ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XXXVIII
2/2019

POLICAJNÉ PROFILOVANIE V KONTEXTE ZÁKLADNÝCH ĽUDSKÝCH PRÁV A SLOBÔD[1]

JUDr. Matúš Mesarčík, LL.M.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra správneho práva a environmentálneho práva
Ústav práva informačných technológií a práva duševného vlastníctva
matus.mesarcik@flaw.uniba.sk

Policajné profilovanie v kontexte základných ľudských práv a slobôd

Predkladaná štúdia sa zaoberá prediktívnou analýzou pri práci policajných zložiek – policajným profilovaním. Pri využití tejto metódy policajné zložky môžu „predpovedať" budúcu kriminalitu a predchádzať tak protiprávnej činnosti. Prvá časť štúdie charakterizuje danú metódu a poskytuje prehľad jej využitia v Spojených štátoch amerických, Rakúsku a Českej republike. Zároveň je analyzovaná možnosť jej využitia v Slovenskej republike. Druhá časť štúdie sa zaoberá základnými ľudskými právami a slobodami, ktoré môžu byť pri policajnom profilovaní ohrozené. Konkrétne ide o právo na súkromie, zákaz nediskriminácie a právo na spravodlivé súdne konanie. Tretia časť štúdie sa venuje konkrétnym inštitútom Policajnej smernice, ktorá upravuje spracúvanie osobných údajov pri vyšetrovaní protiprávnych konaní policajnými zložkami.

Policía predictiva en el contexto de los derechos humanos y las libertades fundamentales

El estudio trata del análisis predictivo en el trabajo de las fuerzas policiales – policía predictiva. Al usar este método, las fuerzas policiales pueden „predecir" el futuro crimen y prevenir las actividades ilegales. La primera parte del estudio caracteriza dicho método y proporciona una visión general de su uso en los Estados Unidos de América, Austria y la República Checa.

[1] Tento príspevok je výstupom z grantu Univerzity Komenského č. UK/208/2019 a názvom Umelá inteligencia a ochrana súkromia. (Zodpovedný riešiteľ: JUDr. Matúš Mesarčík, LL.M.).

Al mismo tiempo, se analiza la posibilidad de su uso en la República Eslovaca. La segunda parte del estudio se ocupa de los derechos humanos y las libertades fundamentales que pueden ser amenazados por la policía predictiva. Específicamente se trata del derecho a la privacidad, la no discriminación y el derecho a un juicio justo. La tercera parte del estudio se dedica a las disposiciones específicas de la Directiva de la Policía, que regula el procesamiento de datos personales durante la investigación de los actos ilegales por parte de las fuerzas policiales.

Predictive policing in the context of fundamental human rights and freedoms

The study deals with predictive analysis in the work of the police forces – predictive policing. By using this method, police forces can "predict" future crime and prevent illegal activity. The first part of the study characterizes the method and provides an overview of its use in the United States, Austria and the Czech Republic. At the same time, the possibility of its use in the Slovak Republic is evaluated. The second part of the study deals with the fundamental human rights and freedoms that may be threatened by predictive policing. Specifically, these include the right to privacy, non-discrimination and the right to a fair trial. The third part of the study is devoted to specific provisions of the Police Directive, which regulates the processing of personal data during the investigation of illegal acts by police forces.

Kľúčové slová: policajné profilovanie, ochrana súkromia, policajná smernica, ne-diskriminácia

Palabras clave: policía predictiva, privacidad, directiva policial, no discriminación

Keywords: predictive policing, privacy, police directive, non-discrimination

Úvod

Americký autor vedecko-fantastickej literatúry Philip K. Dick v roku 1956 publikoval jednu zo svojich najznámejších poviedok – *Minority report*. Dej tejto poviedky sa odohráva v budúcnosti, kde špeciálne policajné zložky využívajú pri svojej práci tzv. *prekogov*, osoby, ktoré dokážu predpovedať budúcnosť. Na základe takýchto predpovedí sú policajné zložky schopné protiprávnemu konaniu zabrániť ešte skôr ako reálne nastane, pričom ich činnosť znižuje kriminalitu v spoločnosti na absolútne minimum.

Spoločnosť ešte síce nepokročila tak, aby prostredníctvom jednotlivcov dokázala predpovedať budúcnosť (to ostáva naďalej v rovine vedecko-fantastickej literatúry či filmu), ale predpovedanie správania

na základe technológie je prítomné už v súčasnosti. Súkromné spoločnosti často prispôsobujú svoje interné, ale aj vonkajšie procesy na základe rozhodnutí, ktoré boli prijaté po využití dátovej analýzy. Ilustrovať to možno na príklade marketingovej analýzy trhu a následnej cielenej reklame voči koncovým užívateľom alebo zmenou celkovej marketingovej stratégie spoločnosti za účelom zvyšovania zisku.

Rozhodovacie procesy na základe dátovej analytiky však už nie sú doménou iba súkromných spoločnosti, ale čoraz častejšie nachádzajú svoje uplatnenie aj vo verejnej správe. Mnohé orgány verejnej moci zriaďujú analytické centrá alebo odbory, ktoré dohliadajú na vydávanie efektívnych rozhodnutí na celoštátnej úrovni. Jednou z prirodzených vyústení zavádzania dátovej analýzy do verejnoprávneho priestoru je aj využitie prediktívnej analýzy údajov na policajnom úseku za účelom prevencie kriminality. Táto metóda sa už etablovala vo viacerých štátoch sveta a skutočne priniesla úžitok v dôsledku zníženia kriminality. Samozrejme, spoločnosť je ešte ďaleko k predpovedaniu budúceho správania, ale technológie, ktoré sú schopné spracovať a analyzovať obrovské množstvo údajov, nám môžu výrazne pomôcť. To však nepochybne nesie so sebou aj určité riziká pre práva a slobody jednotlivcov. Práve na tento aspekt chceme v rámci tejto štúdie upozorniť a načrtnúť základné východiska v kontexte základných ľudských práv a slobôd.

Ambíciou autora je v rámci predkladanej štúdie poskytnúť čitateľovi základný prehľad týkajúci sa vzťahu práva a policajného profilovania. Ako také je policajné profilovanie založené na tzv. prediktívnej analýze údajov. V prvej časti tejto štúdie je analyzovaná práve metóda prediktívnej analýzy údajov a jej rôzne modality. Zároveň je predmetom výskumu v tejto časti využitie prediktívnej analýzy údajov pri policajnom profilovaní vo vybraných štátoch sveta a porovnaním so Slovenskou republikou. V druhej časti je pozornosť zameraná na potenciálny konflikt využitia tejto metódy pri práci policajtov z hľadiska základných ľudských práv a slobôd konkrétne práva na súkromie, zákazu diskriminácie a práva na spravodlivé súdne konanie. Tretia časť štúdie je venovaná analýze legislatívy týkajúcej sa ochrany osobných údajov, ktorá sa aplikuje na činnosť policajných zložiek.

1. Teoretické východiská prediktívnej analýzy údajov

1.1. Úvodné poznámky

Prediktívna analýza údajov (ďalej aj ako „**PAÚ**“) je prostriedok, ktorý sa používa na predpovedanie momentálne neznámych situácií

v budúcnosti. Predmetný prostriedok používa množstvo techník ako štatistické algoritmy, data mining, štatistické modelovanie, strojové učenie a aspekty umelej inteligencie s cieľom analýzy dostupných údajov za účelom vytvorenia predikcie týkajúcej sa ďalšieho diania. Inými slovami, zmyslom je prekročiť rámec toho, čo sa stalo, aby sme poskytli najlepšie hodnotenie toho, čo sa stane.[2]

Táto metóda nie je doménou iba súkromného sektora, kde sa subjekty na trhu snažia presadiť cez svojich konkurentov a získať tak výhodnejšie postavenie. V súvislosti s obrovským množstvom údajov, ktoré sú voľne dostupné, či už v podobe informácií verejného sektora alebo tzv. otvorených údajov je PAÚ vhodnou a jednoduchou na použitie aj pre verejnú správu.

Z hľadiska výhod je potrebné spomenúť aspoň niektoré. V prvom rade je samozrejme vhodné poukázať na predchádzanie negatívnych následkov v rámci organizácií na základe predpovedí. Ako príklad možno uviesť fiktívnu situáciu, keď policajt svojou hliadkovou činnosťou na základe výsledku analytických dát zamedzil poškodzovaniu kultúrnej pamiatky a efektívne zneškodnil páchateľa deliktu. Druhou výhodou je možnosť optimalizácie výkonu činností resp. kompetencií na základe predikcií. Ilustrovať to možno na príklade, keď je na základe PAÚ včas determinované ohnisko chrípkovej epidémie a nemocnica tak môže zabezpečiť dostatok vakcín a lekárskych kapacít na zvládnutie očakávaného návalu pacientov. Prirodzene, esenciou je dostatočná efektivita a reflexia vzhľadom na predpovedané udalosti.

Vo všeobecnosti má prediktívna analýza údajov z technického hľadiska dve fázy, ktoré môžeme zjednodušene charakterizovať ako (i) objavenie a (ii) predpovedanie. V prvej fáze sa vo väčšine prípadov na základe použitia techniky dolovania dát (*data mining*) objavujú vzorce správania a korelácie, ktoré človek vzhľadom na svoje prirodzené limity manuálne nedokáže odhaliť. Následne na základe týchto (často prekvapivých) zistení je vytvorená predpoveď budúcich udalostí.[3]

Prístupy k skúmaniu, vyhodnocovaniu a predikcií údajov sa môžu líšiť z hľadiska špecifických modelov prediktívnej analýzy. Cieľom tejto state je stručne načrtnúť základnú charakteristiku troch modelov prediktívnej analýzy a to:

---

[2] ZHANG, A.: *Data Analytics: Practical Guide to Leveraging the Power of Algorithms, Data Science, Data Mining, Statistics, Big Data, and Predictive Analysis to Improve Business, Work, and Life*. Distribuované Amazon Digital Services LLC, 2017. (EPUB verzia).

[3] MCCUE, C.: *Data Mining and Predictive Analysis Intelligence Gathering and Crime Analysis*. Second Edition. Butterworth-Heinemann, 2015 s. 33 a nasl.

a) Prediktívny model (*Predicting model*);
b) Deskriptívny model *(Descriptive model*);
c) Rozhodovací model (*Decision modeling*).[4]

Ad a) Prediktívne modely skúmajú vzťahy medzi tým ako sa správa jednotlivec patriaci do určitej pozorovanej skupiny, ktorá má určité charakteristické črty a predpovedať, či podobný člen skupiny sa bude správať rovnako alebo odlišne od nastoleného vzorca.

V praxi sa tento model využíva predovšetkým na účely marketingu, kde algoritmus determinuje určité vzorce správania zákazníkov a následne určí ich preferencie na základe už určených vzorcov správania.[5] Svoje využitie ale môže nájsť aj po spáchaní priestupku resp. trestného činu pri predpovedi ohľadom možného páchateľa. V takomto prípade by sa jednalo o analýzu údajov z miesta spáchania deliktu a následne vytvorenie predikcie.

Ad b) Deskriptívny model spočíva v charakteristike udalostí a vzájomného vzťahu faktorov, ktoré ich ovplyvňujú. Typickým príkladom je zber údajov o zákazníkoch a následná cielená reklama. Rôzni zákazníci sú klasifikovaní do skupín na základe určitých vzorcov správania a najaktívnejším zákazníkom je následne zaslaná reklama, ktorá aplikuje aspekty vyhodnotené v rámci determinovaných vzorcov správania.

Ad c) Rozhodovací model sa v súčasnosti teší popularite predovšetkým v súkromnom sektore. Ako už z názvu vyplýva, predmetný model je založený na kombinácií množstva údajov a algoritmov s cieľom zefektívniť výkonnosť spoločnosti. Manažéri tak môžu na základe predikcií urobiť rozhodnutia, ktoré sa zo začiatku javia ako náročné s nepredvídateľnými dôsledkami. Ako príklad možno uviesť rozhodnutia týkajúce sa investovania do nových produktov vzhľadom na aktuálne trendy na trhu, reklamy v online priestore alebo analýza rizík v súvislosti s etablovaním schémy akcií na finančnom trhu.[6]

1.2. Prediktívna analýza údajov a policajné profilovanie

Ak berieme do úvahy teoretické základy načrtnuté v predchádzajúcej stati, je možné na základe týchto informácií vytvoriť ideálnu procedúru prediktívnej analýzy údajov pri výkone policajného profilovania.

V prvej fáze dochádza ku zozbieraniu potrebných údajov primárne z informačných systémov verejnej správy a ich spracúvaniu vrátane

[4] ZHANG, A.: *Data Analytics: Practical Guide to Leveraging the Power of Algorithms, Data Science, Data Mining, Statistics, Big Data, and Predictive Analysis to Improve Business, Work, and Life*. Distribuované Amazon Digital Services LLC, 2017. (EPUB verzia).

[5] Tamže.

[6] Tamže.

dátovej analýzy. V druhej fáze je vytvorená predikcia (predpoveď) na základe dátovej analýzy v predchádzajúcom kroku. Posledným štádiom procesu je samotný výkon činnosti príslušníka policajného zboru na základe vygenerovanej predpovede. Napríklad policajný zbor zozbiera údaje z informačných systémov verejnej správy a spojí ich s údajmi z verejne dostupnej komunikácie jednotlivcov zo sociálnych sietí (prvá fáza). Následne tieto údaje vloží do algoritmu, ktorý prostredníctvom svojej činnosti vytvorí predpoveď (druhá fáza). Nakoniec konkrétny príslušník policajného zboru túto predpoveď posúdi a rozhodne sa v rámci plánovanej hliadky zdržať sa na viditeľnom mieste v lokalite, v ktorej je predpoklad páchania protiprávnej činnosti (tretia fáza).

