny EU se zakazuje jakákoli diskriminace založená zejména na pohlaví, rase, barvě pleti, etnickém nebo sociálním původu, genetických rysech, jazyku, náboženském vyznání nebo přesvědčení, politických názorech či jakýchkoli jiných názorech, příslušnosti k národnostní menšině, majetku, narození, zdravotním postižení, věku nebo sexuální orientaci. Stejně jako EÚLP nezná ani Listina EU žádné legitimní omezení zákazu diskriminace.

Diskriminaci v požívání základních práv a svobod zakazuje Listina základních práv a svobod (dále jen: „Listina“). Podle čl. 3 odst. 1 se základní práva a svobody zaručují všem bez rozdílu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického či jiného smýšlení, národního nebo sociálního původu, příslušnosti k národnostní nebo etnické menšině, majetku, rodu nebo jiného postavení.

V případě rozhodování o rizikovosti osob v reálném čase se může jednat o diskriminaci jak přímou, tak nepřímou. O přímou diskriminaci půjde, pokud systém bude za jednu z hodnot, na jejichž základě bude rozhodovat, považovat jako určující některý z biometrických údajů v širším smyslu či některý další výše uvedený atribut osoby, a jako rizikovější budou v systému hodnoceni jednotlivci, u nichž je přítomen jeden nebo více těchto atributů nebo biometrické údaje v širším smyslu. O přímou diskriminaci se bude jednat též, bude-li systém vyhodnocovat osoby méně příznivě z důvodu jejich rasy či jiných atributů, o nichž jsme hovořili výše, na základě učení se z předchozích rozhodnutí. Tyto atributy nebudou v systému sice od začátku přítomny, ale v průběhu fungování systému dohledu je bude tento systém považovat za důležitý faktor rizikovosti jednotlivce, ne-li faktor nejdůležitější. Pokud bude algoritmus považovat jeden nebo více ze zmíněných atributů jednotlivce za jeden z faktorů zvyšujících jeho rizikovost a na jeho základě bude generovat výsledek a jestliže s takovým jednotlivcem bude zacházeno méně příznivě než s jinou osobou nacházející se na stejném místě, nad níž je vykonán dohled, či dokonce vykazující stejné nebo podobné

[127] Rozsudek ESLP ze dne 24. července 2012, stíž. č. 47159/08 ve věci *B. H. proti Španělsku*.
[128] Rozsudek ESLP ze dne 18. února 1991, stíž. č. 12033/86 ve věci *Fredin proti Švédsku*.

způsoby chování, bude se jednat o diskriminaci přímou. O nepřímou diskriminaci by se jednalo v případě, že by osoba byla vyhodnocena jako riziková, případně by bylo zasaženo do její tělesné integrity či by byla jinak omezena na základě chování, které by bylo algoritmem vyhodnoceno jako rizikové, např. pokud by se osoba začala chovat na monitorovaném místě tak, jak požaduje její náboženství. Systém by v takovém případě nerozlišoval osoby na základě náboženství a víry, ale chování typického pro náboženství nebo víru.

Přestože EÚLP neumožňuje členskému státu omezit z legitimních důvodů zákaz diskriminace, přiznává tento soud členskému státu u některých důvodů širší možnost uvážení. Je tudíž na zvážení státu, zda rozdílné zacházení uplatní, či nikoliv. Toto rozdílné zacházení však musí odůvodnit. Při výkonu dohledu nad jednotlivci v reálném čase bývá rozhodováno na základě hodnot, u nichž ESLP uplatňuje přísnější kritéria míry uvážení státu, tedy pohlaví, rasu, národnost nebo etnický původ. Z toho vyplývá, že pokud by bylo stěžovatelem napadeno rozhodnutí státních orgánů, o němž by stěžovatel tvrdil, že porušuje zákaz diskriminace, musel by stát odůvodnit rozdílné zacházení závažnými a objektivními důvody a mezi užitými opatřeními a účelem by musel existovat vztah proporcionality. Těmito důvody by mohl být kupříkladu požadavek na zachování národní bezpečnosti v případě výkonu dohledu nad jednotlivci, u nichž by byla přítomna některá z biometrických charakteristik nebo jiný atribut, v reálném čase. Domníváme se, že takové rozdílné zacházení by bylo odůvodnitelné, pokud by stát dokázal, že se jednalo o výkon dohledu nad těmito jednotlivci pouze na určitém předem vymezeném místě nebo místech a po předem vymezenou dobu. Na takovém místě a v určené době by muselo nadto existovat předem vymezené riziko pro veřejný pořádek, národní bezpečnost či práva a svobody jiných osob.

Aby byla stížnost k ESLP nebo žaloba úspěšná, musí stěžovatel, resp. žalobce prokázat, že s ním bylo zacházeno méně příznivě než s jinými osobami ve stejné nebo obdobné situaci. Zde narážíme na problém transparentnosti rozhodování na základě algoritmu, kdy osoba, do jejíchž práv bylo zasaženo dohledem orgánu veřejné moci či byl vůči ní na základě vyhodnocení dat algoritmem učiněn zásah ze strany těchto orgánů, nemá povědomí o tom, že k rozhodnutí nebo zásahu došlo na podkladě výsledku generovaného algoritmem. V takovém případě se ani nedozví, že s ní bylo zacházeno méně příznivě než s jinými osobami ve stejné situaci, jelikož nezná ani hodnoty, se kterými algoritmus pracuje.

8.2 Právo na spravedlivý proces

Právo na spravedlivý proces je jedním z pilířů demokratického právního státu. Toto právo zaručuje respektování určitých postupů orgánů veřejné moci v řízení ve vztahu k jeho účastníkům tohoto řízení. Mnohdy bývá právo na spravedlivý proces zmiňováno v souvislosti s trestním řízením a právy obviněného z trestného činu. Právo na spravedlivý proces je v EÚLP zakotveno v čl. 6. Obvykle bývá právo na spravedlivý proces zmiňováno v souvislosti s projednáním věci u nezávislého a nestranného soudu, v přiměřené lhůtě a v procesu, kde jsou zaručena práva obviněného (právo na obhajobu, právo na tlumočníka, právo na veřejné projednání věci). V oblasti občanskoprávní můžeme hovořit o rovnosti zbraní,

o ústním jednání, o přímosti dokazování a principu kontradiktorního procesu vůbec. Součástí práva na spravedlivý proces je i presumpce neviny, tj. považování obviněného za nevinného, dokud se jeho vina neprokáže zákonným způsobem, v českém právu v trestním řízení. V českém právu je právo na spravedlivý proces upraveno v článcích 36 až 40 Listiny a čl. 96, odst. 1, 2 Ústavy. Právo na spravedlivý proces musí být tradičně respektováno v soudním řízení, které již je formalizováno, tj. je zákonným způsobem zahájeno a v jehož průběhu se jedná o právech a povinnostech konkrétních účastníků řízení, nebo o vině a trestu za trestný čin. Otázkou je, zda se některé dílčí aspekty práva na spravedlivý proces nedají uplatnit již v době, kdy k zahájení řízení (ještě) nedošlo, tedy v době, kdy je nad osobami v určitém prostoru vykonáván dohled.

Aspektem, kterým se budeme v souvislosti s tímto dohledem a právem na spravedlivý proces zabývat, je presumpce neviny. Důvodem je skutečnost, že pro systém, který automatizovaně vykonává dohled nad jednotlivci ve vymezeném místě, jsou všechny osoby potenciálně podezřelé, přestože k žádnému trestnému činu (prozatím) nedošlo. Přestože se zásada presumpce neviny uplatňuje v trestním řízení po sdělení obvinění, v *pre-crime society* lze o uplatnění této zásady hovořit i při výkonu dohledu nad jednotlivci, tedy v situaci, kdy k trestnému činu nedošlo, tudíž neexistuje osoba, které by bylo možno sdělit obvinění.

Presumpci neviny garantuje druhý odstavec čl. 6 EÚLP. Každý, kdo je obviněn z trestného činu, se považuje za nevinného, dokud jeho vina nebyla prokázána zákonným způsobem. Podobně je presumpce neviny formulována i v čl. 48 Listiny EU a čl. 40 odst. 2 Listiny.

Zásada presumpce neviny může být porušena při využití systému dohledu, který na základě algoritmu vyhodnocuje a zaznamenává data v reálném čase. Podle Lucie Zedner se ze společnosti, ve které je trestná činnost řešena po spáchání trestného činu (*post-crime society*), stává společnost, v níž se trestná činnost řeší ještě před spácháním trestného činu (*pre-crime society*), tak jak o ní hovořil i David Lyon. V prvně jmenovaném případě se trestným činem zabývají orgány činné v trestním řízení a v trestním řízení vedeném proti obviněnému má tento obviněný práva stanovená zákonem. Tento model zůstává dominantním i nadále, nicméně se stále více uplatňují i prvky pre-crime society, v níž řeší orgány veřejné správy trestnou činnost prospektivně. Nástroji k tomuto řešení trestné činnosti jsou systémy pro algoritmický výpočet rizika ve jménu bezpečnosti.[129] Podle Zedner není dohled nad jednotlivci v pre-crime society vykonáván v rámci trestního řízení, a tudíž nejsou jednotlivcům, nad nimiž je vykonáván dohled, zaručena stejná práva jako obviněnému v trestním řízení.[130] Pokud je vůči určitým jednotlivcům na základě algoritmického vyhodnocení jejich rizika pro bezpečnost přijato opatření a toto opatření se neděje v rámci trestního řízení, docházelo by k disproporci mezi právy obviněných ze spáchání trestného činu a právy jednotlivců, vůči kterým je v rámci prevence trestné činnosti opatření uplatněno, kdyby se tito jednotlivci nemohli odvolat na právo na spravedlivý proces.

Podle judikatury Ústavního soudu je trestní stíhání zásahem do osobní svobody, spojeným s určitým omezením práv, avšak ve svém důsledku se tak musí stát pouze z důvodů a způsobem,

[129] ZEDNER, L. Seeking Security by Eroding Rights: The Side-stepping of Due Process. In: GOOLD, B. J. – LAZARUS, L. *Security and Human Rights*. Portland: Hart Publishing, 2007, s. 264.
[130] Ibid., s. 266.

které stanoví zákon. *„Právě proto mezi základní zásady trestního řízení patří presumpce neviny, která kompenzuje toto omezení i v rámci přípravného řízení. Prokázání viny obviněného je možné pouze na základě nepochybně zjištěných skutečností za použití procesních prostředků, které trestní řád umožňuje proti obviněnému použít. Stejně tak obviněný může na svoji obranu uplatnit všechna práva, která mu dává trestní řád, zejména pak práva stanovená v § 33 tr. ř.“*[131]

Podle Antonyho Duffa nelze mluvit pouze o jedné presumpci neviny. Podle něj existují dvě kategorie presumpcí neviny. Jedna z nich je spjata s formálním obviněním ze spáchání trestného činu a musí být uplatňována v trestním řízení. Druhou kategorii presumpcí neviny nazývá Duff občanskou presumpcí neviny (*civic presumption of innocence*).[132] *„[Z]atímco presumpce neviny v trestním řízení je zvláštní a retrospektivní, jako presumpce neviny určitého údajného minulého trestného činu, občanská presumpce neviny je obecná a perspektivní: musíme býti považováni za nevinné nejen ve vztahu ke konkrétním minulým trestným činům, ale ve vztahu k budoucím trestným činům obecně*.“[133]

Duff nevylučuje, aby byla přijata určitá opatření, která zabraňují páchání trestných činů. Tato opatření nazývá Duff situační prevencí kriminality. Jako příklad této situační prevence kriminality uvádí bezpečnostní opatření na letištích.[134] Situační prevence kriminality může být uplatňována, pokud nepředstavuje pro osoby, vůči nimž je namířena, příliš velkou zátěž. Tento druh prevence kriminality a z toho vyplývající omezení občanské presumpce neviny lze akceptovat, pokud jsou tato opatření aplikována na všechny osoby bez rozdílu, popř. na osoby, které vykonávají nebo hodlají vykonat určitou činnost (cestování letadlem) nebo se nacházejí v určitém prostoru (prostor letiště). Za nepřijatelné omezení presumpce neviny považuje Duff, pokud jsou opatření v rámci situační prevence kriminality uplatňována selektivně, neboli pokud jsou uplatňována ve vztahu k jednotlivcům, kteří jsou příslušníky určité skupiny a jako takoví jsou považováni za podezřelé.[135] Za nepřijatelné omezení presumpce neviny by bylo možné považovat i opatření proti osobám v určitém prostoru pouze pro jejich biometrické charakteristiky, či zejména pro kombinaci biometrických charakteristik z toho důvodu, že za podezřelé jsou tyto osoby považovány *pro futuro*, tedy v době, kdy ke spáchání trestného činu vůbec nedošlo a není ani jisté, zda ke spáchání činu dojde.

Širší vnímání presumpce neviny sdílí i Kim Taipale. Podle něho by se měla presumpce neviny uplatňovat i nad rámec, pro Taipaleho, jejího příliš úzkého vymezení v rámci trestního řízení. Taipale vnímá presumpci neviny jako vztah liberálního státu a jednotlivce, jenž vyžaduje, aby označil jednotlivce za podezřelého pouze při splnění určitých podmínek. Těmito podmínkami by měly být konkrétní důkazy proti jednotlivci. Teprve pokud stát takové důkazy získá, může začít vykonávat svoji moc nad jednotlivcem.[136]

---

[131] Nález Ústavního soudu ze dne 14. června 1995, sp. zn. IV. ÚS 12/95.

[132] DUFF, A. Who must presume whom to be innocent of what? *Netherlands Journal of Legal Philosophy* [online]. 2013, Vol. 42, No. 3, s. 8 [cit. 2016-05-20]. Dostupné z: <http://ssrn.com/abstract=2190593>.

[133] Ibid., s. 9.

[134] Ibid., s. 9.

[135] Ibid., s. 10.

[136] TAIPALE, K. The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence. *IEEE Intelligent Systems* [online]. 2005, Vol. 20, No. 5, s. 82 [cit. 2016-05-20]. Dostupné z: <https://agentlab.ist.psu.edu/lab/publications/x5TandC.pdf>.

Ani ESLP netrvá v některých svých rozsudcích při uplatňování práv podle čl. 6 EÚLP na formálním obvinění ze spáchání trestného činu. Podle ESLP může být za obvinění ze spáchání trestného činu obecně považováno oficiální oznámení ze strany orgánů veřejné správy adresované určité osobě, že je obviněna z trestného činu. V některých případech mohou být práva podle čl. 6 EÚLP uplatňována i bez takovéhoto formálního obvinění, tedy i za situace, kdy jsou vůči jednotlivci uplatněna některá další opatření, která se svými důsledky *de facto* podobají výše uvedenému oficiálnímu oznámení a která mají rovněž podstatný vliv na situaci podezřelého (např. *Foti a další proti Itálii*[137]).

Názor, že masové využití technologií dohledu zasahuje do presumpce neviny, zastávají Jonida Milaj a Jeanne Pia Misfud Bonnici. Podle těchto autorek je sice presumpce neviny spjata s formálním obviněním ze spáchání trestného činu, nicméně masové rozšíření technologií dohledu a nedostatek transparentnosti jejich fungování činí z osob, nad nimiž je vykonáván dohled, podezřelé ze spáchání trestného činu, přestože nebyly ze spáchání trestného činu formálně obviněny. Při uplatňování zásady presumpce neviny po formálním obvinění se tyto osoby nemohou dovolat tohoto aspektu práva na spravedlivý proces, který je zaručen až obviněným.[138] Masovým rozšířením programů dohledu a výměny dat jsou údaje o jednotlivcích, kteří nebyli obviněni z trestného činu, k dispozici orgánům veřejné moci. Tito jednotlivci si nejsou vědomi, že jsou údaje o nich takto zaznamenávány a zpracovávány, nebo pokud si toho alespoň v hrubých rysech jsou vědomi, neví, jakými údaji o jejich osobě, aktivitách a pohybu orgány veřejné moci disponují.[139] Osoby, které jsou podrobeny dohledu, rovněž nevědí, jaké chování je považováno za podezřelé, a proto se nemohou takového jednání zdržet, aby odvrátily možný zásah do osobní integrity nebo jiné omezení, které je následkem takového chování. Pokud by osoby věděly, které chování je systémem považováno za potenciálně rizikové, bude se tato znalost vztahovat k určitému okamžiku. V případě využití algoritmu s funkcí učení se mohou profily rizikového chování v čase měnit.

S programy masového sledování bez nutnosti formálního obvinění konkrétní osoby ze spáchání trestného činu je presumpce neviny spojována i v Usnesení Evropského parlamentu ze dne 12. března 2014 o programu agentury NSA (USA) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí.[140] Podle tohoto usnesení jsou základní práva, zejména svoboda projevu, tisku, myšlení, svědomí, náboženského vyznání a sdružování, právo na soukromí, ochrana údajů a právo na účinné opravné prostředky, presumpce neviny a právo na spravedlivý proces a nediskriminaci, zakotvená v Listině EU a v EÚLP základními

[137] Rozsudek ESLP ze dne 10. prosince 1982, stíž. č. 7604/76, č. 7719/76, č. 7781/77, č. 7913/77 ve věci *Foti a další proti Itálii.*

[138] MILAJ, J. – MIFSUD BONNICI, J. P. Unwitting subjects of surveillance and the presumption of Inocence. *Computer Law and Security Review*. 2014, Vol. 30, No. 4, s. 426.

[139] Ibid., s. 425.

[140] Usnesení Evropského parlamentu ze dne 12. března 2014 o programu agentury NSA (USA) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí (2013/2188(INI)). *Evropský parlament* [online]. [cit. 2016-05-20]. Dostupné z: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=CS&ring=A7-2014-0139>.

kameny demokracie. Hromadné sledování lidí je s těmito základními kameny demokracie neslučitelné. Usnesení považuje programy sledování za další krok směrem k zavedení úplného preventivního státu, v němž se mění model trestního práva zavedený v demokratických společnostech, kde musí být každý zásah do základních práv podezřelého povolen soudcem nebo státním zástupcem na základě důvodného podezření a musí se řídit zákony. Místo něj se prosazuje kombinace vymáhání práva a zpravodajských činností s nejasnými a oslabenými právními zárukami, což často není v souladu s demokratickou kontrolou a vyvážeností a se základními právy, zejména s presumpcí neviny. Výše uvedené usnesení nakonec vyzývá členské státy Evropské unie, aby komplexně vyhodnotily a případně zrevidovaly své vnitrostátní právní předpisy a postupy týkající se činnosti zpravodajských služeb a zajistily, aby tyto předpisy a postupy podléhaly parlamentnímu a soudnímu dohledu a veřejné kontrole, aby respektovaly zásady legálnosti, nezbytnosti, přiměřenosti, řádného postupu, oznámení uživateli a transparentnosti a aby byly v souladu se standardy EÚLP a s povinnostmi členských států v oblasti základních práv, zejména pokud jde o ochranu údajů, soukromí a presumpci neviny. Směrnice Evropského parlamentu a Rady (EU) 2016/343 ze dne 9. března 2016, kterou se posilují některé aspekty presumpce neviny a právo být přítomen při trestním řízení před soudem,[141] mluví o zásadě presumpce neviny nejen ve vztahu k obviněnému z trestného činu, tak jak je tomu v čl. 6 EÚLP a v čl. 48 Listiny EU, ale i ve vztahu k podezřelému. Výše uvedená směrnice by se podle recitálu 12 měla vztahovat na fyzické osoby, které jsou podezřelé nebo obviněné v trestním řízení. Měla by se použít od okamžiku, kdy se určitá osoba stane podezřelou nebo je obviněna ze spáchání trestného činu nebo údajného trestného činu, tudíž již předtím, než byla příslušnými orgány členského státu úředním sdělením nebo jinak uvědomena o tom, že je podezřelou nebo obviněnou osobou. Tato směrnice by se měla použít ve všech stadiích trestního řízení až do nabytí právní moci konečného rozhodnutí o tom, zda podezřelá nebo obviněná osoba uvedený trestný čin spáchala.

Princip presumpce neviny jako aspekt práva na spravedlivý proces můžeme tedy klasifikovat dvěma způsoby. Jako presumpci neviny v užším smyslu, tak jak ji chápou lidsko-právní dokumenty a judikatura, jež musí být zachovávána vůči tomu, proti němuž se vede trestní řízení, tedy vůči tomu, proti kterému byly již učiněny konkrétní formální kroky výše uvedeného procesu, přičemž EÚLP mluví dokonce o obviněném ze spáchání trestného činu.

Další klasifikaci presumpce neviny můžeme nazvat presumpcí neviny v širším smyslu, která působí vůči osobám, nad kterými je vykonáván dohled prostřednictvím systémů, které takový dohled umožňují nad každým, kdo se nachází v určitém prostoru. Uplatňování presumpce neviny v širším smyslu by mělo zabránit orgánům, které dohled vykonávají, užívat při výkonu dohledu algoritmu, který se při dohledu zaměřuje na určité jednotlivce z důvodu jejich rasy, národnosti nebo příslušnosti k etnické, sociální nebo jiné předem vymezené skupině, jejíž příslušníci jsou v důsledku sociálního třídění a diskriminace *a priori* podezřelí z páchání trestné činnosti. K dohledu nad takovým jednotlivcem není totiž třeba, aby tento trestný čin spáchal. Stačí, když je algoritmem vyhodnocen jako nositel určité biometrické

[141] Směrnice Evropského parlamentu a Rady (EU) 2016/343 ze dne 9. března 2016, kterou se posilují některé aspekty presumpce neviny a právo být přítomen při trestním řízení před soudem.

charakteristiky nebo jako příslušník některé sociální skupiny. Systémy, které se na základě algoritmu zaměřují při výkonu dohledu selektivně nebo ve zvýšené míře na příslušníky těchto skupin, porušují podle našeho názoru princip presumpce neviny v širším smyslu a tím i právo na spravedlivý proces.

8.3 Právo na ochranu soukromí

Dohled ve své současné postpanoptické formě v sobě zahrnuje hrozbu ze ztráty soukromí. Algoritmické rozhodování v reálném čase na základě vyhodnocení chování jednotlivce či vyhodnocením jiných dat získaných dohledem, případně ve spojení s databázemi obsahujícími osobní údaje, může ve svém důsledku vést k narušení soukromí např. tím, že se na určitého jednotlivce systém dohledu detailněji zaměří a dohled nad takovou osobou zintenzivní či upozorní odpovědné osoby, jejichž následný zásah proti potenciálně rizikové osobě rovněž může soukromí této osoby narušit.