Ferguson rozlišuje tri úrovne použitia prediktívnej analýzy údajov v súvislosti s činnosťou policajných zložiek v Spojených štátoch.[7] Konkrétne ide o:

a) PAÚ so zameraním na miesta spáchania majetkovej kriminality;
b) PAÚ so zameraním na miesta spáchania násilnej kriminality;
c) PAÚ so zameraním na osoby zapojené do kriminálnych aktivít.

Ad a) Prvá úroveň podľa Fergusona zahrňovala použitie prediktívnej analýzy údajov s cieľom determinovania miesta, kde je možné očakávať tri predefinované typy kriminálnej aktivity – vlámania, krádeže automobilov a krádeže majetku z automobilov. Algoritmus používaný v tomto kontexte spracúval údaje týkajúce sa minulých kriminálnych aktivít. Špecificky išlo o čas, miesto a typ protiprávneho konania. Na základe výsledku PAÚ boli vytvorené mapy, ktoré príslušníci policajných zložiek používali ako základný dokument pri plánovaní hliadok.

Využitie diskutovanej metódy so zameraním na miesta spáchania majetkovej kriminality bolo podmienené myšlienkou, že majetkovú kriminalitu podmieňuje tzv. vlnový efekt (*ripple effect*). V praxi to znamenalo, že úspešné vlámanie motivuje ďalších potenciálnych páchateľov (resp. rovnakých ako v prvom prípade) na páchanie protiprávnej činnosti v tej istej oblasti.[8]

Ad b) S vývojom algoritmov na predpovedania majetkovej kriminality sa vyvíjali aj možnosti použitia tejto metódy na závažnejšie trestné činnosti ako krádeže, prestrelky a kriminalita organizovaných skupín. V tejto úrovni je opäť zdôrazňované miesto spáchania deliktu ako východiskový bod. V tomto kontexte bolo zaujímavé zistenie

[7] FERGUSON, A. Policing Predictive Policing *In Washington University Law Review, vol. 94, n. 5*, 2017.

[8] Tamže, s. 1130 a nasl.

súvislostí medzi drogovými trestnými činmi a použití strelných zbraní pri ďalších aktivitách páchateľov. Používanie PAÚ so zameraním na miesta spáchania násilnej kriminality viedlo k vytvoreniu aplikácie HunchLab, ktorá spracúvala údaje o štatistikách zločinnosti, opakovateľných vzorcov správania, sociálnych a ekonomických faktorov a zohľadňovala taktiež časové hľadisko, ročné obdobie a organizovanie kultúrnych podujatí. Predpovede boli založené na faktoroch ovplyvňujúcich riziko výskytu kriminality na určitých miestach.[9]

Ad c) Z právneho hľadiska azda najkomplikovanejšou metódou PAÚ na úseku policajných zložiek je použitie diskutovanej metódy so zameraním na osoby zapojené do kriminálnych aktivít. Predpovede na tejto úrovni sú založené na predpoklade, že sociálne prostredie ovplyvňuje konanie jednotlivcov a zároveň berie do úvahy aj deliktuálnu minulosť už sankcionovaných osôb. Samozrejme, zatknutia na základe predpovede sú ešte v rovine *science fiction*, ale zistenia na základe prediktívnej analýzy môžu byť použité v rámci prevencie kriminality. Namiesto rizikových miest sú identifikované rizikové osoby, ktoré sú následne kontaktované príslušníkmi policajného zboru s tým, že boli určené ako zdroje potenciálneho spoločenského nebezpečenstva (hlavne z hľadiska minulej trestnej činnosti). Títo jednotlivci boli informovaní ohľadom stíhania a zodpovednosti za spáchanie deliktov v budúcnosti a v rámci prevencie im boli odporúčané rôzne formy sociálnej pomoci. Je ale potrebné dodať, že predikcia týkajúca sa jednotlivca nie je dostatočným dôvodom na zatknutie alebo obmedzenie osobnej slobody.[10]

1.3. Policajné profilovanie vo svete a v Slovenskej republike

Na tomto mieste si dovoľujeme stručne načrtnúť požitie prediktívnej analýzy údajov vo vybraných štátoch. Pozornosť zameriame na Spojené štáty americké a použitie aplikácie PredPol v rámci Policajného zboru Los Angeles (LAPD), ktorá je považovaná za priekopnícku v danej oblasti. Vzhľadom na geografickú blízkosť podrobíme analýze Českú republiku a použitie diskutovanej metódy v meste Pardubice. Pozornosť zameriame taktiež na Rakúsko s dôrazom na systém CriPa. V poslednom rade analyzujeme podmienky v rámci Slovenskej republiky a potenciálnu aplikáciu PAÚ v činnosti Policajného zboru Slovenskej republiky.

[9] Tamže, s. 1138 a nasl.

[10] Viac v FERGUSON, A. Policing Predictive Policing *In Washington University Law Review, vol. 94, n. 5*, 2017, s. 1142 a nasl.

1.3.1. Spojené štáty americké (Los Angeles)

Spojené štáty americké patria z technologického hľadiska medzi najvyspelejšie štáty, čo sa týka zavádzania inovatívnych metód do verejného života. Inovácie neobišli ani policajné zložky, ktoré sa tradične potykajú s vysokou mierou kriminality.[11] Policajný zbor Los Angeles (LAPD) používa na predpovedanie kriminality aplikáciu PredPol.[12] PredPol funguje na báze umelej inteligencie (algoritmu), ktorý pomáha predpovedať kde a kedy sa určitý delikt stane. Aplikácia používa iba tri dátové zdroje a to konkrétne (i) typ deliktu, (ii) miesto spáchania deliktu a (iii) čas spáchania deliktu. Z toho vypláva, že v tomto prípade sa nejedná o spracúvanie osobných údajov.

Tento systém predpovedá vysoké riziko výskytu kriminality pre konkrétny časový úsek konkrétneho miesta. Vytváranie predpovedí je založené na algoritme, ktorý používa štatistické modely. Predpol sa zameriava na korelácie medzi miestami a historickými udalosťami - z kriminalistického hľadiska ide o súvislosti medzi spáchanými deliktami a miestami spáchania deliktu. Následne prostredníctvom matematických modelov predikuje na akom mieste a v akom čase môže byť protiprávna činnosť v budúcnosti páchaná. PredPol analyzuje aj faktory, ktoré súvisia s miestom spáchania deliktov (frekvencia, intervaly, prostredie).[13]

Zjednodušene, počítačový program je „nakŕmený" množstvom historických údajov, ktoré má policajný zbor k dispozícií. Následne je tento program každý deň doplnený o nové informácie na základe činnosti príslušníkov policajného zboru. Algoritmus vytvorí vizuálnu predpoveď vo forme štvorcovej siete rozloženej cez mapu vybranej oblasti. Podľa sfarbenia daného štvorca je možné zistiť pravdepodobnosť rizika protiprávnej činnosti konkrétneho typu v danej oblasti a v danom časovom rámci. Pre interpretáciu informácií daných predikciou sú dôležití analytici policajných oddelení, ktorí svojím názorom ovplyvňujú rozhodovanie o aplikácii a výkone činnosti policajných zložiek.[14]

Príslušníci LAPD nie sú povinní pri svojej práci používať PredPol. Je však nutné poznamenať, že (ne)využívanie prediktívnej analýzy údajov musia vo svojich správach odôvodniť. Systém v praxi zmenil aj hodnotenie jednotlivých členov zboru, keďže sa už neposudzuje

---

[11] https://www.fbi.gov/news/stories/2016-crime-statistics-released (dostupné 17.1.2018).

[12] http://www.predpol.com/ (dostupné 17.1.2018).

[13] HRUŠKA, L. a kol. : *Zborník príspevkov. 2. Odborný workshop : Mapy budoucnosti - moderní nástroj ke zvýšení efektivity a kvality výkonu veřejné správy v oblasti prevence kriminality založený na analýze a predikci kriminality*, http://www.prevencekriminality.cz/evt_file.php?file=838, s. 75 a nasl. (dostupné 15.12.2017).

[14] Tamže.

iba počet odhalených deliktov a zatknutých páchateľov, ale aj plnenie predpovedí generovaného systémom napr. v podobe výkonu hliadku na mieste so zvýšeným rizikom výskytu protiprávneho správania. To znamená, že odmenené je aj naplňovanie prevenčnej funkcie policajných zložiek. Používanie systému PredPol prinieslo očakávané zníženie kriminality – oddelenie LAPD Foothills Division zaznamenalo až 20 % pokles medzi rokmi 2013 a 2014. Nevýhodou využívania diskutovanej metódy je to, že prílišné spoľahnutie na automatizované rozhodnutie môže viesť k strate bdelosti príslušníkov policajných zložiek. To môže mať za následok apatiu k ďalšiemu zlepšovaniu svojho výkonu a závislosť na umelej inteligencií.[15]

1.3.2. Česká republika (Pardubice)

V spolupráci mestskej polície Pardubice a Policajného zboru Českej republiky sa od roku 2014 vytvára v Pardubiciach tzv. mapa kriminality. Prostredníctvom špeciálneho počítačového programu vkladajú príslušníci policajných zložiek do aplikácie údaje o spáchaných priestupkoch a trestných činoch. Systém tak obsahuje komplexné elektronické informácie týkajúce sa udalostí zdokumentovaných mestskou políciou. Mapy kriminality slúžia na zefektívnenie práce polície s ohľadom na stratégiu boja s kriminalitou, plánovanie hliadok a služieb.[16]

Čo sa týka samotnej funkcie predikcie kriminality, tak aplikácia používaná v Pardubiciach umožňuje vytváranie hot spotov (predpovedí miest, kde je možné spáchanie deliktu očakávať). Vzhľadom na vyššie uvedený opis spracúvaných údajov možno konštatovať, že predpovede sú z veľkej miery založené na štatistickom hodnotení historických údajov o kriminalite. Vzhľadom na nedostatok kvalitných historických dát je však využívanie predikcie kriminality značne komplikované.[17] Na mieste je však očakávanie, že s pribúdajúcim časom sa kvalita a kvantita spracúvaných údajov zlepší a prediktívna analýza údajov bude mať svoje pevné miesto pri výkone služby príslušníkov policajných zložiek v Pardubiciach.

1.3.3. Rakúsko (CriPa)

V Rakúskej spolkovej republike bol v ostatnom čase iniciovaný projekt CriPa. Ten si kladie viaceré ciele. V prvom rade sa jedná o predpovede z dlhodobého hľadiska, ktoré sa zameriavajú na budúce trendy krimi-

[15] Tamže, s. 186 – 187.
[16] Tamže, s. 128 a nasl.
[17] Tamže.

nality. Predmetné predikcie by mali byť spracovávané na základe údajov týkajúcich sa demografických zmien krajiny a štruktúry (ne)zamestnanosti a ich dopad na páchanie deliktuálnej činnosti. Získané údaje majú byť použité na vytvorenie geografického informačného systému, ktorý má slúžiť na zefektívnenie práce policajných zložiek v tom zmysle, že včas identifikuje potenciálne riziká z hľadiska miesta a času.[18]

CriPa funguje v dvoch rovinách. Primárne sa zameriava na už vyššie spomínané predikcie dlhodobých trendov v páchaní kriminality za účelom použitia týchto dát na efektívne nastavenie strategických cieľov prevencie kriminality. Sekundárne je však možné použiť získané výsledky na vyhodnotenie krátkodobých rizík v kontexte páchania kriminality vo vymedzenom priestore. Zo štúdie zameranou na analýzu v rámci projektu CriPa vyplýva, že pomocou PAÚ bolo napr. možné predchádzať 30 % vlámaní v oblastiach s vysokým rizikom kriminality a v oblasti s nízkym počtom vlámaní bolo možné kriminalitu znížiť o približne 5 %.[19]

1.3.4. Slovenská republika

V Slovenskej republike v súčasnosti prebieha implementácia projektu Elektronických služieb informačných systémov Ministerstva vnútra na úseku Policajného zboru.[20] Predmetný projekt prebieha v dvoch fázach. Prvá fáza, ktorá sa realizovala od októbra 2013 do decembra 2015 si kládla za cieľ podporiť činnosť Ministerstva vnútra Slovenskej republiky modernými informačnými a komunikačnými technológiami za účelom zlepšenia prijímania a riešenia podnetov od občanov v rámci činnosti polície a tým zefektívniť jej výkon. Cieľmi projektu bolo umožniť občanom asistovane nahlásiť životnú situáciu a komunikovať s jednotlivými zložkami Ministerstva vnútra dostupnými komunikačnými prostriedkami cez centrálny prístupový bod, implementovať informačný systém pre koordináciu, manažment a zefektívňovanie výkonu zložiek; poskytovať štatistické informácie na úseku dopravy. Z hľadiska témy predkladanej štúdie považujeme za vhodné osobitne zvýrazniť vybudovanie rezortného geografického informačného systému (GIS) pre špecifické účely MVSR a sprístupniť informácie z GIS prostredníctvom mobilných zariadení výkonným a iným zložkám rezortu.

---

[18] https://www.joanneum.at/en/policies/reference-projects/cripa-crime-predictive-analytics/ (dostupné 21.1.2017).

[19] HRUŠKA, L. a kol.: *Zborník príspevkov. 2. Odborný workshop : Mapy budoucnosti - moderní nástroj ke zvýšení efektivity a kvality výkonu veřejné správy v oblasti prevence kriminality založený na analýze a predikci kriminality*, http://www.prevencekriminality.cz/evt_file.php?file=838, s. 239 a nasl. (dostupné 15.12.2017).

[20] https://www.minv.sk/?ESISPZ_MV (dostupné 17.1.2017).