V českém ani v mezinárodním nebo evropském právu neexistuje legální definice soukromí. V roce 1890 uveřejnili Samuel D. Warren a Louis Brandeis v Harward Law Review legendární článek *The Right to Privacy*. Právo na soukromí je podle těchto autorů *„právo na to být ponechán o samotě* (*right to be let alone*)*“*.[142] Warren a Brandeis navazují na soudce Cooleyho, který právo být ponechán o samotě považoval za nástroj k ochraně jednotlivců před v té době novými vynálezy a obchodními praktikami zasahujícími do soukromého a rodinného života. Technologickou novinkou byl na konci 19. století fotoaparát.[143]

Teoreticky rozlišujeme vícero dimenzí soukromí.[144] Dimenze relační se vztahuje k právu jednotlivce kontrolovat své okolí a navazovat, popř. udržovat vztahy mezi třetími osobami (rodinou, přáteli apod.). Relační soukromí mají jednotlivci ve vztahu k publikacím informací o svých blízkých.[145]

S relačním soukromím souvisí také soukromí prostorové. Prostorové soukromí představuje zejména ochranu obydlí, tedy prostoru, kde jednotlivec žije buďto sám, nebo ho sdílí s jinými osobami. V tomto prostoru není jednotlivec vystaven kontrole ostatních. Prostorové soukromí je chráněno i přepisy občanského práva. Je to klasická *actio negatoria*, která je v českém právu upravena v § 1042 zákona č. 89/2012 Sb., občanský zákoník.

Ve svém obydlí má jednotlivec svobodu volby jednání. Tato svoboda je omezená převážně předpisy správního a trestního práva. Prostorové soukromí je chráněno právními předpisy

[142] WARREN, S. – BRANDEIS, L. The Right to Privacy, *Harward Law Review* [online]. 1890, Vol. 6, No. 4. [cit. 2012-03-15]. Dostupné z: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

[143] Ibid.

[144] Srov. WÁGNEROVÁ, E. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, V. *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 54.

[145] EMERY, Ch. M. Relational Privacy – A Right To Grieve In The Information Age: Halting The Digital Dissemination Of Death-Scene Images. *Rutgers Law Journal* [online]. 2011, Vol. 42, No. 3, s. 771 [cit. 2014-03-05]. Dostupné z: <http://lawjournal.rutgers.edu/sites/lawjournal.rutgers.edu/files/issues/07EmeryVol.42.3.pdf>.

před neodůvodněným narušením ze strany státu. Jako zásadní vnímá nezbytnost ochrany této svobody v obydlí jednotlivce Ústavní soud. *„Domovní svoboda jako ústavně zaručené právo plynoucí z čl. 12 Listiny svou povahou a významem spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní a dalšími ústavně zaručenými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu, jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec, je nutno respektovat a důsledně chránit; zcela právem proto spadá tato ochrana pod ochranu ústavní, neboť – posuzováno jen z poněkud jiného hlediska – jde o výraz úcty k právům a svobodám člověka a občana (čl. 1 úst. zák. č. 1/1993 Sb.).“*[146]

V případě *Chappell proti Spojenému království*[147] byla prohledána půjčovna videokazet, jež byla provozována v bydlišti pana Chappella. ESLP však v tomto případě shledal příkaz jako dostatečně konkrétní a odůvodněný. Do sféry prostorového soukromí náleží vše, kde jednotlivec není vystaven kontrole ostatních, tedy nejen obydlí, např. i prostory, kde jednotlivec vykonává práci (*Niemietz proti Německu*). Do prostorového soukromí náleží i automobil (*Uzun proti Německu*[148]).

Další dimenzi soukromí představuje dimenze komunikační neboli důvěrnost komunikace a korespondence. Jako korespondence nejsou chráněny pouze klasické dopisy, nýbrž i telefonní hovory (*Amann proti Švýcarsku*[149]), e-maily a osobní komunikace prostřednictvím internetu (*Copland proti Spojenému království*). Monitorování a odposlouchávání komunikace představuje narušení soukromého života. V případě *Huvig proti Francii*[150] dospěl ESLP k závěru, že právo Francouzské republiky nedává dostatečné záruky při používání odposlechů (zákon neomezoval lhůtu pro nasazení odposlechů, chyběla povinnost vést záznamy o odposleších apod.). Přestože se v praxi výše zmíněná opatření přijímala, chybělo jejich zákonné zakotvení. Francouzský zákon nebyl podle ESLP dostatečně předvídatelný (*foreseeable*). Nepředvídatelné a nejasné bylo i britské právo v případu *Malone proti Spojenému království.*[151] Podle ESLP to ale neznamená, že by byla vyžadována taková zákonná úprava, že by jednotlivec mohl předvídat, kdy bude odposlouchávám. Musí však ze zákona mít možnost vědět, za jakých okolností je policie oprávněna odposlech provést.

I v případě, že je zákon dostatečně jasný a předvídatelný, musí mít odposlech legitimní cíl a musí být nezbytný v demokratické společnosti. Jedině taková právní úprava splňuje požadavek orgánů veřejné moci na ochranu bezpečnosti a veřejného pořádku a zároveň poskytuje dostatečné záruky proti zneužití odposlechů (*Klass proti Německu*). Další dimenzi soukromí můžeme nazvat dimenzí tělesné a psychické integrity. Narušení tělesné integrity představuje např. osobní prohlídka (*Gillan a Quinton proti Spojenému království*[152]) či omezení na osobní svobodě.

[146] Nález Ústavního soudu ČR ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.
[147] Rozsudek ESLP ze dne 30. března 1989, stíž. č. 10461/83 ve věci *Chappell proti Spojenému království*.
[148] Rozsudek ESLP ze dne 2. prosince 2010, stíž. č. 35623/05 ve věci *Uzun proti Německu*.
[149] Rozsudek ESLP ze dne 16. února 2000, stíž. č. 27798/95 ve věci *Amann proti Švýcarsku*.
[150] Rozsudek ESLP ze dne 24. dubna 1990, stíž. č. 11105/84 ve věci *Huvig proti Francii*.
[151] Rozsudek ESLP ze dne 2. srpna 1984, stíž. č. 8691/79 ve věci *Malone proti Spojenému království*.
[152] Rozsudek ESLP ze dne 12. ledna 2010, stíž. č. 4158/05 ve věci *Gillan a Quinton proti Spojenému království*.

Dimenzí soukromí, která souvisí s kontrolou nad informacemi jednotlivců o sobě, je dimenze informační. Přestože v současné době bývá tato dimenze soukromí nesprávně zaměňována se soukromím jako takovým,[153] je informační soukromí důležitou součástí práva na ochranu soukromého života. Podle judikatury Ústavního soudu je právo na ochranu soukromého života nezadatelným lidským právem, které zahrnuje, mimo jiné, právo fyzické osoby rozhodnout podle vlastního uvážení, zda, popřípadě v jakém rozsahu a jakým způsobem, mají být skutečnosti jejího osobního soukromí zpřístupněny jiným. K omezení takového práva lze podle Ústavního soudu přikročit za účelem ochrany základních práv jiných osob, anebo za účelem ochrany veřejného zájmu.[154]

Data mining a profilování se vyznačují ztrátou kontroly nad informacemi o sobě, v jejímž důsledku dochází k zásahu do informačního soukromí jednotlivce. Z podstaty data miningu a profilování vyplývá, že jednotlivec nemůže mít kontrolu nad informacemi o sobě, jelikož tyto informace byly z dat vygenerovány dodatečně. Jednotlivec nemůže vykonávat kontrolu nad informací, která v minulosti neexistovala.[155] K zásahu do soukromí dochází i při výkonu dohledu.[156]

Přestože legální definice soukromí chybí, je ochrana soukromí garantována celou řadou lidsko-právních dokumentů. V evropském kontextu je nejdůležitějším dokumentem čl. 8 EÚLP. Podle odst. 1 tohoto ustanovení má každý právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Druhý odstavec čl. 8 EÚLP vymezuje podmínky, za nichž může stát do práva na soukromý a rodinný život v konkrétní věci zasáhnout. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Interpretačním vodítkem pojmu soukromý a rodinný život může být Rezoluce Rady Evropy 428 (1970) o masových komunikačních médiích a lidských právech.[157] Právo na soukromí spočívá podle této Rezoluce *„převážně v právu žít svůj život s minimálními zásahy. Jedná se o soukromý, rodinný a domácí život, fyzickou a mravní integritu, čest a pověst, uvedení do falešného světla, odhalení nemístných a znevažujících skutečností, neoprávněné zveřejnění soukromých fotografií, ochranu proti zneužití soukromých sdělení, ochranu proti zveřejnění poskytnutých nebo přijatých důvěrných informací. Ti, kdo svým jednáním podnítili odhalení skutečností ze soukromí, na nějž si následně stěžují, se nemůžou*

[153] GUTWIRTH, S. *Privacy and the Information Age*. Lanham: Rowman & Littlefield Publishers, 2002, s. 16.
[154] Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06.
[155] Srov. CLARKE, R. *Profiling: A Hidden Challenge to the Regulation of Data Surveillance.* op. cit.
[156] Srov. LYON, D. *The Electronic Eye: The Rise of the Surveillance Society*. op.cit., s. 17, nebo SOLOVE, D. Taxatomy of Privacy. *University of Pennsylvania Law Review* [online]. 2006, Vol. 154, No. 3, s. 500 [cit. 2014-05-14]. Dostupné z: <https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%25282006%2529.pdf>.
[157] Resolution 428 (1970) Declaration on mass communication media and Human Rights ze dne 23. ledna 1970. *Rada Evropy* [online] [cit. 2013-03-08]. Dostupné z: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=15842&lang=en>.

dovolávat práva na soukromí".[158] Ochrana soukromého a rodinného života je garantována i Listinou EU. Podle čl. 7 Listiny EU každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence či jiných druhů komunikace. Na rozdíl od čl. 8 EÚLP nezmiňuje Listina EU specifické legitimní důvody, na jejichž základě by bylo možné právo na soukromý a rodinný život omezit. Bude-li třeba posoudit legitimnost zásahu do soukromého a rodinného života, bude aplikován druhý odstavec čl. 8 EÚLP. Toto vyplývá z čl. 53 odst. 3 Listiny EU. Pokud Listina EU obsahuje práva odpovídající právům zaručeným EÚLP, jsou smysl a rozsah těchto práv stejné jako ty, které jim přikládá uvedená úmluva. Toto ustanovení nebrání tomu, aby právo Unie poskytovalo širší ochranu.