V druhej fáze, ktorej plánovaný interval je od júla 2014 do februára 2017 projekt implementácie elektronických služieb Ministerstva vnútra na úseku policajného zboru mal za úlohu vytvoriť predpoklady pre začlenenie operačných stredísk Policajného zboru do poskytovania elektronických služieb občanom a zlepšiť dostupnosť informácií zo sektora Ministerstva vnútra a štatistických informácií o činnosti polície pre širokú verejnosť. Z hľadiska predpokladaných výsledkov a dopadov implementácie predmetného projektu je vhodné upozorniť, že *„z interného hľadiska výstupy projektu budú môcť využívať relevantné zložky MVSR pri riešení nahlásených udalostí, koordinácii hliadok v teréne alebo pri dopravných činnostiach.“*[21]

Na základe uvedených skutočností je možné konštatovať, že Slovenská republika a Policajný zbor disponujú zdrojmi dát, ktoré by mohli tvoriť relevantný základ v procese využitia prediktívnej analýzy údajov. Tomuto záveru nasvedčuje aj pravidelné zverejňovanie tzv. máp kriminality,[22] ktoré majú primárne štatistickú hodnotu z hľadiska páchanej kriminality v Slovenskej republike. Z verejnej dostupných informácií však nevyplýva, že Slovenská republika a jej policajné zložky využívajú metódu policajného profilovania tak, ako je charakterizovaná v úvodných častiach predkladanej štúdie.

2. Policajné profilovanie a základné ľudské práva a slobody

V druhej časti predkladanej štúdie považujeme za nevyhnutné podrobiť analýze právnu úpravu, ktorá sa (potenciálne) týka použitia prediktívnej analýzy údajov na úseku policajných zložiek. Z hľadiska metodiky je vhodné v prvom rade determinovať základné ľudské práva a slobody, ktoré sú v rámci využitia diskutovanej metódy v ohrození a následne pozornosť zamerať na osobitnú právnu úpravu. Na účely predkladanej štúdie vyberáme právo na súkromie, zákaz diskriminácie a právo na spravodlivý.

2.1. Základné právne východiská a aplikačné problémy

Prediktívna analýza údajov a jej využitie v zložkách policajných zborov je diskutovanou témou medzi akademikmi a aj praktikmi.

[21] Tamže.

[22] https://www.minv.sk/?Mapy_trestnych_cinov_v_Slovenskej_republike_za_rok_2016 (dostupné 17.1.2018).

Debaty však naberajú väčšiu hodnotu v prípadoch, keď skutočne dôjde k implementovaniu predmetnej metódy do praxe ako sa to stalo napr. v Spojených štátoch amerických prostredníctvom programu PredPol. Napriek tomu, že analytici vidia v diskutovanej metóde obrovský prínos pre zníženie kriminality, tak ako každá technológia zavádzaná do praxe, prináša so sebou určité riziká. Niektoré z nich spôsobujú problémy aj pri ich právnej regulácií. Identifikovať možno nasledovné štyri problémy resp. riziká:[23]

1. Zvýšenie rasového profilovania

Diskriminácia bola v minulosti prirodzenou súčasťou spoločnosti a tak aj dáta, ktoré by boli vložené do algoritmu a ich následne vyhodnotenie na základe nich by potenciálne mohlo byť diskriminačné. Algoritmus totiž nevie „rozoznať," či predchádzajúce rozhodnutia alebo konania boli urobené s predsudkami alebo nie. Následné spoliehanie sa na predpovede na základe takýchto údajov by mohlo viesť k zvýšenému profilovaniu a neoprávnenému sledovaniu minorít či príslušníkov niektorých rás. Ako ukazujú štatistiky,[24] takáto obava nie je len fikciou.

2. Ohrozenie súkromia

Tento problém nastáva iba v prípade, ak sú spracúvané osobné údaje, teda dáta na základe ktorých je možné identifikovať fyzickú osobu. Je zdokumentovaný prípad z mesta Chicago,[25] kde na základe prediktívnej analýzy bola označená určitá osoba ako riziková a následne kontaktovaná príslušníkmi policajného zboru s tým, že je potenciálne nebezpečná a pod dohľadom. Otázka ochrany súkromia a osobných údajov je tak skutočne namieste.

3. Výrazné spoliehanie sa na technológie

Spoločnosť má tendenciu si myslieť, že technológie vyriešia „staré problémy." Málokedy je však tomu tak, keďže technológia by mala byť len nástrojom a nie samotným riešením. Algoritmus, ktorý urobí predpoveď je síce iba počítačovým programom, ale predikciu do praxe pretavujú jednotlivci (policajný zbor). Posledné výskumy ukazujú, že

[23] https://www.floridatechonline.com/blog/criminal-justice/4-problems-with-predictive-policing/ (dostupné 9.6. 2018).

[24] Pozri viac http://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/be-cautious-about-data-driven-policing (dostupné 9.6.2018).

[25] http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist (dostupné 9.6.2018).

zameranie sa na správnosť informácií namiesto ich reálnej využiteľnosti môže spôsobovať problémy.[26]

4. Nepochopenie súvislostí (kontextu)

Ľudský faktor je absolútne nevyhnutný na úspešné pretavenie prediktívnej analýzy do praxe. Kritické myslenie pri hľadaní súvislostí medzi výsledkami a predpoveďami je tak esenciálnou súčasťou diskutovanej metódy napr. informácia, že trestné činy sú nahlasované medzi siedmou a ôsmou hodinou ráno môže viesť k dvom záverom – (i) trestné činy sú páchané v tomto časovom rámci alebo (ii) ľudia v tomto čase zistili, že bol nejaký trestný čin spáchaný. Z tohto dôvodu je dôležité nazerať na výsledky prediktívnej analýzy v širšom kontexte a nekonať na základe urýchlených záverov.

2.2. Právo na súkromie v kontexte prediktívnej analýzy údajov

Dohovor o ochrane ľudských právach a základných slobôd (ďalej len „**Dohovor**“) upravuje právo na rešpektovanie súkromného a rodinného života v článku 8. Prvý odsek ustanovuje, že *„každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.“* Druhý odsek vytvára derogáciu predchádzajúceho ustanovenia a poskytuje priestor pre výnimku z dodržiavania práva na rešpektovanie súkromného a rodinného života – *„Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.“*

Z historického hľadiska je článok 8 vykladaný tak, že zahŕňa aj ochranu ukladania, zverejňovania a vo všeobecnosti spracúvania údajov, ktoré sa týkajú súkromného života jednotlivcov.[27] V tomto kontexte je potrebné zvýrazniť, že Charta základných práv Európskej únie (ďalej len „**Charta**“) diferencuje medzi právom na rešpektovanie súkromného a rodinného života a právom na ochranu osobných údajov.[28]

---

[26] Pozri viac PERRY, W. - MCINNIS, B. - PRICE, C. - SMITH, S. - HOLLYWOOD, J.: Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations, https://www.rand.org/pubs/research_reports/RR233.html (dostupné 6.9.2018).

[27] Napr. Rozsudok ESĽP vo veci Leander v Švédsko zo dňa 26. marca 1987, rozsudok ESĽP vo veci Rotaru v Rumunsko č. 28341/95 resp. rozsudok vo veci Amann v Švajčiarsko č. 27798/98.

[28] Článok 7 Charty: *„Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie.“*

Na doplnenie je ešte potrebné zvýrazniť, že základné práva a slobody upravené v Charte rozsahovo a obsahovo korešpondujú s právnou úpravou v Dohovore, avšak zákonodarca v rámci Európskej únie môže priznať širší rozsah ochrany základných práv a slobôd.[29] Dopĺňame, že právo na súkromie (ochranu osobných údajov) je upravené aj v Ústave Slovenskej republiky[30] a to vo viacerých rovinách. Článok 16 ods. 1 ustanovuje, že *„nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom.“* Na ústavnoprávnu ochranu súkromia nadväzuje článok 19. Druhý odsek diskutovaného článku zakotvuje právo každého pred neoprávneným zasahovaním do súkromného a rodinného života. Tretí odsek výslovne upravuje právo na ochranu osobných údajov.[31]

Drgonec uvádza, že nevyhnutným predpokladom na interpretáciu práva na súkromie je diferenciácia medzi samotným právom a súkromím ako sociologickou kategóriou.[32] Súkromie možno vymedziť ako *„ríšu, v ktorej je človek sám pánom, je to územie absolútnej suverenity, oblasť v ktorej má plnú a neoddeliteľnú moc rozhodovať „kým a čím je,“ a odtiaľ sa môže vydávať von so zámerom, aby boli vnímané jeho vlastné rozhodnutia.“*[33] Ústavný súd Slovenskej republiky definoval rozdiel medzi súkromím a právom na súkromie nasledovne: *„Súkromím sa chápe predovšetkým sféra života človeka, do ktorej nemožno zasahovať bez jeho súhlasu. Právom na súkromie sa zaručuje osobe možnosť rozhodovať samostatne o tých záležitostiach, ktoré sa uznávajú za súkromné.“*[34]

Keďže právo na rešpektovanie súkromného a rodinného života tak, ako je vymedzené a interpretované v rámci Dohovoru, poskytuje relatívne veľký priestor na extenzívne uplatňovanie, jeho precízna aplikácia je neoddeliteľnou súčasťou aj pri výkone určitých špecifických činností. Jednou z nich je aj výkon činnosti policajných zložiek v štáte.

V kontexte vyššie uvedených činností dochádza k zberu a spracúvaniu osobných údajov osôb, ktoré sú či už podozrivé zo spácha-

---

Článok 8: *„1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. 2. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu. 3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.“*

[29] Článok 53 (3) Charty základných práv EÚ.

[30] 460/1992 Zb. Ústava Slovenskej republiky.

[31] Čl. 19 ods. 3 Ústavy Slovenskej republiky: *„Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.“*

[32] DRGONEC, J.: Ústava Slovenskej republiky. Veľký komentár. Praha: C.H.Beck, 2015, s. 423.

[33] BAUMAN, Z. – LYON, D.: *Tekutý dohled*. Praha : Broken books, 2013, s. 37.

[34] PL. ÚS 10/2014-78. Nález z 29. apríla 2015, s. 36.

nia trestného činu resp. priestupku alebo boli riadne odsúdené. Prirodzene, právna ochrana súkromia resp. ochrany osobných údajov je v súvislosti s týmito činnosťami oslabená v dôsledku verejného záujmu na riadnom vyšetrení protiprávnych aktov, sankcionovaní zodpovedných osôb a ochrane jednotlivcov pred nimi. Avšak je nevyhnutné poznamenať, že napriek predchádzajúcej konštatácií zásah do diskutovaných práv a slobôd musí byť v súlade s právom, nevyhnutný v demokratickej spoločnosti a musí smerovať k dosiahnutiu legitímneho cieľa.

Judikatúra Európskeho súdu pre ľudské práva je pomerne bohatá na interpretáciu vyvažovania práva na súkromie v súvislosti s výkonom policajných zložiek. V prejednávaných prípadoch išlo predovšetkým o sledovanie osôb podozrivých zo spáchania trestnej činnosti, ale aj o použitie a retenčné doby uchovávania biometrických a genetických údajov nielen u týchto osôb. Vzhľadom na zameranie príspevku považujeme za vhodné aspoň stručne načrtnúť rozhodovaciu prax ESĽP v predmetných veciach s cieľom lepšie pochopiť a analyzovať výkon spomínaných činností v praktickom živote.

Jedným z ťažiskových rozhodnutí v predmetnej oblasti je rozsudok ESĽP vo veci **S. a Marper proti Spojenému kráľovstvu**.[35] Toto rozhodnutie je prvé, ktoré skúmalo využitie tzv. Veľkých dát (*Big data*) v súvislosti s prácou policajných zložiek. Skutkovo prípad spočíval v tom, že sťažovatelia, ktorí boli obvinení zo spáchania trestných činov (nie odsúdení) namietali uchovávanie ich odtlačkov prstov, DNA a vzoriek buniek pre ďalšie potreby policajných zložiek, ktoré im príslušníci policajného zboru odobrali. Problematickým bolo ustanovenie britského právneho poriadku, ktoré povoľovalo prakticky bez obmedzenia uchovávať biometrické a genetické údaje osôb podozrivých zo spáchania trestnej činnosti. Uchovávanie údajov pretrvávalo aj vtedy, ak bola osoba zbavená v rámci trestného konania alebo prepustená z výkonu trestu resp. zadržania. Sťažovatelia sa domáhali výmazu diskutovaných údajov z policajných databáz, ale ich žiadosť bola policajnými zložkami zamietnutá. Navyše, britské právo neobsahovalo žiadne faktory, ktoré by ovplyvňovali dĺžku uchovávania údajov ako závažnosť spáchanej činnosti, vek podozrivých či predchádzajúce trestná činnosť. Legislatíva neposkytovala ani nezávislé preskúmanie žiadosti o vymazanie údajov v prípade zamietnutia takýchto sťažností. Európsky súd pre ľudské práva vo svojom rozhodnutí konštatoval, že takéto neobmedzené uchovávanie citlivých osobných údajov bez akéhokoľvek rozlišovania a s obmedzenými právami

[35] ESĽP, S. a Marper/Spojené kráľovstvo, č. 30562/04 a 30566/04, 4. decembra 2008.

dotknutých osôb ovplyvnenia vymazania týchto údajov je v rozpore s ustanovením článku 8 Dohovoru. Sťažovateľom vyhovel a rozhodol, že došlo k porušenie práva na rešpektovanie súkromného a rodinného života zo strany štátu.

Obdobnému skutkovému stavu čelil Európsky súd pre ľudské práva vo veci **B.B. proti Francúzsku**.[36] V ňom bol sťažovateľ zahrnutý do vnútroštátnej súdnej databázy v súvislosti s odsúdením za sexuálny trestný čin. Sťažovateľ namietal porušenie práva na rešpektovanie súkromného a rodinného života. Štát ale na rozdiel od vyššie diskutovaného prípadu prijal primerané bezpečnostné a organizačné opatrenia týkajúce sa uchovávania údajov. Konkrétne sa jednalo o zavedenie práva na vymazanie, ktorým disponovala dotknutá osoba, lehota uchovávania údajov bola obmedzená a taktiež existovali limity prístupu k osobným údajom. Francúzsko tak primerane vyvážilo verejný záujem a záujem na ochrane súkromia (osobných údajov). V tomto prípade ESĽP konštatoval, že nedošlo k porušeniu práva na rešpektovanie súkromného a rodinného života.