Na omezení základního práva se kromě příslušného ustanovení EÚLP uplatní čl. 52 odst. 1 Listiny EU, podle něhož každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého. Omezení základního práva musí odpovídat cílům obecného zájmu uznaným Evropskou unií. Podle výkladového stanoviska jsou jimi cíle obsažené v čl. 3 Smlouvy o Evropské unii[159] a další zájmy chráněné Smlouvou o Evropské unii či Smlouvou o fungování Evropské unie.[160]

V českém právním řádu je ochrana soukromí jako základní právo zakotvena v čl. 7 odst. 1 Listiny, který zaručuje nedotknutelnost osoby a jejího soukromí. Omezena může být jen

---

[158] *„The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially. Those who, by their own actions, have encouraged indiscreet revelations, about which they complain later on, cannot avail themselves of the right to privacy."*

[159] Čl. 3 Smlouvy o Evropské unii:

1. Cílem Unie je podporovat mír, své hodnoty a blahobyt svých obyvatel.
2. Unie poskytuje svým občanům prostor svobody, bezpečnosti a práva bez vnitřních hranic, ve kterém je zaručen volný pohyb osob ve spojení s vhodnými opatřeními týkajícími se ochrany vnějších hranic, azylu, přistěhovalectví a předcházení a potírání zločinnosti.
3. Unie vytváří vnitřní trh. Usiluje o udržitelný rozvoj Evropy, založený na vyváženém hospodářském růstu a na cenové stabilitě, vysoce konkurenceschopném sociálně tržním hospodářství směřujícím k plné zaměstnanosti a společenskému pokroku a na vysokém stupni ochrany a zlepšování kvality životního prostředí. Podporuje vědecký a technický pokrok.
   Bojuje proti sociálnímu vyloučení a diskriminaci, podporuje sociální spravedlnost a ochranu, rovnost žen a mužů, mezigenerační solidaritu a ochranu práv dítěte.
   Podporuje hospodářskou, sociální a územní soudržnost a solidaritu mezi členskými státy.
   Respektuje svou bohatou kulturní a jazykovou rozmanitost a dbá na zachování a rozvoj evropského kulturního dědictví.
4. Unie vytváří hospodářskou a měnovou unii, jejíž měnou je euro.
5. Ve svých vztazích s okolním světem Unie zastává a podporuje své hodnoty a zájmy a přispívá k ochraně svých občanů. Přispívá k míru, bezpečnosti, udržitelnému rozvoji této planety, k solidaritě a vzájemné úctě mezi národy, volnému a spravedlivému obchodování, vymýcení chudoby, ochraně lidských práv, především práv dítěte, a k přísnému dodržování a rozvoji mezinárodního práva, zejména k dodržování zásad Charty Organizace spojených národů.
6. Unie sleduje své cíle vhodnými prostředky na základě pravomocí, které jsou jí Smlouvami svěřeny.

[160] Vysvětlení k Listině základních práv ze dne 14. prosince 2007 (2007/C 303/02).

v případech stanovených zákonem. Respektování soukromého a rodinného života je dále garantováno v čl. 10 odst. 2 Listiny. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

EÚLP umožňuje jednotlivcům a skupinám dovolávat se porušení svého práva na soukromí ze strany smluvního státu. V takovém případě hovoříme o vertikálním účinku EÚLP. Stát má především povinnost respektovat soukromí jednotlivce a zdržet se jakýkoliv zásahů do něho s výjimkou případů uvedených ve druhém odstavci.

K určení, zda došlo k porušení čl. 8 EÚLP, používá ESLP test skládající se ze čtyř otázek, které si na základě tohoto článku pokládá. První otázkou, jež si ESLP klade, je existence zásahu do soukromí. ESLP zkoumá, zda došlo k zásahu do soukromého a rodinného života. ESLP nezakládá svoje posouzení, zda došlo k zásahu, na žádné předchozí judikaturou vymezené definici soukromého a rodinného života. Dále ESLP zkoumá, zda k omezení práva na soukromí došlo na základě zákona nebo v souladu se zákonem, např. soudním rozhodnutím. Zákon musí být rovněž předvídatelný. V rozsudku *Malone proti Spojenému království* ESLP uvádí, že zákon musí být sice předvídatelný, nikoliv však do té míry, aby umožňoval jednotlivcům předvídat, kdy je pravděpodobné, že budou odposloucháváni, a přizpůsobí tomu své jednání.

Pro výkon tajného dohledu, zvláště pak pro případy, v nichž se jedná o použití odposlechů, ESLP požaduje minimální záruky, které by měly být stanoveny v zákoně, aby se zabránilo zneužívání moci. Těmito zárukami je kategorie trestných činů, u kterých lze vydat příkaz k odposlechu, vymezení kategorií osob, u nichž lze odposlech provést, doba trvání odposlechu, postup, který je třeba dodržet při analýze a uchovávání údajů, opatření, která mají být přijata v případě sdělování údajů třetím osobám, a okolnosti, za nichž mohou nebo musí být záznamy vymazány nebo zničeny (např. *Szabó a Vissy proti Maďarsku*[161]).

Třetí otázkou je, zda omezení práva spočívá v důvodech vymezených v druhém odstavci. Omezení práva na soukromí musí mít legitimní cíl (*legitimate aim*). Co je legitimním cílem, stanoví EÚLP ve druhém odstavci čl. 8. K omezení práva může dojít pouze v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Poslední otázkou je, zda je toto omezení v demokratické společnosti nezbytné. ESLP se při svých úvahách nespokojí pouze se zjištěním, že omezení práva na soukromí mělo legitimní cíl. Omezení musí být navíc v demokratické společnosti nezbytné, tzn. existuje naléhavá společenská potřeba (*pressing social need*) pro toto omezení a zásah do práva na soukromí musí být proporcionální k cíli, jehož má být dosaženo. Proporcionalita spočívá v posouzení a) kritéria vhodnosti, tj. zda zásah do soukromí vedl k požadovanému cíli, b) kritéria potřebnosti, tedy zda neexistují jiné méně omezující opatření k dosažení stanoveného cíle

[161] Rozsudek ESLP ze dne 12. ledna 2016, stíž. č. 37138/14 ve věci *Szabó a Vissy proti Maďarsku*.

a c) kritéria proporcionality stricto sensu, který znamená porovnání významu zásahu se zájmy jednotlivce na ochraně jeho základních práv a svobod.[162] Při posuzování, zda je omezení práva na soukromí v demokratické společnosti nezbytné, zkoumá ESLP v konkrétním případě prostor pro uvážení (*margin of appreciation*) veřejných orgánů smluvního státu. Prostor pro uvážení se liší podle práva, které bylo omezeno, podle důvodů pro omezení i podle konkrétní situace v projednávané kauze.[163] Zásahem do soukromí je podle ESLP sledování polohy policií pomocí GPS (*Uzun proti Německu*[164]) nebo sledování orgány činnými v trestním řízení nebo zpravodajskými službami (např. *Rotaru proti Rumunsku*).

Podle ustálené judikatury ESLP nemusí porušit EÚLP pouze stát, který sám zasáhne do práva na soukromí (tzv. vertikální účinek směrnice). Čl. 8 EÚLP může stát porušit i tím, že nepřijme opatření, aby zásahu do soukromí jednotlivce ze strany jiného soukromého subjektu zabránil. Zde mluvíme o pozitivní povinnosti státu.[165] Stát může porušit své pozitivní povinnosti nejen nepřijetím opatření, které by zabránilo v zásahu, ale též nepřijetím právní úpravy, která by porušení práva na soukromí zabránila.[166] V kontextu dohledu může stát tedy porušit své pozitivní povinnosti tím, že nepřijme opatření, která by ochránila jednotlivce v případě porušení práva na soukromí ze strany soukromých subjektů, pokud v právní úpravě státu chybí ustanovení, která by porušení práva na soukromí zabránila. Tato ustanovení mohou mít např. podobu vhodných záruk proti zneužití osobních údajů. Těmito zárukami mohou být specifikace účelu zpracování osobních údajů, kvalita údajů, transparentnost, omezení užití údajů, bezpečnost údajů, právo subjektu údajů na přístup k údajům, právo na opravu neaktuálních nebo chybných údajů a v neposlední řadě existence dozorového orgánu.[167]

Jak již bylo výše uvedeno, k zásahu do soukromí může dojít v případě algoritmického rozhodování v reálném čase. Zásah do soukromí v případě algoritmického rozhodování v reálném čase může mít podobu zásahu do informačního soukromí, kdy jednotlivec, nad kterým je vykonáván dohled, ztrácí kontrolu nad informacemi o sobě, nad tím, kdo má k informacím přístup, na základě dat z jakých databází je tento jednotlivec vyhodnocen jako potenciálně rizikový či komu jsou údaje o něm dále předávány pro účely vyhodnocení rizika. K výkonu dohledu za účelem posouzení rizika pro národní či veřejnou bezpečnost a následného algoritmického vyhodnocení dochází typicky v předem vymezených prostorách. V těchto prostorách je chování jednotlivce monitorováno. Již při vstupu do předem vymezených prostor může systém pomocí techniky rozpoznávání obličejů zobrazit identifikační údaje jednotlivce, a upozornit tedy na jeho přítomnost v místě, nad nímž je vykonáván dohled. Právo na informační soukromí je narušeno právě nedostatkem kontroly nad informacemi o své osobě, které tohoto jednotlivce identifikují jako určitou osobu v situaci, kde tento jednotlivec nepředpokládá, že těmito informacemi budou orgány veřejné moci disponovat.

---

[162] Viz např. GÜTTLER, V. – MATEJKA, J. *K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů*, op. cit., s. 1040.

[163] NIEUWENHUIS, A. J. *Tussen privacy en persoonlijkheidsrecht*. Nijmegen: Ars Aequi Libri, 2001, s. 116.

[164] Rozsudek ESLP ze dne 2. září 2010, stíž. č. 35623/05 ve věci *Uzun proti Německu.*

[165] Např. Rozsudek ESLP ze dne 5. září 2017, stíž. č. 61496/08 ve věci *Bărbulescu proti Rumunsku*.

[166] Např. Rozsudek ESLP ze dne 26. března 1985, stíž. č. 8978/80 ve věci *X. a Y. proti Nizozemí*.

[167] GÜTTLER, V. – MATEJKA, J. *K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů*. op. cit., s. 1042.

Do soukromí může být zasaženo i narušením některé z jeho dalších dimenzí. Těmito dimenzemi je dimenze relační neboli vztahová, kdy se systém na základě vyhodnocení algoritmem zaměří i na osoby, s nimiž se potenciálně riziková osoba nachází, nebo s nimiž se v místě, nad nímž je vykonáván dohled, setkala. Systém může na základě chování těchto osob, popřípadě ve spojení s dalšími informacemi, které má k dispozici, určit sociální vazby mezi těmito osobami. Dále může dojít i k zásahu do komunikačního soukromí. K tomuto zásahu dojde v případě, že se systém po vyhodnocení potenciálního rizika určité osoby zaměří na její komunikaci, např. prostřednictvím mobilního telefonu.

V neposlední řadě může na základě algoritmického vyhodnocení rizika dojít i k zásahu do soukromí v podobě fyzické integrity jednotlivce. Pokud tohoto jednotlivce systém vyhodnotí jako potenciálně rizikového, případně jako osobu, u níž je riziko pro národní či veřejnou bezpečnost zvýšené, a upozorní na tuto skutečnost odpovědné osoby, může dojít k přijetí opatření proti jednotlivci. Odpovědné osoby mohou takového jednotlivce podrobit osobní prohlídce či ho dokonce omezit na osobní svobodě.