Ďalším z radu relevantných prípadov je **Vetter proti Francúzsku**.[37] Skutkovo spočíval prípad v tom, že do domácnosti priateľa sťažovateľa bolo so súhlasom sudcu nainštalované odpočúvacie zariadenie, na základe výpovede svedka, ktorý tvrdil, že sťažovateľ spáchal trestný čin vraždy. Vzhľadom na to, že sťažovateľ odpočúvanú domácnosť svojho priateľa navštevoval frekventovane, policajné zložky na základe ich rozhovorov sťažovateľa zatkli a obvinili zo spáchania tohto trestného činu. Následne v trestnom konaní sťažovateľ namietal neprípustnosť nahrávok ako dôkazu v trestnom konaní. Európsky súd pre ľudské práva posudzoval zásah do súkromia sťažovateľa v kontexte požiadavky na súladu s právom na predmetný zásah zo strany štátu. Francúzsky trestný procesný kódex neustanovoval podrobnosti úvahy orgánov pri nariaďovaní odpočúvania súkromných rozhovorov. ESĽP konštatoval, že sťažovateľ nedisponoval vyžadovaným minimálnym stupňom ochrany pri zásahu do práva na súkromie. Vzhľadom na vyššie uvedené súd konštatoval porušenie práva na rešpektovanie súkromného a rodinného života.

2.2.1. Policajná smernica a jej implementácia

Ako už bolo v predchádzajúcej stati poukázané, z hľadiska práva Rady Európy je právo na rešpektovanie súkromného a rodinného živo-

[36] ESĽP, B.B./Francúzsko, č. 5335/06, 17. decembra 2009.
[37] ESĽP, Vetter/Francúzsko, č.59842/00, 31. mája 2005.

ta interpretované príslušným súdnym orgánom tak, že imanentne zahŕňa aj právo na ochranu osobných údajov. V práve Európskej únie je v Charte diferencované právo na rešpektovanie súkromného a rodinného života (článok 7) a právo na ochranu osobných údajov (článok 8). Zákonodarca sa v rámci Európskej únie rozhodol regulovať právo na ochranu osobných údajov v rámci svojej výlučnej pôsobnosti a diskutovaná problematika zažíva v súčasnosti svoju druhú renesanciu.

Reformný balík na úrovni Európskej únie obsahuje dva právne akty, ktoré nahrádzajú doteraz platný právny rámec. Konkrétne bolo prijaté nariadenie Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „**GDPR**“)[38] a smernica Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov (ďalej len „**Policajná smernica**“).[39]

Berúc do úvahy charakter a zameranie štúdie, v ďalšom texte považujeme za nevyhnutné aspoň rámcovo posúdiť spracúvania osobných údajov na základe Policajnej smernice. Detailnejšiu analýzu relevantných inštitútov v kontexte prediktívnej analýzy údajov si dovoľujeme spracovať v tretej časti predkladanej štúdie.

Policajná smernica nahrádza rámcové rozhodnutie Rady 2008/977/SVV (rámcové rozhodnutie),[40] ktoré upravovalo spracúvanie osobných údajov v rámci polície a justície. Pôsobnosť smernice je vymedzená v článku 1 (1) na prípady spracúvania osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu. Základnými cieľmi je (i) ochrana základných práv a slobôd fyzických osôb, najmä ich právo na ochranu osobných údajov a (ii) zabezpečenie, aby výmena osobných údajov medzi príslušnými orgánmi v rámci Únie, ak sa takáto výmena vyžaduje podľa práva Únie alebo práva členského štátu, nebola obmedzená ani zakázaná z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov.[41] V kontexte pôsobnosti došlo k zásadnému posunu opro-

[38] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679.

[39] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680.

[40] Rada Európskej únie (2008), rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce (rámcové rozhodnutie o ochrane údajov), Ú. v. EÚ L 350, 2008.

[41] Článok 1 (2) Policajnej smernice.

ti rámcovému rozhodnutiu, keďže to sa vzťahovalo len na medzištátnu spoluprácu v policajných a justičných veciach. Oproti tomu Policajná smernica upravuje vzťahy aj v rámci jednotlivých štátov na úrovni policajných zložiek a súdov.

Z hľadiska stručného náčrtu najvýznamnejších zmien vyberáme nasledovné ustanovenia a inštitúty:

- Rozlišovanie medzi rôznymi kategóriami dotknutých osôb (podozrivý, odsúdený, obeť a tretia osoba);
- Rozlišovanie medzi osobnými údajmi založenými na základe skutočnosti a založených na osobných hodnoteniach;
- Automatizované individuálne rozhodovanie;
- Posilnenie práv dotknutých osôb;
- Špecificky navrhnutá a štandardná ochrana údajov;
- Záznamy o spracovateľských činnostiach a logovanie;
- Posúdenie vplyvu na ochranu údajov;
- Bezpečnostné opatrenia (oznámenie porušenia ochrany osobných údajov);
- Poverenie zodpovednej osoby.

Domnievame sa, že mnohé z vyššie uvedených inštitútov reagujú aj na rozvoj nových technológií a ich potenciálu v rámci výkonu činnosti policajných zložiek. Nasvedčuje tomu aj ustanovenie recitálu 3 Policajnej smernice, ktorý zdôrazňuje, že *„rýchly technologický rozvoj a globalizácia so sebou priniesli nové výzvy v oblasti ochrany osobných údajov. Rozsah získavania a zdieľania osobných údajov sa výrazne zväčšil. Technológia umožňuje pri výkone činností, ako napríklad predchádzaní trestným činom, ich vyšetrovaní, odhaľovaní alebo stíhaní alebo pri výkone trestných sankcií, spracúvať osobné údaje v bezprecedentnom rozsahu.“*

Implementáciu predmetnej smernice v právnom poriadku Slovenskej republiky obsahuje tretia hlava nového zákona o ochrane osobných údajov[42] s názvom „Osobitné pravidlá ochrany osobných údajov fyzických osôb pri ich spracúvaní príslušnými orgánmi. Je možné konštatovať, že slovenská právna do značnej miery preberá jazykovo totožné znenie ustanovení z Policajnej smernice.

2.3. Zákaz diskriminácie a prediktívna analýza údajov

Európsky dohovor o ľudských právach upravuje zákaz diskriminácie v článku 14. Podľa predmetného ustanovenia *„užívanie práv a slobôd priznaných týmto dohovorom musí byť zabezpečené bez diskrimi-*

[42] Zákon č. 18/2018 Z. z. o ochrane osobných údajov.

nácie založenej na akomkoľvek dôvode, ako je pohlavie, rasa, farba pleti, jazyk, náboženstvo, politické alebo iné zmýšľanie, národnostný alebo sociálny pôvod, príslušnosť k národnostnej menšine, majetok, rod alebo iné postavenie." Predmetné ustanovenie reflektuje dodatkový Protokol č. 12, ktorý bol prijatý v Ríme v roku 2000.

Podobnú právnu úpravu obsahuje aj Charta základných práv EÚ v rámci článku 21, ktorý ustanovuje všeobecný zákaz *„akejkoľvek diskriminácie najmä z dôvodu pohlavia, rasy, farby pleti, etnického alebo sociálneho pôvodu, genetických vlastností, jazyka, náboženstva alebo viery, politického alebo iného zmýšľania, príslušnosti k národnostnej menšine, majetku, narodenia, zdravotného postihnutia, veku alebo sexuálnej orientácie."* Navyše, Charta explicitne zakazuje diskrimináciu na základe štátnej príslušnosti.[43]

Z hľadiska interpretácie ustanovení Dohovoru je nutné upozorniť na to, že zákaz diskriminácie predstavuje podpornú právnu úpravu pre zákaz zasahovania do ostatných práv a slobôd vymedzených v Dohovore. Nasvedčuje tomu dikcia ustanovenia *„užívanie práv a slobôd priznaných"* Dohovorom. V praxi to znamená, že diskriminácia v zásade vždy súvisí s porušovaním iného práva alebo slobody. Je však potrebné dodať, že na efektívne uplatnenie zákazu diskriminácie nie je obligatórne preukázať porušenie iného práva alebo slobody chráneného Dohovorom.[44] Európsky súd pre ľudské práva túto skutočnosť zvýraznil vo svojom rozhodnutí vo veci **National Union of Belgian Police proti Belgicku**,[45] v ktorom prejudikoval, že zákaz diskriminácie je integrálnou súčasťou každého z práv a slobôd zaručených Dohovorom.

Diskriminácia znamená zaobchádzanie s osobami v obdobných (analogických) situáciách iným (odlišným) spôsobom bez objektívneho a primeraného odôvodnenia.[46] Vzhľadom na použitie slovného spojenia „obdobné (analogické) situácie," nie každé odlišné zaobchádzanie konštituuje diskriminačné správanie. Dôležitým faktorom pre posúdenie skutkových okolností je, či existujú alternatívne cesty na dosiahnutie rovnakého cieľa.[47]

Okrem úmyselnej resp. priamej diskriminácie právna úprava pozná aj inštitút tzv. nepriamej diskriminácie. Legálnu definíciu nepriamej diskriminácie explicitne zakotvuje článok 2 smernice Rady 2000/43/ES kto-

[43] Článok 21 (2) Charty základných práv EÚ.

[44] SCHABAS, W.: *The European Convention on Human Rights. A commentary*. 1st edition. Oxford University Press, 2015, s. 562.

[45] National Union of Belgian Police v. Belgium, 27 October 1975, § 44, Series A no. 19.

[46] Napr. Rozsudky ESĽP D.H. a ostatní proti Českej republike[VK], č. 57325/00 alebo Willis proti Spojenému kráľovstvu, č. 36042/97.

[47] Glor proti Švajčiarsku, no. 13444/04.

rou sa zavádza zásada rovnakého zaobchádzania s osobami bez ohľadu na rasový alebo etnický pôvod v rámci sekundárneho práva Európskej únie: *„Za nepriamu diskrimináciu sa považuje prípad, ak by v dôsledku navonok neutrálneho predpisu, kritéria alebo zvyklosti bola znevýhodnená osoba určitej rasy alebo etnického pôvodu v porovnaní s inými osobami, iba ak uvedený predpis, kritérium alebo zvyklosť je objektívne odôvodnený legitímnym cieľom a prostriedky na jeho dosiahnutie sú primerané a nevyhnutné.“* Naopak, priama diskriminácia nastáva v prípade, ak *„sa s jednou osobou z dôvodu rasy alebo etnického pôvodu zaobchádza, zaobchádzalo, alebo by sa zaobchádzalo v porovnateľnej situácii menej priaznivo ako s inou osobou.“*[48] Samozrejme, je potrebné brať do úvahy, že akákoľvek forma diskriminácie nemusí byť doménou len právnej úpravy, ale môže vyplynúť aj zo skutkových okolností konkrétnych situácií.

V súvislosti s výkonom činnosti policajných zložiek v štáte považujeme za vhodné upozorniť na transfer dôkazného bremena v rámci sporových strán pri dokazovaní diskriminačného správania. V zásade platí *affirmanti incumbit probatio* – ten, kto z niečoho obviňuje, musí obvinenie dokázať. Avšak pri dokazovaní diskriminácie je v mnohých prípadoch dôkazné bremeno presunuté na orgány štátnej moci. V prípade použitia prediktívnej analýzy údajov, kde by hypoteticky bez zjavného odôvodnenia algoritmus smeroval svoje predpovede voči špecifickej etnickej skupine, tak dôkazné bremeno by najprv spočívalo na sťažovateľoch a v prípade preukázanie rozdielnosti správania orgánov štátnej moci by následne tieto orgány boli vyzvané na preukázanie odôvodnenia svojich zásahov.

Právna úprava v Dohovore upravuje demonštratívny výpočet dôvodov (základov) diskriminačného správania, čo potvrdzuje aj dôvodová správa k Dohovoru.[49]

Diskriminácia môže byť založená napríklad na:

- pohlaví;
- rase;
- farbe pleti;
- jazyku;
- náboženstve;
- politickom alebo inom zmýšľaní;
- národnostnom alebo sociálnom pôvode;

[48] Článok 2 (1) smernice Rady 2000/43/ES.

[49] Explanatory Report to the Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms.

– príslušnosti k národnostnej menšine;
– majetku, rode alebo inom postavení.

Na prvý pohľad by sa mohlo zdať, že rozbor právnej úpravy diskriminácie pri prediktívnej analýze údajov využívanej v rámci práce policajných zložiek nemá svoje opodstatnenie. Opak je však pravdou a prvky diskriminácie sa môžu vyskytnúť už pri programovaní resp. nastavení algoritmu, ktorý by cielene perzekvoval určité skupiny obyvateľstva. Na diskutovaný problém upozorňujú aj viacerí autori.[50]

2.4. Právo na spravodlivé súdne konanie

V prípade, ak by boli vyvodzované dôsledky z konania páchateľa na základe výstupov z prediktívnej analýzy údajov, považujeme za dôležité charakterizovať aj právnu úpravu práva na spravodlivé súdne konanie. Dohovor upravuje diskutované právo v článku 6. Prvý odsek článku 6 Dohovoru ustanovuje právo každého *„na to, aby jeho vec bola spravodlivo, verejne a v primeranej lehote prejednaná nezávislým a nestranným súdom zriadeným zákonom, ktorý rozhodne o jeho občianskych právach alebo záväzkoch alebo o akomkoľvek trestnom čine, z ktorého je obvinený. Rozsudok musí byť vyhlásený verejne, ale tlač a verejnosť môžu byť vylúčené buď po dobu celého alebo časti procesu v záujme mravnosti, verejného poriadku alebo národnej bezpečnosti v demokratickej spoločnosti, keď to vyžadujú záujmy maloletých alebo ochrana súkromného života účastníkov alebo, v rozsahu považovanom súdom za úplne nevyhnutný, pokiaľ by vzhľadom na osobitné okolnosti mohla byť verejnosť konania na ujmu záujmom spravodlivosti.“* Z hľadiska predmetu predkladanej štúdie je ale dôležitejší odsek 2, ktorý ustanovuje zásadu prezumpcie neviny. Na obvineného sa hľadí ako na nevinného, kým mu nie je zákonným spôsobom preukázaný opak.[51] Tretí odsek článku 6 upravuje základné práva obvineného, predovšetkým v kontexte procesnoprávnych práv.[52]

---

[50] MADDEN, M. - GILMAN, M. - LEVY, K. - MARWICK, A.: Privacy, poverty, and Big data: A matrix of vulnerabilities for poor americans *In 95 Washington University Law Review, Vol. 53* (2017).

[51] Článok 6 (2) Dohovoru.

[52] *„Každý, kto je obvinený z trestného činu, má tieto minimálne práva:*
a) byť bez meškania a v jazyku, ktorému rozumie, podrobne oboznámený s povahou a dôvodom obvinenia vzneseného proti nemu;
b) mať primeraný čas a možnosti na prípravu svojej obhajoby;
c) obhajovať sa osobne alebo prostredníctvom obhajcu podľa vlastného výberu, alebo pokiaľ nemá dostatok prostriedkov na zaplatenie obhajcu, aby sa mu poskytol bezplatne, ak to záujmy spravodlivosti vyžadujú;

Prvý odsek sa aplikuje na civilné, administratívne a trestné konanie. Naopak, druhý a tretí odsek má pôsobnosť predovšetkým na trestné konanie.[53] ESĽP opakovane potvrdil, že pri napádaní diskutovaného práva nie je úlohou tohto súdu posudzovať chyby aplikácie práva alebo vyhodnotenia skutkové stavu. ESĽP posudzuje hodnotenie národných súdov z pohľadu potenciálnej ľubovôle.[54]

Z hľadiska zamerania tohto príspevku je potrebné zvýrazniť, že právo na spravodlivé súdne konanie vymedzené v článku 6 sa vzťahuje aj na predbežné vyšetrovania spáchania deliktov v rámci priestupkového resp. trestného konania. Európsky súd pre ľudské práva túto skutočnosť zdôraznil z dôvodu, že ak sa obvinený dostane pred súd, je nevyhnutné, aby celé trestné konanie bolo v súlade s právom a za zachovania základných práv a slobôd.[55] Rovnako sa právo na spravodlivé súdne konanie vzťahuje aj na podozrivého v prípadoch, keď ešte nie je formálne obvinený zo spáchania trestného činu. Preferuje sa viac materiálny ako formalistický pohľad na interpretáciu predmetných ustanovení.[56]

Vzhľadom na to, že prediktívna analýza údajov má primárne preventívny účinok je dôležité upozorniť na to, že článok 6 Dohovoru sa nevzťahuje na preventívne opatrenia policajných zložiek, ktoré mieria voči predchádzaniu kriminality pred tým, než je vôbec spáchaná. Vyššie uvedené potvrdil vo svojom rozhodnutí **Raimond proti Taliansku**[57] ESĽP, v ktorom sa sťažovateľ domáhal porušenia práva na spravodlivé súdne konanie na vzhľadom na to, že sa stal predmetom špeciálneho dohľadu policajných zložiek. Tento dohľad bol založený na podozrení členstva sťažovateľa v organizovanej zločineckej skupine. ESĽP v tomto rozhodnutí konštatoval, že pôsobnosť článku 6 Dohovoru sa nevzťahuje na preventívne opatrenia policajných zložiek.

Pre doplnenie európskeho kontextu danej problematiky je potrebné dodať, že Charta základných práv EÚ upravuje právo na spravodlivé súdne konanie v niekoľkých ustanoveniach. Konkrétne ide o články 47 až 50. Článok 47 obsahuje všeobecnú klauzulu práva na účinný prostriedok náprav a na spravodlivý proces. Zásada prezumpcie neviny a právo na obhajobu sú zakotvené v článku 48. Článok 49 upravu-

d) vypočúvať alebo dať vypočúvať svedkov proti sebe a dosiahnuť predvolanie na vypočúvanie svedkov vo svoj prospech za rovnakých podmienok, ako v prípade svedkov proti nemu;

e) mať bezplatnú pomoc tlmočníka, ak nerozumie jazyku používanému pred súdom, alebo ak týmto jazykom nehovorí."

[53] SCHABAS, W. : *The European Convention on Human Rights. A commentary*. 1st edition. Oxford University Press, 2015, s. 271.

[54] Sisojeva a ostatní proti Lotyšsku, 60654/00 § 89.

[55] Rozsudok ESĽP vo veci Saman proti Turecku, č. 35292/05.

[56] Rozsudok ESĽP vo veci G.S.P. proti Rumunsku, č. 20899/03.

[57] Rozsudok ESĽP vo veci Raimondo proti Taliansku z 22. Februára 1994.

je zásadu zákonnosti a zásadu primeranosti trestných činov a trestov. Zásada *ne bis in idem* je ustanovená v článku 50.

3. Policajné profilovanie v kontexte Policajnej smernice

Pri množstve nových technológií, ktoré využívajú prostriedky umelej inteligencie (vrátane prediktívnej analýzy údajov v kontexte policajného profilovania) je zvýraznený vplyv na jednotlivca. V tejto stati považujeme za vhodné poukázať na právnu úpravu v Policajnej smernici práve v súvislosti so základnými právami a slobodami uvedenými v predchádzajúcej časti tohto príspevku. Vzhľadom na komplexnosť právnej úpravy a pre lepšiu čitateľnosť delíme analýzu jednotlivých ustanovení podľa fáz vymedzených vyššie. Z tohto hľadiska ide o:

1. Zber údajov (relevantné inštitúty pred vytvorením predikcie);
2. Vytvorenie predpovede;
3. Aplikácia predpovede (právo nebyť predmetom individuálneho automatizovaného rozhodovania).

3.1 Zber údajov (relevantné právne inštitúty pred vytvorením predikcie)

Spracúvanie osobných údajov vo všeobecnosti upravuje GDPR ako všeobecný právny predpis pre ochranu osobných údajov na úrovni Európskej únie. Ak však chceme analyzovať spracúvanie osobných údajov policajných zložiek, je potrebné nahliadnuť do tzv. Policajnej smernice.[58] Policajná smernica je *lex specialis* voči GDPR. To znamená, že ak právna úprava v Policajnej smernici niektorú otázku spracúvania osobných údajov nerieši, aplikuje sa GDPR. Keďže predkladaný príspevok sa zaoberá policajným profilovaním resp. prediktívnou analýzou údajov pri činnosti policajných zložiek, je nevyhnutné v pravom rade hľadať relevantné ustanovenia v Policajnej smernici. V statiach, kde sa to javilo vhodné, sme odkazovali aj na implementáciu v zákone č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „**Zákon o ochrane osobných údajov**“) a zákone č. 171/1993 Z. z. o Policajnom zbore (ďalej len „**Zákon o policajnom zbore**“).

[58] Článok 1 ods. 1 Policajnej smernice: „*Touto smernicou sa stanovujú pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu.*“

3.1.1. Spracúvanie informácií, účel a právny základ

Zber a spracúvanie nielen (osobných) údajov a potenciálne problémy pri týchto činnostiach sa netýkajú len využívania nových technológií vo verejnom priestore, ale sú ťažiskovou otázkou pri každej spracovateľskej operácií.

Úvodom je nevyhnutné zvýrazniť dva problémy. Na jednej strane je dôležité určiť, či v tejto fáze dochádza k zberu osobných alebo iných ako osobných údajov. Na druhej strane je z tohto hľadiska potrebné vymedziť aj to, čo vlastne tvorí zdroj týchto údajov. Pri analýze legislatívy ochrany osobných údajov vychádzame z implementácie Policajnej smernice v tretej časti Zákona o ochrane osobných údajov.

Prvým aspektom nevyhnutným na posúdenie je, či ide o zber a následné spracúvanie osobných alebo iných ako osobných údajov. Policajná smernica v článku 3 bode 1 obsahuje totožnú definíciu osobných údajov ako GDPR v článku 4 bode 1, podľa ktorého osobné údaje predstavujú *„akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.“*[59] Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo (prostredníctvom jedného identifikátora) alebo nepriamo (prostredníctvom viacerých identifikátorov). Zákon o ochrane osobných údajov demonštratívne vypočítava niektoré identifikátory ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkaz na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. V tomto kontexte je nutné poznamenať, že teória aj prax má tendenciu aplikovať definíciu osobného údaju značne extenzívne a dochádza tak k situácií, keď každá informácia má potenciál figurovať ako osobný údaj. Od osobných údajov musíme odlíšiť kategóriu iných ako osobných údajov. Iné ako osobné údaje definuje návrh nariadenia o voľnom toku iných ako osobných údajov[60] v článku 3 ods. 1 ako *„iné údaje ako osobné údaje, ktoré sú vymedzené v článku 4 ods. 1 nariadenia (EÚ) 2016/679.“* Nariadenie (EÚ) 2016/679 obsahuje v článku 4 ods. 1 totožnú definíciu pojmu osobný údaj ako vyššie uvedená definícia v Policajnej smernici. Z tohto dôvodu možno konštatovať, že do kategórie iných ako osobných údajov budú spadať všetky údaje, ktoré nespĺňajú definíciu pojmu osobný údaj podľa Zákona o ochrane osobných údajov resp. GDPR.

---

[59] Zákon o ochrane osobných údajov v § 2 definuje osobné údaje ako *„akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.“*

[60] Návrh Nariadenia Európskeho Parlamentu a Rady (EÚ) o rámci pre voľný tok iných ako osobných údajov v Európskej únii COM(2017) 495 final 2017/0228(COD).

V praxi je ale niekedy veľmi náročné určiť hranicu toho, čo je alebo nie je osobný údaj a to hlavne v dôsledku rozvoja nových technológií a unikátnych možností identifikácie osôb prostredníctvom zariadení a služieb napr. zákaznícka karta, cookies,[61] IP adresy,[62] IMEI[63] atď. Pri práci policajných zložiek to platí o to viac, že príslušníci policajných zložiek majú prístup k rôznym databázam, ktoré bežným občanom nie sú dostupné, prípadne disponujú oprávneniami (právnymi nástrojmi) na zistenie ďalších skutočností, na základe ktorých je možné konkrétnu osobu identifikovať. Ilustrovať to možno na príklade poskytovateľa internetového pripojenia alebo telekomunikačného operátora poskytujúceho informácie policajným zložkám o osobách registrovaných na určitý uzol v sieti alebo telekomunikačné pripojenie. Na základe vyššie uvedeného je možné konštatovať, že vzhľadom na kontext činnosti policajných zložiek vo všeobecnosti a právomoci tohto ozbrojeného zboru platí vysoká pravdepodobnosť identifikácie konkrétnych osôb na základe rôznych identifikátorov (uzol v sieti, poloha, použité telekomunikačné zariadenie) a v tom prípade sa bude jednať o osobné údaje v zmysle definície čl. 3 ods. 1 Policajnej smernice. Ak zozbierané a spracúvané údaje spĺňajú definíciu osobného údaju, potom je nevyhnutné spracovateľské operácie vykonávať v súlade s legislatívou upravujúcou konkrétne povinnosti pri spracúvaní osobných údajov s ohľadom na rešpektovanie práva na súkromný a rodinný život.

Druhým aspektom je, z akého zdroja údaje pochádzajú. Pri používaní prediktívnej analýzy údajov môžu mať zdroje údajov štyri podoby:

a) údaje dostupné iba orgánom verejnej moci;
b) otvorené údaje;
c) údaje v dispozícii súkromného sektora;
d) kombinácie vyššie uvedených.

Ad a) V prvom rade môže ísť o údaje, ktoré sú dostupné (v rámci databáz) iba orgánom verejnej moci a bežný občan k nim nemá prístup. Ilustrovať to možno na príklade údajov z elektronickej zdravotnej knižky,[64] údajov týkajúcich sa páchania priestupkovej alebo trestnej

[61] Súbory cookies slúžia na identifikáciu jednotlivých používateľov webových stránok a okrem iného obsahujú údaje o používateľských predvoľbách a preferenciách jednotlivých užívateľov.

[62] IP adresa je označenie uzla v internetovej sieti.

[63] IMEI je unikátne identifikačné číslo mobilného zariadenia v telekomunikačnej sieti.

[64] § 5 (1) b) zákona č.153/2013 Z. z. o národnom zdravotníckom informačnom systéme (Zákon o NZIS) definuje obsah elektronickej zdravotnej knižky. Elektronická zdravotná knižka obsahuje (i) identifikačné údaje osoby, (ii) elektronické zdravotné záznamy, (iii) údaje z účtu poistenca, (iv) vlastné záznamy osoby, (v) záznam o prístupe, o poskytnutí údajov a každý pokus o prístup alebo o poskytnutie údajov. Elektronický zdravotný záznam zahŕňa pacientsky sumár, záznam o preventívnej prehliadke, záznam žiadanky na vyšetrenia spoločných vyšetrovacích a liečebných zložiek vrátane popisu vzorky, záznam o výsledku vyšetrenia

činnosti, register obyvateľov SR,[65] evidencia držiteľov strelných zbraní[66] a podobne (príklady sú zasadené do reálií slovenského právneho poriadku).