Na tomto místě je nutné zmínit koncept rozumného očekávání soukromí (*reasonable expectation of privacy*). Rozumné očekávání soukromí vyjadřuje, zda a do jaké míry se dotčená osoba na své soukromí mohla v konkrétní situaci spoléhat. Rozumné očekávání soukromí v sobě zahrnuje dvě kritéria. Prvním z nich je subjektivní kritérium, které vyjadřuje aktuální očekávání soukromí v určité situaci. Druhým, objektivním kritériem je posouzení, zda společnost uznává toto očekávání jako přiměřené. Tento test byl poprvé užit v rozsudku Nejvyššího soudu Spojených států *Katz v. United States.*[168]

ESLP též uplatňuje při svém rozhodování koncept rozumného očekávání soukromí nebo také legitimního očekávání (*legitimate expectation*), přestože výslovně daná kritéria nezmiňuje. Legitimní očekávání soukromí nepovažuje ESLP na rozdíl od judikatury amerických soudů za rozhodující kritérium pro určení, zda došlo k porušení práva na soukromý a rodinný život dle čl. 8 EÚLP. Legitimní očekávání má v judikatuře ESLP spíše doplňující charakter. Určujícím kritériem porušení čl. 8 EÚLP je pro ESLP výše zmíněný čtyřstupňový test.

Rozumné očekávání soukromí má podle ESLP zaměstnanec na pracovišti ohledně svých soukromých hovorů, pokud mu nebylo předem řečeno, že je jeho telefon odposloucháván (*Halford proti Spojenému království,*[169] *Copland proti Spojenému království*[170]), rozumné očekávání má i podezřelý ve výslechové místnosti, jestliže nebyl upozorněn na snímání výslechu na kameru a následného použití záznamů u soudu (*Perry proti Spojenému království*[171]).

[168] Rozsudek Nejvyššího soudu Spojených států ze dne 18. prosince 1967 *Katz v. United States*, 389 U.S. 347 (1967).
[169] Rozsudek ESLP ze dne 27. května 1997, stíž. č. 20605/92 ve věci *Halford proti Spojenému království*.
[170] Rozsudek ESLP ze dne 3. dubna 2007, stíž. č. 62617/00 ve věci *Copland proti Spojenému království*.
[171] Rozsudek ESLP ze dne 17. července 2003, stíž. č. 63737/00 ve věci *Perry proti Spojenému království*.

Někteří autoři se však k rozumnému očekávání staví kriticky. Rouvroy celý koncept rozumného očekávání soukromí odmítá.[172] Solove uvádí, že *„[…] soukromí není jen empirickou a historickou otázkou, podle níž daná společnost posuzuje, co je a má být považováno za soukromé. […] Pokud bychom se zaměřili pouze na očekávání soukromí, jež v současnosti lidé mají, naše pojetí soukromí by se vzhledem k rostoucímu sledování ve světě modernu neustále smršťovalo. Stejně tak by mohla vláda postupně formovat občany, aby akceptovali odposlechy nebo jiná narušení soukromí, čímž by se změnilo soukromí očekávání celé společnosti".*[173]

Přestože ESLP legitimní očekávání nehodnotí jako rozhodující kritérium, mohl by v konkrétním případě při posuzování zásahu do soukromí učiněného rozhodováním na základě algoritmu v reálném čase posoudit, zda měla osoba, nad níž byl vykonáván dohled, legitimní očekávání soukromí v konkrétním místě a čase.

Lze se domnívat, že ESLP v konkrétním případě rozhodne, že dohledem a algoritmickým rozhodnutím o jednotlivci dochází k zásahu do soukromí tohoto jednotlivce. ESLP bude poté zkoumat, zda k zásahu došlo na základě zákona nebo v souladu se zákonem. Pokud tento soud shledá, že algoritmické rozhodování, na jehož základě došlo k zásahu do soukromí, nemá oporu v zákoně nebo zákon není dostatečně předvídatelný a neobsahuje dostatečné záruky proti zneužití moci, rozhodne ESLP, že čl. 8 EÚLP byl porušen.

Pokud ESPL shledá, že má zásah do soukromí oporu v zákoně, který je navíc dostatečně předvídatelný, bude zkoumat, zda existují legitimní důvody pro omezení práva stanovené ve druhém odstavci čl. 8 EÚLP. Legitimními důvody budou v případě algoritmického rozhodování v reálném čase požadavky národní bezpečnosti. Nakonec bude ESLP zkoumat, zda je v demokratické společnosti omezení soukromí nezbytné, tj. zda existuje naléhavá společenská potřeba a omezení je přiměřené sledovaným cílům. Pokud budou existovat dostatečné zákonné záruky, ESLP shledá omezení soukromí algoritmickým rozhodováním jako nezbytné v demokratické společnosti pro potřeby národní bezpečnosti, zvláště pokud bude v konkrétním případě naléhavá potřeba k ochraně života a zdraví osob. Jak uvedl ESLP v případě *Klass proti Německu*, demokratické společnosti se v dnešní době ocitly v ohrožení vysoce sofistikovanými formami špionáže a terorismu. V důsledku tohoto ohrožení musí být stát schopen účinně čelit takovým hrozbám, třeba i tajným výkonem dohledu a sledováním. ESLP v rozsudku *Klass* uznal nezbytnost existence právních předpisů umožňujících dohled, neboť jsou nezbytné v demokratické společnosti v zájmu ochrany národní bezpečnosti a pro předcházení narušení veřejného pořádku a zločinnosti, pokud tyto předpisy obsahují dostatečné záruky proti zneužití moci.

[172] ROUVROY, A. Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence Privacy. *Studies in Ethics, Law, and Technology* [online]. 2008, Vol. 2, No. 1, s. 26 [cit. 2014-05-14]. Dostupné z: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984>.

[173] SOLOVE, D. J. Conceptualizing Privacy. *California Law Review* [online]. 2002, Vol. 90, s. 1142 [cit. 2014-04-20]. Dostupné z : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103>.

Pokud by byl dohled a algoritmické rozhodování, na jehož základě by bylo zasaženo do práva na soukromí, vykonáván masově nebo na místech, kde by nebyla hrozba teroristického útoku vzhledem k současné situaci akutní (např. mimo letiště), lze předpokládat, že by ESLP takový dohled shledal v rozporu s čl. 8 EÚLP. Tomuto názoru nasvědčuje rozsudek z nedávné doby, a to rozsudek ve věci případu *Szabó a Vissy proti Maďarsku*.

Podle názoru ESLP v případu *Szabó a Vissy proti Maďarsku* je přirozeným důsledkem hrozby terorismu, že se vlády snaží používat moderní technologie pro předcházení teroristickým útokům. Technologie používaná pro tyto účely učinila podle ESLP v posledních letech významný pokrok a dosáhla takové úrovně sofistikovanosti, která je pro průměrného občana jen těžko představitelná. Ve výše uvedeném případě mohl být dohled vykonáván nad každým občanem Maďarska. *„Tváří v tvář tomuto pokroku musí soud zkoumat otázku, zda je vývoj metod dohledu, jenž má za následek obrovské množství shromážděných údajů, doprovázen současným vývojem právních záruk zajišťujících dodržování práv občanů garantovaných Úmluvou. Tyto údaje jsou často spojeny s dalšími informacemi o podmínkách, za kterých byly orgány poprvé zachyceny, jako je čas a místo, jakož i používané zařízení, vytváření počítačových souborů, digitálních fotografií, elektronických a textových zpráv a podobně. Ve skutečnosti by se příčilo účelu snažení vlád udržet terorismus na uzdě, a obnovovat důvěru občanů ve své schopnosti zachovávat veřejnou bezpečnost, pokud by teroristická hrozba byla paradoxně nahrazena hrozbou neomezené výkonné moci narušující soukromou sféru občanů z titulu výkonu nekontrolovaného dalekosáhlého dohledu a dalších výsad. V této souvislosti Soud rovněž odkazuje na připomínky Soudního dvora Evropské unie, a zejména na stanovisko zvláštního zpravodaje OSN, které zdůrazňují důležitost příslušných právních předpisů obsahujících dostatečné záruky proti rozšíření technických možností státních orgánů odposlouchávat soukromé informace.“*[174]

Podle ESLP je možný výkon dohledu, pokud je takový zásah do práva na soukromí nezbytný v demokratické společnosti. Musí se jednat o opravdovou nutnost (*strict necessity*), která spočívá ve dvou aspektech. Za prvé musí být zásah nutný pro zachování demokratických institucí. Za druhé musí být účelem zásahu získání důležitých informací ve zvláštní operaci. Ostatní případy užití technologií k tajnému dohledu považuje ESLP podle rozsudku *Szabó a Vissy* za zneužitelné.

[174] Rozsudek ESLP ze dne 12. ledna 2016, stíž. č. 37138/14 ve věci *Szabó a Vissy proti Maďarsku*.

Část IX. Závěr

Algoritmy a neuronové sítě (někdy též nazývané umělou inteligencí) využívají soukromé i veřejné subjekty k vyhodnocování nejrůznějších aspektů lidského chování a lidské existence. Od hodnocení finanční situace po analýzu chování za účelem k posouzení míry rizika, které může jednotlivec znamenat pro národní bezpečnost nebo veřejný pořádek. V některých případech tato technologie na základě vložených dat a modelů nebo/a dat a modelů, které si sama vytvořila, rozhodne o dalším postupu. Důvodem pro využívání těchto technologií je rychlost takového rozhodování a víra v objektivitu automatizovaného rozhodování čili představa, že algoritmy vyhodnotí situaci nebo chování člověka správným způsobem. Využití automatizovaného rozhodování se objevuje stále častěji tím, jak roste objem dat a možnosti jejich zpracování na jedné straně a nástroje pro zpracování na straně druhé.

V této práci jsme se zabývali automatizovaným rozhodováním v rámci dohledu nad jednotlivci v určitém prostoru, ve kterém může dojít k zásahu na podkladě automatizovaného rozhodnutí okamžitě po vyhodnocení nastalé situace nebo události v místě dohledu (vlaková nádraží či jiná veřejná místa s vysokým počtem osob). Jestliže systém detekuje určitou aktivitu či situaci, může být na základě vyhodnocení zaznamenané aktivity nebo situace rozhodnuto algoritmem o dalším postupu. Vyhodnotí-li systém na základě profilů chování jednotlivce jako potenciálně nebezpečného, mohou být na něj upozorněny bezpečnostní složky, které mohou proti tomuto jednotlivci zasáhnout ve snaze zabránit potenciálně nebezpečné události. Chování jednotlivce může být dále ovlivněno přímo systémem, např. automatickým odepřením vstupu. Takové automatizované rozhodování může porušovat základní lidská práva a svobody, a to zejména právo nebýt diskriminován, právo na spravedlivý proces a právo na soukromí.

Zákaz diskriminace může být při výše uvedeném automatizovaném rozhodování porušeno tím, že s jednotlivci určité rasy, etnicity, národnosti, pohlaví, věku nebo jako s příslušníky určité sociální skupiny bude zacházeno jinak, než s osobami, které do těchto kategorií nespadají. Tito jednotlivci mohou být pouze na podkladě svoji příslušnosti klasifikováni jako rizikoví či rizikovější pro veřejnou nebo národní bezpečnost. Jednotlivci, kteří jsou klasifikováni jako rizikoví, jsou pak podrobeni zvýšenému dohledu a následně mohou být i omezeni na svých právech. Toto rozhodnutí může být prezentováno jako objektivní, neboť o rizikovosti jednotlivce bylo rozhodnuto na základě automatizovaně.