Ad b) Ďalším zdrojom údajov, z ktorých je možné čerpať sú otvorené údaje. Zjednodušene povedané v tomto prípade ide o informácie od orgánov verejnej moci, ktoré sú voľne dostupné v špecifickej forme a štruktúre (datasetoch).

Ad c) Pri prediktívnej analýze údajov je možné využívať aj údaje, ktoré má k dispozícii súkromný sektor. Už v predchádzajúcich častiach práce bolo naznačené, že to budú údaje, ktoré sa predovšetkým týkajú informácií, na základe ktorých je možné identifikovať dotknutú osobu ako napríklad prevádzkovateľmi webových sídel, prevádzkovateľov internetového pripojenia, telekomunikačných operátorov alebo záznamy z priemyselných kamier, ktoré monitorujú priestor vo vstupnej hale súkromnej spoločnosti.

Ad d) Do úvahy prichádza aj kombinácia a analýza údajov z vyššie uvedených zdrojov, avšak predpokladá spoluprácu verejného a súkromného sektora.

Ak v rámci spracúvania údajov nastane situácia, že predmetné údaje sú osobné (aj keď osobné údaje tvoria iba časť datasetu), je nevyhnutné vykonávať spracúvanie osobných údajov v súlade s platnými právnymi predpismi na úseku ochrany osobných údajov.

Vymedzenie zdroja dát používaných v rámci prediktívnej analýzy značne pomôže k identifikácii ďalších dôležitých aspektov týkajúcich sa spracúvania osobných údajov.

Už samotné zbieranie osobných údajov predstavuje spracúvanie osobných údajov.[67] Recitál 34 Policajnej smernice uvádza, že *„spracú-*

---

spoločných vyšetrovacích a liečebných zložiek, záznam o zásahu pri poskytnutí neodkladnej zdravotnej starostlivosti, záznam o odporúčaní lekára na špecializovanú ambulantnú zdravotnú starostlivosť, záznam o odporúčaní ošetrujúceho lekára na prijatie do ústavnej zdravotnej starostlivosti, záznam o poskytnutej ambulantnej zdravotnej starostlivosti, záznam o prepustení osoby z ústavnej zdravotnej starostlivosti, preskripčný záznam, dispenzačný záznam, medikačný záznam, záznam návrhu na zaradenie do zoznamu poistencov čakajúcich na poskytnutie plánovanej zdravotnej starostlivosti.

[65] Zákon č. 253/1998 Z. z. o hlásení pobytu občanov Slovenskej republiky a registri obyvateľov Slovenskej republiky.

[66] § 64 a nasl. Zákona č. 190/2003 Z. z. o strelných zbraniach a strelive a zmene a doplnení niektorých zákonov.

[67] Čl. 3 ods. 2 Policajnej smernice definuje spracúvanie (osobných údajov) ako *„operáciu alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie,* štruktúrovanie*, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.“*

vanie osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu by malo zahŕňať akúkoľvek operáciu alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov na uvedené účely, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, preskupovanie alebo kombinovanie, obmedzenie spracúvania, vymazanie alebo likvidácia, a to bez ohľadu na to, či sa vykonávajú automatizovanými prostriedkami alebo inými prostriedkami.“ Z tohto hľadiska prevádzkovateľ (v týchto prípadoch policajné zložky alebo im organizačne nadriadená entita) musí nevyhnutne disponovať (i) účelom spracúvania osobných údajov a (ii) platným právnym základom. § 53 Zákona o ochrane osobných údajov ustanovuje, že osobné údaje musia byť získané na konkrétne určené, výslovné uvedené a legitímne účely a nesmú byť spracúvané spôsobom, ktorý je nezlučiteľný s týmito účelmi. Inými slovami, prevádzkovateľ je povinný vymedziť prečo vykonáva spracovateľské operácie Účel v kontexte spracúvania osobných údajov v rámci Policajnej smernice je explicitne uvedený v samotnej smernici, ktorá sa vzťahuje na *„spracúvanie osobných údajov príslušnými orgánmi na účely **predchádzania** trestným činom, ich vyšetrovania, **odhaľovania** alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu.“*[68] Z toho vyplýva, že aj použitie prediktívnej analýzy údajov, ktorá slúži primárne na prevenciu a včasné zabránenie páchania kriminality je zahrnuté vo vyššie uvedenom vymedzení účelu spracovateľskej operácie. Podrobnejšiu právnu úpravu obsahuje Zákon o policajnom zbore, ktorý priamo v § 69a[69] ods. 1 ustanovuje špecifické povinnosti z hľadiska účelu pri spracúvaní osobných údajov pri plnení úloh policajného zboru na účely trestného konania. Špecificky je policajný zbor pri získavaní a spracúvaní osobných údajov povinný (i) písomne určiť účel, na ktorý sa majú osobné údaje spracúvať, (ii) zhromažďovať osobné údaje zodpovedajúce len určenému účelu a v rozsahu nevyhnutnom na určený účel, (iii) uchovávať osobné údaje len na čas, ktorý je nevyhnutný na účely ich spracúvania a (iv) spracúvať osobné údaje získané na tieto účely oddelene od osobných údajov spracúvaných pri plnení iných úloh Policajného zboru. V týchto ustanoveniach je pretavená zásada vymedzenia účelu

[68] Článok 1 ods. 1 Policajnej smernice.

[69] Vychádzame z verzie účinnej a platnej od 25.5.2018.

spracúvania osobných údajov, zásada minimalizácie uchovávania údajov a zásada bezpečnosti.

Právny základ – titul spracúvania osobných údajov je v tomto prípade priamo závislý od výslovného vymedzenia účelu. Toto konštatovanie vyplýva z dikcie § 55 ods. 1 podľa ktorého *„príslušný orgán je oprávnený spracúvať osobné údaje na plnenie úloh na účely trestného konania podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.“*

3.1.2. Niektoré špecifiká Policajnej smernice

Pri zbieraní a spracúvaní osobných údajov a ich následnom použití v rámci prediktívnej analýzy údajov je nevyhnutné upriamiť pozornosť na špecifické povinnosti, ktoré orgánom činným v trestnom konaní vyplývajú z Policajnej smernice.

Ako už bolo v predchádzajúcich častiach práce stručne naznačené, Zákon o ochrane osobných údajov operuje § 57 s rozlišovaním medzi rôznymi kategóriami dotknutých osôb, teda jednotlivcov, ktorých sa osobné údaje spracúvané na účely podľa smernice týkajú. Predmetné kategórie možno diferencovať na:

e) Podozrivých - osoby, v prípade ktorých sa možno odôvodnene domnievať, že spáchali alebo sa chystajú spáchať trestný čin;
f) Odsúdených - osoby odsúdené za spáchanie trestného činu;
a) (Potenciálne) obete - obete trestného činu, alebo osoby, v prípade ktorých sú na základe určitých skutočností dôvody domnievať sa, že sú alebo by mohli byť obeťami trestného činu; a
b) Iné tretie osoby - napríklad osoby, ktoré môžu byť vyzvané, aby svedčili v rámci vyšetrovania v súvislosti s trestnými činmi alebo v rámci následného trestného konania, osoby, ktoré môžu poskytnúť informácie o trestných činoch, alebo kontaktné osoby či spoločníci niektorej z osôb uvedených v písmenách a) a b).

Policajná smernica zakotvuje povinnosť „jasne rozlišovať“ medzi vyššie uvedenými kategóriami osobných údajov. To v praxi môže znamenať, že v informačných systémoch a pri spracúvaní údajov policajnými zložkami je nevyhnutné okrem osobných údajov mať aj informáciu, o ktorú kategóriu dotknutej osoby ide.

Ďalším aspektom je rozlišovanie medzi osobnými údajmi z hľadiska kvality. Článok 7 ods. 1 Policajnej smernice ustanovuje povinnosť, čo najprecíznejšie diferencovať *„osobné údaje založené na skutočnostiach od osobných údajov založených na osobných hodnoteniach.“* Predmetnú požiadavku možno ilustrovať na príklade, keď si príslušník policajných zložiek pri vyšetrovaní zapisuje poznámky a svoje

osobné dojmy napr. z výsluchu svedka alebo obhliadky miesta spáchania trestného činu. Predmetné ustanovenie smernice dopĺňa § 58 ods. 3 Zákona o ochrane osobných údajov na základe ktorého *„príslušný orgán k poskytnutiu a prenosu osobných údajov pripojí dostupné informácie, ktoré umožnia prijímajúcemu príslušnému orgánu posúdiť ich mieru správnosti, úplnosti, aktuálnosti a spoľahlivosti, ak to okolnosti dovoľujú. Nesprávne osobné údaje príslušný orgán nemôže poskytovať a prenášať; neoverené osobné údaje príslušný orgán musí pri poskytovaní alebo prenose takto označiť a musí uviesť mieru ich spoľahlivosti. Ak príslušný orgán neoprávnene poskytne osobné údaje alebo neoprávnene prenesie osobné údaje alebo poskytne nesprávne osobné údaje alebo prenesie nesprávne osobné údaje, je povinný bez zbytočného odkladu informovať príjemcu a žiadať príjemcov osobných údajov, ktorým sa také osobné údaje poskytli, aby ich bez zbytočného odkladu opravili, doplnili, vymazali alebo aby obmedzili spracúvanie takých osobných údajov.“*

Ustanovenia smernice dopĺňa aj Zákon o policajnom zbore, ktorý výslovne zakotvuje možnosť spracúvať aj nepravdivé osobné údaje za podmienky, že sa za nesprávne označia.[70]

Takéto údaje je teda potrebné vnímať v inom režime a s náležitou opatrnosťou. V tomto kontexte je ale potrebné poznamenať, že v prípade prediktívnej analýzy údajov by dáta mali byť zbierané a spracúvané v určitej kvalite a na tieto účely by nemali byť využívané údaje, ktoré tvoria osobné hodnotenia. Avšak, ak by aj dochádzalo k spracúvaniu údajov založených na osobných skutočnostiach, na mieste je legitímna otázka, ako sa s touto skutočnosťou vysporiadať pri programovaní a nastavení algoritmu, ktorý prediktívnu analýzu vykoná.

Policajná smernica podobne ako GDPR diferencuje medzi osobnými údajmi a osobitnými kategóriami osobných údajov – tzv. citlivé osobné údaje.[71] Základne pravidlo spracúvania týchto údajov je, že ich spracúvanie je možné len vtedy, ak je úplne nevyhnutné (vzhľadom na účel) a podlieha primeraným zárukám ochrany práv a slobôd dotknutej osoby a to len v prípade (i) ak je prípustné podľa práva Únie alebo práva členského štátu, (ii) ochraňuje životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby, alebo (iii) ak sa takéto spracúvanie týka údajov,

[70] § 69a ods. 2 Zákona o policajnom zbore.

[71] Článok 10 Policajnej smernice definuje osobitné kategórie osobných údajov ako údaje, ktoré *„odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na účely individuálnej identifikácie fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby“*

ktoré preukázateľne sprístupnila dotknutá osoba.[72] Spracúvanie údajov z verejne dostupných registrov prípadne vo forme otvorených údajov tak spĺňa požiadavku sprístupnenia dotknutou osobu. V ostatných prípadoch je ale nutné hľadať osobitnú právnu úpravu, ktorej účel by spracúvanie citlivých osobných údajov povoľovalo. V kontexte spracúvania citlivých osobných údajov Policajným zborom SR je táto požiadavka splnená v Zákone o policajnom zbore, kde § 69 ods. 3 dovoľuje Policajného zboru pri plnení úloh v súvislosti s trestným konaním spracúvať aj citlivé osobné údaje. Navyše, Policajný zbor SR je oprávnený spracúvať osobitné kategórie osobných údajov aj o osobách určitej komunity, ktoré spáchali trestný čin, ak sa hromadne vyskytujú trestné činy páchané osobami tejto komunity.

3.1.3. Posúdenie vplyvu

Policajná smernica v článku 27 (analogicky § 42 Zákona o ochrane osobných údajov) upravuje inštitút tzv. posúdenia vplyvu na ochranu údajov. Tento inštitút je v rámci rekodifikácie právnej úpravy ochrany osobných údajov jedným z najžiarivejších príkladov zmeny základných pravidiel v tejto oblasti. Do 25.5.2018 totiž bola zakotvená povinnosť prevádzkovateľov notifikovať dozorný orgán o tom, že vykonávajú spracovateľské operácie. Od účinnosti GDPR a Policajnej smernice už ale táto povinnosť odpadá a na miesto toho je prevádzkovateľ povinný niesť zodpovednosť za spracovateľské operácie a vykonať určité úkony, ktoré mu legislatíva predpisuje. Posúdenie vplyvu na ochranu údajov znamená že *„ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, členské štáty stanovia, že prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.“*[73] Druhý odsek obsahuje konkrétne požiadavky na dosiahnutie súladu a efektívne využitie tohto inštitútu. Posúdenie vplyvu na ochranu údajov by malo obsahovať minimálne (i) opis plánovaných spracovateľských operácií, (ii) hodnotenie rizík pre práva a slobody dotknutých osôb, (iii) opatrenia na riešenie daných rizík, záruky, (iv) bezpečnostné opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu s touto smernicou, s ohľadom na práva a oprávnené záujmy dotknutých osôb a prípadných ďalších osôb.

[72] Článok 10 Policajnej smernice.
[73] Článok 27 ods. 1 Policajnej smernice.

Na tomto mieste je nevyhnutné vyhodnotiť, či (i) posúdenie vplyvu na ochranu údajov je potrebné vykonať v kontexte prediktívnej analýzy údajov a ak je odpoveď kladná (ii) ako ku predmetnému posúdeniu vplyvu metodologicky pristúpiť.

Policajná smernica ako určujúce kritérium pre vykonanie posúdenia vplyvu na ochranu údajov nastavuje, či spracovateľská operácia povedie k vysokému riziku pre práva a slobody fyzických osôb. Pracovná skupina čl. 29 vo svojom usmernení k diskutované inštitútu (ďalej len „**Usmernenie**“)[74] determinovala deväť indikátorov, na základe ktorých možno vyhodnotiť, či pri spracúvaní osobných údajov dochádza k vysokému riziku pre práva a slobody fyzických osôb. Kritéria vysokého rizika sú:

a) Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby;
b) Automatizované rozhodovanie s právnym alebo podobne závažným účinkom;
c) Systematické monitorovanie osobných údajov;
d) Spracúvanie citlivých osobných údajov;
e) Spracúvanie údajov vo veľkom rozsahu;
f) Spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií;
g) Spracúvanie údajov týkajúcich sa „zraniteľných“ dotknutých osôb;
h) Využitie nových technológií, technologických alebo organizačných riešení a postupov;
i) Spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu.

Ad a) Pracovná skupina čl. 29 vo svojom Usmernení výslovne zahŕňa medzi príklady vyhodnocovania určitých aspektov dotknutých osôb profilovanie a vytváranie predpovedí o dotknutej osobe. Medzi relevantné aspekty demonštratívne uvádza hodnotenie činnosti dotknutej osoby v rámci výkonu práce, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom. Nie je nutné opäť zdôrazňovať, že všetky vyššie uvedené aspekty môžu byť predmetom spracúvania v rámci prediktívnej analýzy údajov.

Ad b) Ďalší indikátor predstavuje situácia, ak je spracúvanie osobných údajov vykonané automatizovane s automatizovaným rozhodnu-

[74] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, s. 9-11.

tím, ktoré má právny alebo podobne závažný účinok na dotknutú osobu. Zjednodušene povedané, automatizované rozhodovanie je také, v ktorom nie je prítomný ľudský zásah. Ilustrovať to možno na príklade turniketu, ktorý sa otvorí alebo neotvorí na základe priloženia identifikačnej karty na skener. Prediktívna analýza údajov je do istej miery závislá na automatizovanom rozhodovaní algoritmu, aj keď samotný výkon činnosti vykonávajú príslušníci policajného zboru. Avšak samotná predikcia je iba v réžii algoritmu. Rozhodnutie v rámci predpovede následne vytvára priestor pre aplikáciu či už preventívnych alebo donucovacích prostriedkov pri činnosti policajtov a to môže mať vplyv na práva a slobody dotknutých osôb. Vzhľadom na to je možné konštatovať, že aj tento indikátor v súvislosti s prediktívnou analýzou údajov je relevantný.

Ad c) Systematické monitorovanie údajov je potrebné interpretovať v intenciách takých situácií, keď dotknuté osoby nevedia, že sú sledované a údaje o nich zhromažďované a spracúvané. Tento záver vystihuje aj podstatu prediktívnej analýzy údajov na účely prevencie kriminality bez (priameho) vedomia dotknutých osôb.

Ad d) Ďalším indikátorom je spracúvanie citlivých osobných údajov a údajov týkajúcich sa páchanie priestupkov a trestných činov. Ako už bolo na iných miestach predkladanej práce uvedené, pri prediktívnej analýzy údajov prirodzene dochádza k spracúvaniu týchto kategórií osobných údajov. Navyše, Pracovná skupina čl. 29 uvádza, že medzi citlivé osobné údaje možno zahrnúť aj osobné dokumenty, elektronické správy, denníky, poznámky a údaje spracúvané v rámci mobilných aplikácií, ktoré odhaľujú osobnostné aspekty o dotknutých osobách.

Ad e) Posúdenie vplyvu na ochranu údajov je potrebné vykonať aj v prípadoch, ak spracúvanie je vykonávané vo veľkom rozsahu. Pracovná skupina čl. 29 menuje faktory, ktoré indikujú, či ide o spracúvanie osobných údajov vo veľkom rozsahu alebo nie – (i) počet dotknutých osôb, (ii) kvantita údajov a ich rozsah, (iii) doba spracovateľskej operácie a (iv) geografických rozsah spracúvania osobných údajov. Pri využití prediktívnej analýzy údajov určite ide o spracúvanie obrovského množstva údajov o nepomerne veľkom množstve dotknutých osôb. Tieto údaje môžu byť uchovávané po značne dlhú dobu vzhľadom na ich potenciál a účel – prevencia kriminality. Možno povedať, že pri takejto spracovateľskej operácií ide o dotknuté osoby na území Slovenskej republiky, takže geografický rozsah je daný hranicami štátu. Samozrejme, nie je vylúčené, že v rámci cezhraničnej spolupráci policajných zložiek dôjde aj k spracúvaniu osobných údajov o dotknutých osobách, ktoré sa momentálne na území Slovenskej republiky nenachádzajú.

Ad f) Pri prediktívnej analýze údajov je imanentné prítomné spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií, keďže hovoríme o spracúvaní údajov pochádzajúcich z viacerých zdrojov (verejné registre, otvorené údaje, verejne dostupné sociálne siete atď.).

Ad g) Zraniteľné osoby sú v diskutovanom Usmernení Pracovnej skupiny čl. 29 vymedzené ako také osoby, ktoré nie sú v rovnoprávnom postavení voči prevádzkovateľovi, čo sa okrem iného prejavu nemožnosťou oponovať rozhodnutiu. Predmetný aspekt je prítomný aj pri práci Policajného zboru, keďže príslušníci tohto ozbrojeného zboru disponujú prostriedkami, voči ktorým ich adresát nemá možnosť rozhodnutia, či ich akceptuje alebo nie napr. kontrola automobilového prostriedku policajtom alebo použitie donucovacích prostriedkov v zákonom vymedzenom rozsahu.

Ad h) Prediktívna analýza údajov reprezentuje využitie nových technológií, technologických alebo organizačných riešení a postupov.

Ad i) Ku spracúvaniu údajov, ktoré bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu dochádza napr. vtedy, keď banka preverí klienta v referenčnej databáze úverov a na základe toho s ním neuzavrie zmluvu. Tento faktor je pri prediktívnej analýze údajov irelevantný.

Vzhľadom na vyššie uvedené je na mieste zvýrazniť, že osem z deviatich indikátorov vysokého rizika pre práva a slobody dotknutých osôb je pri využití prediktívnej analýzy údajov splnených. Z tohto dôvodu sa domnievame, že je nevyhnutné posúdenie vplyvu na ochranu údajov vykonať. Tento inštitút je potrebné aplikovať pred začatím využívania predmetnej metódy a pred zbieraním dát z rôznych zdrojov.

Policajný zbor SR by mal posúdenie vplyvu vykonať komplexne z hľadiska využitia prediktívnej analýzy na celom území štátu. To znamená, že v prípade, ak by diskutovanú metódu využívalo viacero organizačných zložiek v rámci Policajného zboru SR, je možné argumentovať, že posúdenie vplyvu je nevyhnutné vykonať iba raz pre Policajný zbor SR ako celok.[75]

Samotné posúdenie vplyvu obsahuje niekoľko krokov, ktoré je potrebné pri aplikácií tohto inštitútu dodržať. Prvým krokom je charakteristika spracovateľských operácií v aspoň všeobecnom meradle.

[75] Pozri analogicky Recitál 92 GDPR: *„Existujú okolnosti, za ktorých môže byť vhodné a hospodárne, aby sa predmet posúdenia vplyvu na ochranu údajov nevzťahoval len na jeden projekt, ale bol širší, napríklad ak orgány verejnej moci alebo verejnoprávne subjekty zamýšľajú vytvoriť spoločnú aplikáciu či spracovateľskú platformu alebo ak niekoľko prevádzkovateľov zamýšľa zaviesť spoločnú aplikáciu či spracovateľské prostredie v rámci odvetvia alebo segmentu priemyslu alebo na široko rozvetvenú horizontálnu činnosť.“*

Spolu s opisom spracovateľskej operácie je potrebné pozornosť upriamiť aj na nevyhnutnosť a proporcionalitu spracúvania osobných údajov a opatrenia, ktoré sú už pretavené do praxe. Pri testovaní nevyhnutnosti a proporcionality je primerane vhodné vziať do úvahy, že prediktívna analýza údajov sa uskutočňuje za účelom prevencie kriminality a teda vo verejnom záujme. Bezpečnosť občanov by mala byť jedným z najdôležitejších postulátov v demokratickom a právnom štáte. Druhým krokom je analýza rizika pre práva a slobody dotknutých osôb. V tejto súvislosti je potrebné preskúmať povahu, účely, rozsah a kontext spracovateľských operácií.[76] Identifikátory vysokého rizika sú uvedené v predchádzajúcej stati. Tretím krokom je zavedenie opatrení na riešenie daných rizík, záruky, bezpečnostné opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov. V praxi by sa mohlo jednať o autorizovanie konkrétnych osôb, ktoré majú prístup k osobným údajom, šifrovanie a pseudonimizácia údajov či zavedenie pravidelných auditov.

3.1.4. Špecificky navrhnutá a štandardná ochrana osobných údajov

Ak už máme osobné prípadne iné ako osobné údaje zozbierané, ďalším krokom prediktívnej analýzy údajov je samotný proces dátovej analýzy. V tejto súvislosti je potrebné poznamenať, že dátovú analýzu nevykonáva človek, ale údaje sú vyhodnocované algoritmom (počítačovým programom), primárne bez ľudského zásahu prostredníctvom metód lineárnej regresie a strojového učenia.

Na prvý pohľad by sa mohlo zdať, že právo nedisponuje nástrojmi na korigovanie alebo úpravu špecifických povinností pre procesy vykonané algoritmom. Domnievame sa, že opak je pravdou. V tejto súvislosti považujeme za osobitné dôležité zvýrazniť špecifický inštitút na úseku ochrany osobných údajov – špecificky navrhnutá a štandardná ochrana osobných údajov. Predmetný inštitút zohráva významnú rolu práve pri vyhodnocovaní osobných údajov prostredníctvom algoritmu. Samozrejme, tento inštitút sa aplikuje iba v prípadoch, keď dochádza k spracúvaniu osobných údajov.

Policajná smernica uvádza v článku 20 jednu z noviniek v legislatíve ochrany osobných údajov (analogicky § 32 Zákona o ochrane osobných údajov). Predmetný článok ustanovuje, že jednou z povinností prevádzkovateľa je *„so zreteľom na najnovšie poznatky. náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúva-*

[76] Pozri analogicky Recitál 76 GDPR.

nia, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.“ Toto ustanovenie je predmetom mnohých diskusií a problémov súvisiacich s jeho výkladom a správnym pochopením.

Špecificky navrhnutá ochrana údajov zjednodušene znamená, že už od raných fáz plánovania spracovateľských operácii a taktiež v čase ich výkonu, je potrebné brať na zreteľ ochranu osobných údajov dátových subjektov. V takom prípade je možné determinovať riskantné operácie už v úvodnej fáze a ešte pred implementáciou spracovateľskej operácie a v konečnom dôsledku ušetriť nemalé finančné prostriedky prevádzkovateľom. V kontexte prediktívnej analýzy údajov to znamená, že už pri programovaní algoritmu, ktorý bude vyhodnocovať údaje a vytvárať predpovede je potrebné vziať do úvahy osobitosti takýchto spracovateľských operácií a ich dopad na základné práva a slobody dotknutých osôb.

Tento inštitút je odvodený od všeobecne uznávanej koncepcie Privacy by Design (špecificky navrhnutá ochrana súkromia). Možno konštatovať, že špecificky navrhnutá ochrana osobných údajov je jeho sub-kategóriou. Ann Cavoukian určila sedem nosných zásad,[77] na ktorých musí stáť každé poňatie vyššie diskutovaného inštitútu. Na tomto mieste považujem za vhodné tieto zásady uviesť a analyzovať z hľadiska ochrany osobných údajov a prediktívnej analýzy údajov. Konkrétne ide o tieto zásady:

1. Byť proaktívny, nie reaktívny
2. Ochrana súkromia ako pôvodné (predvolené) nastavenie
3. Ochrana súkromia zabudovaná vo výslednom produkte
4. Úplná funkčnosť (zásada plusovej hodnoty)
5. Bezpečnosť od začiatku až do konca
6. Viditeľnosť a transparentnosť
7. Rešpektovanie súkromia užívateľa

Ad 1) Proaktívny prístup v tomto význame znamená, že prevádzkovatelia by mali v prvom rade prechádzať neželaným únikom dát alebo iným bezpečnostným incidentom. Prevádzkovatelia by mali predvídať

[77] CAVOUKIAN, A.: *Privacy by Design – The Seven Foundational Principles*, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (dostupné 18.3.2018).

a koncipovať preventívne opatrenia, inými slovami byť povestný „krok vpred“ pri analýze rizík spracovateľských operácii. Pri samotnom programovaní alebo výbere algoritmu, ktorý bude prediktívnu analýzu dát vykonávať je tak potrebné dbať na potenciálne rizika spracovania už pri výbere prípadne programovaní novej technológie. Samotné predvídanie predpokladaných problémov by malo byť založené na kooperácií príslušníkov Policajného zboru SR, dátových analytikov, právnikov a špecialistov na bezpečnosť IT systémov.