Automatizované rozhodování použité při dohledu může znamenat zásah do práva na spravedlivý proces, přestože v této době není zahájeno žádné soudní ani správní řízení. Aspektem práva na spravedlivý proces je totiž presumpce neviny. Presumpci neviny můžeme dělit na presumpci neviny v užším smyslu, tedy po formálním obvinění ze spáchání trestného

činu, a presumpci neviny v širším smyslu. Presumpce neviny v širším smyslu působí vůči osobám, nad kterými je vykonáván dohled. Uplatňování presumpce neviny v širším smyslu by mělo zabránit orgánům veřejné moci užívat při výkonu dohledu algoritmu, který se při dohledu zaměřuje na určité jednotlivce z důvodu jejich rasy, národnosti, nebo příslušnosti k etnické, sociální nebo jiné skupině, na jejíž příslušníky pohlíží algoritmus na základě předem definovaných profilů jako na podezřelé z páchání trestné činnosti, přestože v době výkonu dohledu se tito jednotlivci žádného trestného činu nedopustili ani nedopouštějí.

Automatizované rozhodování může znamenat zásah do práva na soukromí. Právo na soukromí znamená mimo jiné i právo jednotlivce na kontrolu nad informacemi o sobě, neboli právo na rozhodování, zda a v jakém rozsahu a jakým způsobem mají být skutečnosti jejího soukromí zpřístupněny jiným. Při výkonu dohledu a následném automatizovaném rozhodování na podkladě informací získaných při výkonu tohoto dohledu spolu s informacemi z nejrůznějších databází, dochází k narušení informačního soukromí, neboť jednotlivec nemá zpravidla povědomí o přítomnosti dohledu a využíváním informací, natož aby měl nad informacemi kontrolu. K porušení práva na soukromí, tentokrát v podobě psychické a fyzické integrity, dochází i za situace, kdy systém vyhodnotí jednotlivce jako rizikového a na základě takového rozhodnutí je proti jednotlivci učiněn zásah ze strany odpovědných osob.

Základními nedostatky automatizovaného rozhodování jsou především, za prvé, nedostatek transparentnosti, tedy nevědomost osob, nad kterými je vykonáván dohled, o způsobu dohledu, o fungování automatizovaného rozhodovávání a o informacích, které jsou pro rozhodování využívány a za druhé, víra v objektivitu automatizovaného rozhodování, na kterém se zdánlivě nepodílí lidský faktor. Lidský faktor je ovšem přítomen ve fázi designování modelu pro rozhodování ať již importováním dat a informací, podle kterých bude systém rozhodovat, nebo tím, že se algoritmus sám naučí určitá data a informace při rozhodování upřednostňovat na základě předchozích, lidských hodnocení situace.

Základním stavebním kamenem automatizovaného rozhodování musí být, tedy kromě uplatnění silného atributu spravedlnosti ve smyslu procesním i hmotněprávním, především přesvědčivá argumentace a kvalitní výklad dotčených právních předpisů realizovaný ve formě důsledného odůvodnění a transparentních procesů, jež doprovází rozhodnutí samotná[175]. V rámci procesu rozhodování tak musí ten, kdo rozhoduje, aplikovat jak nabyté teoretické i praktické poznatky, tak i důsledně domýšlet reálný dopad svých rozhodnutí, včetně určitého preventivního působení takového rozhodnutí do budoucnosti.

Potencionalita automatizovaného rozhodování je však natolik široká a nepředvídatelná, že lze důvodně očekávat, že nepřinese pouze pozitivní efekty v oblasti efektivity a realizace

[175] Ústavní soud konstatuje, že porušením práva na spravedlivý proces podle čl. 36 odst. 1 Listiny základních práv a svobod může být i situace, kdy v hodnocení skutkových zjištění absentuje určitá část skutečností, která vyšla v řízení najevo, event. nebo tím spíše – pokud ji účastník řízení namítal, nicméně obecný soud ji náležitým způsobem v celém souhrnu posuzovaných skutečností nezhodnotil, aniž by např. dostatečným způsobem odůvodnil jejich irelevantnost. Pokud obecný soud postupuje takto, dopouští se mj. i libovůle, zakázané v článku 2 odst. 2 Listiny základních práv a svobod. (Z nálezu Ústavního soudu sp. zn. I.ÚS 2232/07 ze dne 2. 6. 2010).

práva. Naopak lze předpokládat, že v blízké budoucnosti povede mimo jiné k odosobnění většiny rozhodovacích procesů, jakož i k vytváření vysoce efektivních nástrojů zneužití práva. Následkem předmětné automatizace se totiž rozhodování přesune o něco dále od člověka, dojde tak určitému „útěku od osobní odpovědnosti", a ve svém důsledku k enormnímu nárůstu rozhodovacích procesů realizovaných výlučně na základě chladně-kalkulujících algoritmů, a to jak v oblasti práva procesního i hmotného, veřejného či soukromého, resp. smluvního. Důsledkem bude nejenom zrychlení a zefektivnění samotné realizace práva, ale také vznik řady dalších nespecifických právních nástrojů, jež svými charakteristickými rysy mohou svádět své tvůrce či adresáty k sofistikovanému patologickému zneužití, lhostejno, zda se tak stane v důsledku rovnosti, formalismu, distributivní či procesní spravedlnosti.

Z uvedeného tak plyne několik věcí. Soudní či správní automatizovaná rozhodování v současném právním a technologickém prostředí naráží na řadu poměrně odlišných doktrín, přístupů i dílčích problémů. Samotná efektivita právní regulace je v této oblasti nedílně svázána se schopností pružně, a především rozumně a efektivně reagovat na rozvoj informačních a komunikačních technologií, jakož i operativně řešit existující problémy či rozpory jednotlivých dotčených hodnot či práv v této oblasti. Převažující ryze pozitivistický (resp. normativní) přístup všech hlavních aktérů automatizovaného rozhodování bude v blízké budoucnosti čelit celé řadě výzev, a to napříč širokého spektra odvětví; samotná technologie automatizovaného rozhodování a její aktuální trendy by však nikdy neměly být upřednostněny před průběžným a zejména svědomitým zkoumáním samotné technické podstaty automatizovaného rozhodování.[176] V rámci systémů automatizovaného rozhodování tak musí být implementovány určité ochranné či kontrolní mechanismy průběžně vyhodnocující všechny podstatné faktory, jež toto rozhodování přímo či nepřímo ovlivňují, a to včetně jejich dopadu do právních vztahů.

Jako naprosto klíčové se jeví trvat na důsledné aplikaci všech souvisejících právních i technologických záruk proti případnému zneužití samotné technologické podstaty automatizovaného rozhodování za současné existence transparentního postupu doprovázeného legitimním právním titulem pro zpracování relevantních osobních údajů a dat; to vše se zřetelem na právní rámec veřejnoprávní regulace na jedné straně, se zřetelem k ochraně lidských práv na straně druhé, kde, jak ostatně trefně poznamenal V. Güttler,[177] na vedoucím místě nutně stojí ochrana základního práva na lidskou důstojnost, tedy práva, k jehož naplnění prakticky téměř všechna ostatní lidská práva přímo či nepřímo směřují. Pouze všechny tyto aspekty, v právním, společenském i technologickém kontextu,[178] mohou vést k efektivní ochraně jak individuálních práv i svobod, tak i samotného veřejného zájmu a integrity všech relevantních lidskoprávních zásad.

[176] K obdobným závěrům v oblasti např. nekalé soutěže viz PODSZUN, R. Kartellrecht in der Internet- Wirtschaft: Zeit für den more technological approach, *Wirtschaft und Wettbewerb*. 2014, Nr. 3, s. 1.

[177] GÜTTLER, V. – MATEJKA, J. *K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů.* op. cit., s. 1055.

[178] MATEJKA, J. – KRAUSOVÁ, A. – GÜTTLER, V. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie.* [online]. 2018, č. 17, s. 91–129. [cit. 2019-12-01]. Dostupné z: <https://journals.muni.cz/revue/article/view/8801>.

Část X. Seznam použité literatury

Odborné monografie

BAUMAN, Z. *Liquid Modernity*. Cambridge: Polity Press, 2002, 228 s. ISBN 0-7456-2410-3.

BAUMAN, Z. – LYON, D. *Tekutý dohled*. Olomouc: Broken Books, 2013, 150 s. ISBN 978-80-905309-1-1.

BEJČEK, J. Chytré smlouvy jakožto smlouvy „chytře" protiprávní. In: SUCHOŽA, J. – HUSÁR, J. – HUČKOVÁ, R. *Právo Obchod Ekonomika IX*. Košice: UPJŠ v Košiciach, Právnická fakulta, 2019, 571 s. ISBN 978-80-8152-775-3.

BĚLINA, M. – DRÁPAL, L. a kol. *Zákoník práce: komentář.* Praha: C. H. Beck, 2012, 1616 s. ISBN 978-80-7179-251-2.

BOBEK, M. – BOUČKOVÁ, P. – KÜHN, Z. (eds). *Rovnost a diskriminace*. Praha: C. H. Beck, 2007, 471 s. ISBN 978-80-7179-584-1.

BOULAY, B. – BRÉMOND, F. Activity Recognition. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, 340 s. ISBN: 978-1-848-21433-0.

DE HERT, P. Biometrics and the Challenge to Human Rights in Europe. In: CAMPISI, P. *Security and Privacy in Biometrics*. Dordrecht: Springer, 2013, 438 s. ISBN 978-1447152293.

GUTWIRTH, S. *Privacy and the Information Age*. Lanham: Rowman & Littlefield Publishers, 2002, 143 s. ISBN 0-7425-1746-2.

KABELOVÁ DOLEJŠOVÁ, K. *Zákaz diskriminace jako právní problém* v judikatuře *Evropského soudu pro lidská práva*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2012, 182 s. ISBN 978-80-87146-60-6.

KNAPP, V. *O možnosti použití kybernetických metod v právu*. Praha: Nakladatelství Československé akademie věd, 1963, 242 s.

KNAPP, V. *Právo a informace*. Praha: Academia, 1988, 289 s.

KNUTH, D, E. *Umění programování. 1. díl. Základní algoritmy*. Brno: Computer press, 2008, 649 s. ISBN 978-80-251-2025-5.

LESSIG, L. *Code V.2*. New York: Basic Books, 2006, 426 s. ISBN 978-1441437648.

LYON, D. Surveillance as social sorting. Computer codes and mobile bodies. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003, 287 s. ISBN 0-203-99488-4.

LYON, D. *The Electronic Eye: The Rise of the Surveillance Society*. Minneapolis: University of Minnesota Press, 1994, 270 s. ISBN 0-8166-2515-8.

MAGGIO, S. – HAUGEARD, J.-E. – MEDEN, B. – LUVISON, B. – AUDIGIER, R. – BURGER, B. – PHAM, Q. C. Tracking of Objects of Interest in a Sequence of Images. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, 340 s. ISBN 978-1-848-21433-0.

MARRAUD, D. – CÉPAS, B. – SULZER, J.-F. – MULAT, Ch. – SÈDESA, F. Posteriori Analysis for Investigative Purposes. In: DUFOUR, J.-Y. *Intelligent Video Surveillance Systems*. London: ISTE, 2013, 322 s. ISBN 978-1-848-21433-0.

MARX, G. T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press, 1988, 283 s. ISBN 0-520-06969-2.

MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, ISBN 978-80-904248-7-6, 256 s. Dostupné [online] z: <https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf>.

MATEJKA, J. Zaměstnanec jako objekt profilování a automatizovaného rozhodování dle obecného nařízení o ochraně osobních údajů. In: HROMADA, M. *Pocta Jarmile Pavlátové k 85. narozeninám*. Plzeň: Západočeská univerzita v Plzni, 2018, 223 s. ISBN 978-80-261-0809-2.

MAYER-SCHÖNBERGER, V. – CUKIER, K. *Big Data: a revolution that will transform how we live, work and think*. London: John Murray, 2013, 242 s. ISBN 978-1-84854-790-2.

MICHAEL, MG – MICHAEL, K. A Note on "Überveillance". In: MICHAEL, MG. *The Second Workshop on the Social Implications of National Security. From Dataveillance to* Überveillance *and the Realpolitik of the Transparent Society* [online]. 2007, 306 s. [cit. 2014-08-14]. Dostupné z: <http://works.bepress.com/cgi/viewcontent.cgi?article=1050&context=kmichael>.

MILLER, M. I. –VAILLANT, M. – HOFFMAN, W. – SCHUEPP, P. 2D-to-3D Systems Face Recognition. In: VOELLER, J. G. *Detection and Intelligent Systems for Homeland Security (1)*. Somerset, US: Wiley, 2014, 129 s. ISBN 9781118787366.

MINELLI, M. – CHAMBERS, M. – DHIRAJ, A. B*ig Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*. Hoboken: John Wiley & Sons, Inc., 2012, 224 s. ISBN 978-1118147603.

MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The ethical, Legal and Social Context.* Dordrecht: Springer, 2011, 354 s. ISBN 978-9400738911.

MORDINI, E. – ASHTONS, H. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, E. – TZOVARAS, D. *Second Generation Biometrics: The ethical, Legal and Social Context*. Dordrecht: Springer, 2011, 354 s. ISBN 978-9400738911.

NIEUWENHUIS, A. J. *Tussen privacy en persoonlijkheidsrecht*. Nijmegen: Ars Aequi Libri, 2001, 232 s. ISBN 9789069164281.

NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, D. (eds). *Surveillance as social sorting: Privacy, risk and automated discrimination*. London: Routledge, 2003, 287 s. ISBN 0-203-99488-4.

PODSZUN, R. Kartellrecht in der Internet- Wirtschaft: Zeit für den more technological approach. *Wirtschaft und Wettbewerb.* 2014, Nr. 3, s. 1.

POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s. ISBN 978-80-87284-22-3.

REVETT, K. *Behavioral Biometrics. A Remote Access Aproach*. Hoboken: Wiley, 2008, 250 s. ISBN 978-0470518830.

SLOBOGIN, Ch. *Proving the Unprovable. The Role of Law, Science, and Speculation in Adjudicating Culpability and Dangerousness.* Oxford: Oxford University Press, 2007, 193 s. ISBN 0-19-518995-7.

STEINER, Ch. *Automate This. How Algorithms Came to Rule Our World*. London: Penguin Books, 2012, 256 s. ISBN 978-1-101-57215-3.

SVOBODA, P. et al. *Právní a daňové aspekty e-obchodu*. Praha: Linde Praha, 2001, 464 s. ISBN 80-7201-311-4.

VAN ,T HOF, Ch. – VAN EST, R. – DAEMEN, F. *Check In / Check Out. The Public Space as an Internet of Things.* Rotterdam: NAi Publishers, 2011, 157 s. ISBN 978-90-5662-808-6.

WÁGNEROVÁ, E. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, V. *Právo na soukromí*. Brno: Masarykova univerzita, 2011, 212 s. ISBN 978-80-210-5449-3.

WÁGNEROVÁ, E. a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer ČR, 2012, 931 s. ISBN 978-80-7357-750-6.

WACHS, M. – FINK, C. N. Y. – LOUKAITOU-SIDERIS, A. – TAYLOR, B. D. Securing Public Transit Systems. In: HAKIM, S. – ALBERT, G. – SHIFTAM, Y. *Securing Transporation Systems*. Hoboken: Wiley, 2016, 388 s.

WIENER, N. *The Human Use of Human Beings: cybernetics and society*. London: Free Association Books, 1989, 199 s. ISBN 978-1-118-97793-4.

YANNOPOULOS, A. – ANDRONIKOU, V. – VARVARIGOU, T. Behavioural Biometric Profiling and Ambient Intelligence. In: HILDEBRANDT, M. – SERGE, G. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008, 374 s. ISBN 978-1402069130.

ZEDNER, L. Seeking Security by Eroding Rights: The Side-stepping of Due Process. In: GOOLD, B. J. – LAZARUS, L. *Security and Human Rights*. Portland: Hart Publishing, 2007, s. 391. ISBN 978-1-84113-608-0.

Periodické publikace

BRUNTON, F. – NISSENBAUM, H. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* [online]. 2011, Vol. 16, No. 5. [cit. 2016-05-08]. Dostupné z: <http://firstmonday.org/article/view/3493/2955>.

CLARKE, R. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* [online]. 1997 [cit. 2014-06-15]. Dostupné z: <http://www.rogerclarke.com/DV/Intro.html#InfoPriv>.

CLARKE, R. *Profiling: A Hidden Challenge to the Regulation of Data Surveillance* [online]. 1993 [cit. 2012-03-15]. Dostupné z: <http://www.rogerclarke.com/DV/PaperProfiling.html>.

CRAWFORD, K. – SCHULTZ, J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Review* [online]. 2014, Vol. 55, No. 1, s. 93–128 [cit. 2016-04-30]. Dostupné z: <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr>.

CRAWFORD, K. *Can An Algorithm be Agonistic? Scenes of Contest in Calculated Publics* [online]. 2016, 9 s. [cit. 2016-04-30]. Dostupné z: <http://www.katecrawford.net/docs/CanAnAlgorithmBeAgonistic-Ap>.

DUFF, A. Who must presume whom to be innocent of what? *Netherlands Journal of Legal Philosophy* [online]. 2013, Vol. 42, No. 3, 18 s. [cit. 2016-05-20]. Dostupné z: <http://ssrn.com/abstract=2190593>.

EMERY, Ch. M. Relational Privacy – A Right To Grieve In The Information Age: Halting The Digital Dissemination Of Death-Scene Images. *Rutgers Law Journal* [online]. 2011, Vol. 42, No. 3, s. 765–818 [cit. 2014-03-05]. Dostupné z: <http://lawjournal.rutgers.edu/sites/lawjournal.rutgers.edu/files/issues/07EmeryVol.42.3.pdf>.

GILLESPIE, T. *The relevance of algorithms* [online]. 2012, 32 s. [cit. 2016-04-30]. Dostupné z: <http://www.tarletongillespie.org/essays/Gillespie%20-%20The%20Relevance%20of%20Algorithms.pdf>.

GÜTTLER, V. – MATEJKA, J. K otázkám některých základních lidských práv a svobod v souvislosti s právní ochranou biometrických údajů. *Právník*. 2016, roč. 155, č. 12, s. 1033–1056. ISSN 0231-6625.

HITZLER, P. – JANOWICZ, K. *Linked Data, Big Data, and the 4th Paradigm* [online]. 2013, 3 s. [cit. 2014-06-15]. Dostupné z: <http://www.semantic-web-journal.net/system/files/swj488.pdf>.

HOSPEDALES, T. – GONG S. – XIANGS, T. *A Markov Clustering Topic Model for Mining Behaviour in Video* [online]. 2009, 8 s. [cit. 2018-02-01]. Dostupné z: <http://www.eecs.qmul.ac.uk/~sgg/papers/HospedalesGongXiang_ICCV09.pdf>.

HU, M. Biometric Cyberintelligence and the Posse Comitatus Act. *Emory Law Journal*. 2017, Vol. 66, No. 4, s. 697–763. ISSN 0094-4076.

INTRONA, L. D. – WOOD, D. Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance & Society* [online]. 2004, Vol. 2, No. 2/3, s. 177–198 [cit. 2016-05-13]. Dostupné z: <http://www.surveillance-and-society.org/cctv.htm\nhttp://eprints.lancs.ac.uk/28931/>.

KNIGH, H. System improves automated monitoring of security cameras. New approach uses mathematics to reach a compromise between accuracy, speed. *MIT News* [online]. 5. 6. 2012 [cit. 2016-06-01]. Dostupné z: <http://news.mit.edu/2012/auto-video-surveillance-algorithm-0605>.

KOOIJ, J. F. P. – ENGLEBIENNE, G. – GAVRILA, D. A Non-parametric Hierarchical Model to Discover Behavior Dynamics from Tracks. *Proc. of the European Conference on Computer Vision* [online], Vol. 6, Florence, Italy, 2012, s. 271–283 [cit. 2016-05-27]. Dostupné z: <https://www.informationsystems.foi.se/main.php/A-Non-parametric-Hierarchical-Model-to-Discover-Behavior-Dynamics-from-Tracks.pdf?fileitem=7340168>.

KOOPS, B.-J. Technology and the Crime Society: Rethinking Legal Protection. *Selected Works* [online]. 2009, 23 s. [cit. 2014-05-14]. Dostupné z: <http://works.bepress.com/bert_jaap_koops>.

KUNER, Ch. *The 'Internal Morality' of European Data Protection Law.* November 24, 2008. [online] [cit. 2019-12-08]. Dostupné z: <http://ssrn.com/abstract=1443797>.

LIEM, M. – GAVRILA, D. M. Person Appearance Modeling and Orientation Estimation using Spherical Harmonics. *Proc. of the IEEE International Conference on Automatic Face & Gesture*, Shanghai [online], China, 2013, 6 s. [cit. 2016-05-27]. Dostupné z: <https://www.informationsystems.foi.se/main.php/Person-Appearance-Modeling-and-Orientation-Estimation-using-Spherical-Harmonics.pdf?fileitem=7340161>.

LYON, D. – HAGGERTY, K. D. The Surveillance Legacies of 9/11: Recalling, Reflecting on, and Rethinking Surveillance in the Security Era. *Canadian Journal of Law and Society*. 2012, Vol. 27, No. 2, s. 291–300. ISSN 0829-3201.

MATEJKA, J. – KRAUSOVÁ, A. – GÜTTLER, V. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, č. 17, s. 91–129. [cit. 2019-12-01]. Dostupné z: <https://journals.muni.cz/revue/article/view/8801>.

MILAJ, J. – MIFSUD BONNICI, J. P. Unwitting subjects of surveillance and the presumption of Inocence. *Computer Law and Security Review*. 2014, Vol. 30, No. 4, s. 419–428. ISSN 0267-3649.

MORNIN, J. D. NSA Metadata Collection And The Fourth Amendment. *Berkeley Technology Law Journal* [online]. 2014, Vol. 29, s. 985–1006 [cit. 2016-03-15]. Dostupné z: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2042&context=btlj>.

MORRIS, V. R. Identity and Biometrics Enabled Intelligence (BEI) Sharing for Transnational Threat Actors. *Small Wars Journal* [online]. 22. 3. 2016 [cit. 2018-02-01]. Dostupné z: <http://smallwarsjournal.com/jrnl/art/identity-and-biometrics-enabled-intelligence-bei-sharing-for-transnational-threat-actors>.

NORRIS, C. – ARMSTRONG, G. CCTV and the Social Structuring of Surveillance. *Crime Prevention Studies* [online]. 1999, Vol. 10, s. 157–178 [cit. 2016-04-30]. Dostupné z: <http://www.popcenter.org/library/crimeprevention/volume_10/06-NorrisArmstrong.pdf>.

NORRIS, C. Video Charts: Algorithmic Surveillance. *Criminal Justice Matters* [online]. 1995, Vol. 20, No. 1, s. 157–178 [cit. 2016-05-06]. Dostupné z: <http://www.popcenter.org/library/crimeprevention/volume_10/06-NorrisArmstrong.pdf>.

RAGHAVENDRA, R. – BUSCH, Ch. Improved Face Recognition by Combining Information from Multiple Cameras in Automatic Border Control System. *12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* [online]. 2015, s. 1 [cit. 2016-06-01]. Dostupné z: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7301748&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F7295687%2F7301715%2F07301748.pdf%3Farnumber%3D7301748>.

ROSENZWEIG, P. Proposals for Implementing the Terrorism Information Awareness System. *Heritage.org* [online]. 7. 8. 2003 [cit. 2016-04-30]. Dostupné z: <http://www.heritage.org/research/reports/2003/08/proposals-for-implementing-the-terrorism-information-awareness-system>.

ROUVROY, A. – BERNS, T. Gouvernementalité algorithmique et perspectives d'émancipation: le disparate comme condition d'individualisation par la relation? *Réseaux* [online]. 2013, Vol. 177, No. 1, 23 s. [cit. 2016-05-18]. Dostupné z: <http://works.bepress.com/antoinette_rouvroy/47/>.

ROUVROY, A. – STIEGLER, B. Le régime de vérité numérique. De la gouvernementalité algorithmique à un nouvel État de droit. *Scio* [online]. 2015, Vol. 4, s. 113–140 [cit. 2016-04-30]. Dostupné z: <https://pure.fundp.ac.be/ws/files/13160335/socio_1251_4_le_regime_de_verite_numerique.pdf>.

ROUVROY, A. *"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data* [online]. 2011, 37 s. [cit. 2016-05-04]. Dostupné z: <http://works.bepress.com/antoinette_rouvroy/64/>.

ROUVROY, A. L'algorithme n'est „pas un système de prédiction mais d'intervention". *Medipart* [online]. 2015, s. 1–3 [cit. 2016-04-30]. Dostupné z: <https://www.academia.edu/12603930/Lalgorithme_nest_pas_un_système_de_prédiction_mais_d_intervention_Entretien_réalisé_par_Jérôme_Hourdeaux_pour_Mediapart_25_mai_2015>.

ROUVROY, A. Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence Privacy. *Studies in Ethics, Law, and Technology* [online]. 2008, Vol. 2, No. 1, 54 s. [cit. 2014-05-14]. Dostupné z: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984>.

RUBINSTEIN, I. S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law* [online]. 2013, Vol. 3, No. 2, s. 1–14 [cit. 2014-05-10]. Dostupné z: <http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.full>.

SCHULZ, D. M. – GILBERT, S. *Video Surveillance Uses by Rail Transit Agencies. A Synthesis of Transit Practice* [online]. Washington, 2011, 79 s. [cit. 2018-03-05]. Dostupné z: <http://www.safetyvision.com/sites/safetyvision.com/files/rail_1.pdf>.

SOLOVE, D. Taxatomy of Privacy. *University of Pennsylvania Law Review* [online]. 2006, Vol. 154, No. 3, s. 477–560 [cit. 2014-05-14]. Dostupné z: <https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%25282006%2529.pdf>.

SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review* [online]. 2002, Vol. 90, s. 1087–1155 [cit. 2014-04-20]. Dostupné z: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103>.

SPREEUWERS, L. J. – HENDRIKSE, J. A. – GERRITSEN, K. J. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport. *Biometrics Special Interest Group (BIOSIG) – Proceedings of the International Conference* [online]. 2012, s. 99–110 [cit. 2016-06-01]. Dostupné z: <http://cs.emis.de/LNI/Proceedings/Proceedings196/99.pdf>.

TAIPALE, K. The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence. *IEEE Intelligent Systems* [online]. 2005, Vol. 20, No. 5, s. 80–82 [cit. 2016-05-20]. Dostupné z: <https://agentlab.ist.psu.edu/lab/publications/x5TandC.pdf>.

THUY, O. Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints. *The Verge* [online]. 10. 10. 2017 [cit. 2018-02-24]. Dostupné z: <https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium>.

TOPAK, Ö. E. – BRACKEN-ROCHE, C. – SAULNIER, A. – LYON, D. From Smart Borders to Perimeter Security: The Expansion of Digital Surveillance at the Canadian Borders. *Geopolitics*. 2015, Vol. 20, č. 4, s. 880–899. ISSN 1465-0045.

VELASTIN, S. A. – BOGHOSSIAN, B. A. – PING LAI LO, B. – SUN, J. – VICENCIO-SILVA, M. A. PRISMATICA: Toward Ambient Intelligence in Public Transport Environments. *IEEE Transactions On Systems, Man, and Cybernetics—Part A: Systems and Humans* [online]. 2005, Vol. 35, No. 1, s. 164–182 [cit. 2016-06-01]. Dostupné z: <http://ids.snu.ac.kr/w/images/9/9e/AmI04.pdf>.

WACHTER, S. – MITTELSTADT, B. – FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*. 2017, Vol. 7, No. 2, s. 76–99. ISSN 2044-3994.

WARREN, S. – BRANDEIS, L. The Right to Privacy, *Harward Law Review* [online]. 1890, Vol. 6, No. 4. [cit. 2012-03-15]. Dostupné z: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

ZARSKY, T. Governmental Data Mining and its Alternatives. *Penn State Law Review* [online]. 2011, Vol. 116, No. 2, s. 285–330 [cit. 2016-05-04]. Dostupné z: <http://www.pennstatelawreview.org/116/2/116 Penn St. L. Rev. 285.pdf>.

Ostatní prameny

EVROPSKÁ KOMISE. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a Sociálnímu výboru a Výboru regionů. Umělá inteligence pro Evropu. 2018 [cit. 2019-12-03]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0237&from=CS>.

EVROPSKÁ KOMISE. Odborná skupina na vysoké úrovni pro umělou inteligenci (AI HLEG). Etické pokyny pro zajištění důvěryhodnosti UI. 2019. [online] [cit. 2019-12-03]. Dostupné z: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

PRACOVNÍ SKUPINA 29. Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679. Úřad pro ochranu osobních údajů [online]. 38 s. [2019-10-30]. Dostupné z: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31893>.

PRACOVNÍ SKUPINA 29. Vodítka k souhlasu podle Nařízení 2016/679. Úřad pro ochranu osobních údajů [online]. 32 s. [2019-10-30] Dostupné z: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896>.

Public Perceptions of Privacy and Security in the Post-Snowden Era. *Pew Research Center* [online]. 12. 11. 2014 [cit. 2014-05-14]. Dostupné z: <http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pd>.

Resolution 428 (1970) Declaration on mass communication media and Human Rights ze dne 23. ledna 1970. *Rada Evropy* [online] [cit. 2013-03-08]. Dostupné z: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=15842&lang=en>.

Usnesení Evropského parlamentu ze dne 12. března 2014 o programu agentury NSA (USA) pro sledování, subjektech členských států pro sledování a dopadech na základní práva občanů EU a na transatlantickou spolupráci v oblasti spravedlnosti a vnitřních věcí (2013/2188(INI)). *Evropský parlament* [online] [cit. 2016-05-20]. Dostupné z: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=CS&ring=A7-2014-0139>.

Část XI. Seznam použité judikatury

Rozsudek ESLP ze dne 10. prosince 1982, stíž. č. 7604/76, č. 7719/76, č. 7781/77, č. 7913/77 ve věci *Foti a další proti Itálii.*

Rozsudek ESLP ze dne 2. srpna 1984, stíž. č. 8691/79 ve věci *Malone proti Spojenému království.*

Rozsudek ESLP ze dne 26. března 1985, stíž. č. 8978/80 ve věci *X. a Y. proti Nizozemí*.

Rozsudek ESLP ze dne 30. března 1989, stíž. č. 10461/83 ve věci *Chappell proti Spojenému království*.

Rozsudek ESLP ze dne 24. dubna 1990, stíž. č. 11105/84 ve věci *Huvig proti Francii.*

Rozsudek ESLP ze dne 18. února 1991, stíž. č. 12033/86 ve věci *Fredin proti Švédsku.*

Rozsudek ESLP ze dne 27. května 1997, stíž. č. 20605/92 ve věci *Halford proti Spojenému království*.

Rozsudek ESLP ze dne 29. dubna 1999, stíž. č. 25088/94, 28331/95 a 28443/95 ve věci *Chassagnou a ostatní proti Francii.*

Rozsudek ESLP ze dne 16. února 2000, stíž. č. 27798/95 ve věci *Amann proti Švýcarsku.*

Rozsudek ESLP ze dne 17. července 2003, stíž. č. 63737/00 ve věci *Perry proti Spojenému království.*

Rozsudek ESLP ze dne 24. července 2003, stíž. č. 40016/98 ve věci *Karner proti Rakousku*.

Rozsudek ESLP ze dne 3. dubna 2007, stíž. č. 62617/00 ve věci *Copland proti Spojenému* království.

Rozsudek ESLP ze dne 10. března 2009, stíž. č. 44256/06 ve věci *Turan Cakir proti Belgii*.

Rozsudek ESLP ze dne 12. ledna 2010, stíž. č. 4158/05 ve věci *Gillan a Quinton proti Spojenému království.*

Rozsudek ESLP ze dne 2. prosince 2010, stíž. č. 35623/05 ve věci *Uzun proti Německu*.

Rozsudek ESLP ze dne 24. července 2012, stíž. č. 47159/08 ve věci *B. H. proti Španělsku.*

Rozsudek ESLP ze dne 12. ledna 2016, stíž. č. 37138/14 ve věci *Szabó a Vissy proti Maďarsku.*

Rozsudek ESLP ze dne 5. září 2017, stíž. č. 61496/08 ve věci *Bărbulescu proti Rumunsku.*

Rozsudek SDEU ze dne 19. října 2016, věc C-582/2014 (*Breyer*).

Nález Ústavního soudu ze dne 14. června 1995, sp. zn. IV. ÚS 12/95.

Nález sp. zn. Pl. ÚS 21/96, Sbírka nálezů a usnesení Ústavního soudu, svazek 7, nález č. 13.

Nález Ústavního soudu ČR ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.

Nález sp. zn. 19/98, Sbírka nálezů a usnesení Ústavního soudu, svazek 13, nález č. 19.

Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06.

Nález Ústavního soudu ze dne 2. června 2010, sp. zn. I.ÚS 2232/07.

Rozsudek Nejvyššího soudu Spojených států ze dne 18. prosince 1967 *Katz v. United States*, 389 U.S. 347 (1967).

Bundesverfassungsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.

Část XII. Seznam použitých zkratek

CCTV	Closed Circuit Television
GDPR nebo nařízení	Nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu údajů
ESLP	Evropský soud pro lidská práva
EÚLP	Evropská úmluva o lidských právech a základních svobodách
Listina	Listina základních práv a svobod
Listina EU	Listina základních lidských práv Evropské unie
SDEU	Soudní dvůr Evropské Unie
Směrnice 2016/680	Směrnice Evropského Parlamentu a Rady (EU) 2016/680 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