Ad 2) Predvolené nastavenie akéhokoľvek systému, produktu alebo aplikácie musí v prvom rade chrániť súkromie užívateľa. Prakticky to znamená, že aj bez aktivity užívateľa je nutné zabezpečiť, čo najpreciznejšiu ochranu dotknutej osoby. Policajná smernica túto požiadavku precizuje v rámci tzv. štandardnej ochrany osobných údajov.[78] Možno zhrnúť, že efektívna aplikácia diskutovanej zásady vyžaduje dôsledné plnenie zásady minimalizácie údajov a minimalizácie uchovávania. Inými slovami, malo by sa spracúvať iba obmedzené množstvo údajov nevyhnutných na daný účel a iba po nevyhnutne dlhé časové obdobie. V kontexte prediktívnej analýzy údajov a Policajného zboru SR je však súlad s vyššie uvedenými požiadavkami značne problematický, keďže na účely prevencie kriminality môže slúžiť obrovské množstvo údajov, ktorých uchovávanie po značne dlhú dobu môže byť legitímne, keďže niektoré (budúce) vzorce správania sa môžu prejaviť až pri kombinácií údajov. To ale neznamená, že pri výbere prípadne programovaní algoritmu by sa nemohol vybrať ten nástroj, ktorý najlepšie dokáže chrániť súkromie užívateľa v predvolenom režime a invazívnejšie zásahy spôsobovať iba vo vymedzených prípadoch (napr. riešenie prípadov týkajúcich sa organizovaného zločinu, terorizmu alebo vraždy).

Ad 3) Zabudovanie ochrany súkromia do výsledného produktu vyjadruje integrálne spojenie výsledku technologického procesu a ochrany súkromia. Nemožno ich nikdy vnímať oddelene a opatrenia na ochranu súkromia sa nemôžu vyskytovať v podobe nutných vylepšení alebo doplnkov. V kontexte ochrany osobných údajov to znamená už vyššie uvedené prihliadanie na predmetné aspekty pred spracovateľskou operáciou. Na ochranu osobných údajov je potrebné myslieť od momentu prvotného plánovania kreovania novej technológie. Vyššie

[78] Článok 20 Policajnej smernice: *„...prevádzkovateľ vykoná primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.“*

uvedené je nevyhnutné brať na zreteľ aj pri programovaná alebo výbere algoritmu, ktorý bude predpovedať správanie dotknutých osôb.

Ad 4) Zásada plusovej hodnoty predstavuje myšlienku, že ochrana súkromia nemôže byť substituovaná namiesto iných hodnôt. Ilustrovať to možno na príklade, keď rôzne funkcie sú implementované na úkor ochrany súkromia (obmedzenie funkcionality produktu prevádzkovateľom z dôvodu zvýšenia ochrany osobných údajov). V súvislosti s prediktívnou analýzou údajov tak nemôže ochrana súkromia predstavovať akési „nutné zlo" alebo opatrenie, ktoré je nutné si splniť a obmedziť fungovanie algoritmu. V ideálnom prípade sa na riziká ochrany súkromia myslí už pri návrhu algoritmu a pri jeho programovaní. Následne je tak znížená pravdepodobnosť, že by súlad s legislatívou akokoľvek obmedzil výkon a analýzu algoritmu.

Ad 5) Efektívna aplikácia špecificky navrhnutej ochrany súkromia pred spracovateľskou operáciou znamená, že dáta podliehajú bezpečnostným opatreniam od momentu ich zberu až po ich koncovú deštrukciu. Tieto aspekty rieši množstvo inštitútov, ilustratívne možno uviesť pseudonymizáciu alebo anonymizáciu údajov, zásadu minimalizácie údajov, časové rámce stanovené zákonodarcom a pod. Pri práci s osobnými údajmi v rámci Policajného zboru SR je túto požiadavku možné ešte viac zvýrazniť, keďže samotné údaje, ktoré má tento ozbrojený zbor k dispozícii môžu byť veľmi citlivé a navyše, predpovede ohľadom budúcej kriminality by sa taktiež nemali dostať do nepovolených rúk.

Ad 6) Viditeľnosť alebo transparentnosť možno vyjadriť ľudovým „dôveruj ale preveruj." V tomto význame je esenciálnou súčasť spracovateľskej operácie dodržanie sľubov a cieľov z hľadiska ochrany súkromia. GDPR predmetnú požiadavku konzervuje v zásade transparentnosti alebo v inštitútoch zabezpečujúcich nezávislý dozor nad úsekom ochrany osobných údajov. Na rozdiel od Nariadenia, Policajná smernica vzhľadom na jej pôsobnosť (orgány činné v trestnom konaní) oslabuje zásadu transparentnosti, ktorá je prevážená účelom spracúvania osobných údajov, keďže zverejnenie informácií týkajúcich sa prebiehajúceho vyšetrovania by akiste zmarilo daný zámer.

Ad 7) Výrobcovia produktov musia pracovať s ideou, že záujmy spotrebiteľa alebo užívateľa sú na prvom mieste. Ak hovoríme o ochrane súkromia, tak tento postulát možno implementovať do užívateľsky prívetivého prostredia nastavenia súkromia. Inými slovami, dátový analytik musí byť schopný ovládať algoritmus a policajt musí byť schopný správne interpretovať výsledok prediktívnej analýzy údajov.

Implementácia inštitútov špecificky a štandardne navrhnutej ochrany osobných údajov by mala v dostatočnej miere zabezpečiť, že analýza údajov je vykonaná v súlade právom na ochranu osobných úda-

jov. Zosúladenie postupu pri práci policajných zložiek s diskutovanými inštitútmi je navyše silným argumentačným faktorom pri preukazovaní súladnosti s príslušnou legislatívou.

3.2. Vytvorenie predpovede

Druhou fázou prediktívnej analýzy údajov je azda najdôležitejšia časť – vytvorenie samotnej predpovede, ktorá je základom celého procesu. Táto fáza je charakteristická tým, že je plne automatizovaná a predpoveď tvorí algoritmus s minimálnym (ideálne žiadnym) ľudským zásahom na základe zozbieraných údajov. Domnievame sa, že základným atribútom predikcie musí byť jej objektivita. Z tohto hľadiska je preto nevyhnutné posúdiť, či algoritmus môže pri svojej analýze pracovať s predsudkami, ktoré majú ľudské bytosti. V takom prípade by niektoré predpovede mohli mať diskriminačný efekt a viesť k porušeniu zákazu diskriminácie tak, ako je uvedená v Dohovore či Charte.

Pri tvorbe umeleckých diel je častým javom, že autor pri ich tvorbe prežíva určité emócie, ktoré sú následne pozorovateľné v básni, novele alebo obraze. Dnes už síce nemôžeme so 100 % pravdepodobnosťou rekonštruovať pocity fyzickej osoby v minulosti, ale tieto reflexie je vidieť v jej umeleckej tvorbe. Podobne ako ľudské emócie, môžu byť do umeleckých diel prenesené aj predsudky autora. Predsudky môžu byť voľne definované ako odklon od normativity alebo racionality pri usudzovaní. Podľa Šinského je predsudok *„sklon ku chybe...a... je voľným prekladom anglického slova ´bias´ a vyjadruje rozdiel medzi skutočným konaním (deskripciou) a predikciou určitých normatívnych modelov.“*[79] Tento *„sklon k chybe v sebe zahŕňa tendenciu/náklonnosť k dopúšťaniu sa chybných rozhodnutí na systematickej a predvídateľnej báze.“*[80]

Predsudky sú takmer neoddeliteľnou súčasťou ľudského uvažovania a ľudského bytia ako takého. Často sa v živote stretávame s predsudkami voči určitej rase, povolaniu alebo jednoduchému hodnoteniu inej osoby na základe toho, čo má oblečené alebo akú má prácu.[81]

Úvodom tejto časti sme načrtli, akým spôsobom sa predsudky môžu odzrkadľovať v umeleckých dielach. Následne je potrebné položiť si

[79] ŠINSKÝ, M. (2010). Taxonómia sklonov k chybám. In BAČOVÁ , V. (ed.), Rozhodovanie a usudzovanie. Pohľady psychológie a ekonómie I. Bratislava: Ústav experimentálnej psychológie SAV, s. 162.

[80] Tamže.

[81] Pozri viac GÁBRIŠ, T. *Kognitívne sklony v právnej vede a právnej prax* In GÁBRIŠ, T a kol.: Nedogmatická právna veda. Od marxizmu po behaviorálnu ekonómiu. Wolters Kluwers, Praha, 2018, s. 229 - 247.

otázku, či predsudky nemôžu byť prítomné aj v algoritme (počítačovom programe), keďže ako taký je tiež vytváraný človekom a zákonodarca sa ho rozhodol chrániť v režime autorského práva – teda ako diela ostatných umelcov s určitými špecifikami.[82] Predmetná myšlienka možno vyznieva ako z vedecko-fantastického románu, avšak štúdie ukazujú, že algoritmy skutočne môžu predsudkami disponovať a tým ovplyvňovať výsledky ich analýzy a mať diskriminačný efekt.[83]

Diskriminačné efekty pri výsledkoch analýzy algoritmov nastávajú predovšetkým v prípadoch, keď rozhodnutia sú vytvorené na základe algoritmu, ktorý je zostavený na báze strojového učenia. To znamená, že algoritmus ako taký sa učí na základe vlastných „skúseností" a nadobúda nové funkcie svojou vlastnou činnosťou, ktorá možno nebola ani predpokladaná v prvotnej fáze tvorby algoritmu. Tieto „skúsenosti" naberá vzhľadom na to, že spracúva obrovské množstvo údajov a vyhľadáva v nich vzorce, ktoré sú bežne ľudským okom neviditeľné. V skutočnosti ale môže dochádzať k situáciám, keď takéto rozhodnutia samo-učiaceho sa algoritmu môžu byť ovplyvnené ľudskými predsudkami a nemožno uplatniť prezumpciu, že rozhodnutia urobené umelou inteligenciu sú zbavené vplyvov ľudských neduhov.[84]

K rozhodnutia urobených algoritmom s diskriminačným efektom môže dochádzať v troch prípadoch. V prvom prípade ide o situácie, keď sú algoritmy trénované na historických príkladoch, v ktorých je prítomný predsudok alebo zaujatosť. K takejto situácií môže dochádzať v praxi vtedy, keď je algoritmus trénovaný a naučený na analýzu situácií, v ktorých dochádzalo k nerovnakému zaobchádzaniu zo strany ľudí napr. ak pri predchádzajúcich výberových konaniach vedených človekom na určitú pracovnú pozíciu dochádzalo k nerovnakému zaobchádzaniu resp. k diskriminácií (na základe rasy, pohlavia, sexuálnej orientácie, vzdelania atď.) a tieto dáta sú následne vložené a vyhodnocované algoritmom. Tento algoritmus nemusí nutne rozpoznať, že v minulosti k takémuto správaniu došlo a z tejto historickej skúsenosti môže čerpať aj naďalej a pri ďalších výberových konania, ktoré bude vyhodnocovať zohľadniť túto skúsenosť a produkovať ďalšie diskriminačné výsledky. Podobný prípad sa stal pri práci policajných zložiek v New Yorku, kde väčšina predpovedí algoritmu mierila voči minoritám a následne boli poslané policajné hliadky práve do oblastí, kde tie-

[82] § 87 a nasl. zákona č. 185/2015 Z. z. Autorský zákon.

[83] KROLL, J. - HUEY, J. - BAROCAS, S. - FELTEN, E.- REIDENGERG, J. - ROBINSON, D. - YU, H.: Accountable Algorithms *In University of Pennsylvania Law Review, Vol. 165*.

[84] SCHWARTZ, P.: Data processing and Government Administration: The Failure of the American Legal Response to Computer *In 43 Hastings Law Journal 1992*, s. 1321 a 1342.

to minority žili, napriek tomu, že nie vždy to malo relevantný základ.[85] Možno si predstaviť, že pri práci policajného zboru by mohlo dochádzať aj k takýmto prípadom, keď by na základe predchádzajúcej činnosti policajtov dochádzalo k produkovaniu diskriminačných rozhodnutí napr. voči rómskej komunite.

Druhým prípadom keď môže dochádzať k diskriminácií je nevhodne zvolený model údajov. To znamená, že určitému typu údaju (pohlavie, rasa) sa výslovne určí vyššia priorita a takomto prípade to môže viesť až ku systematickej diskriminácií.[86] V súvislosti s prediktívnou analýzou údajov na úseku Policajného zboru SR je možné predstaviť si prípady, keď určitému údaju je pripisovaná väčšia či menšia hodnota ako napr. príslušnosť k etnickej skupine alebo národnostnej menšine, zamestnanie, vzdelanie alebo či ide o bezdomovca alebo vysokoškolského profesora. V takomto prípade je predsudok neoddeliteľnou súčasťou rozhodovacích procesov algoritmu a vytvára diskriminačné efekty.

Tretím spôsobom ako ovplyvňovať algoritmus pri rozhodovaní je úmyselný výber takých údajov, ktoré budú vytvárať rozhodnutia s predsudkami alebo zaujatosťou. Takýto výber sa primárne uskutočňuje vo fáze kreovania rozhodovacieho modelu algoritmu, ktorý následne generuje diskriminačné rozhodnutia.[87]

Z vyššie uvedenej štúdie tak vyplýva, že aj algoritmy za určitých okolností môžu mať predsudky ako ľudské bytosti. Takéto rozhodovanie by však značne ohrozilo dodržiavanie zákazu diskriminácie a taktiež aj právo na dobrú správu, keďže jednou z integrálnych zásad tohto práva je aj zásada rovnosti a zásada objektivity. Otázkou však ostáva, ako takémuto konaniu zabrániť a či právo by vôbec malo regulovať tieto otázky. Sme toho názoru, že právo by v tomto prípade malo prenechať pole pôsobnosti regulácie spoločenských vzťahov na iné entity. V tomto kontexte vychádzame z doktrinálneho vymedzenia modalít regulácie spoločenských vzťahov podľa profesora Lessiga.[88] Profesor Lessig vychádzal z toho, že právo vzhľadom na svoju nemennosť a často pomalú reakciu na reguláciu spoločenských vzťahov predpisov v porovnaní s dynamikou rozvoja nových technológií. nie je vždy

[85] KROLL, J. - HUEY, J. - BAROCAS, S. - FELTEN, E.- REIDENGERG, J. - ROBINSON, D. - YU, H.: Accountable Algorithms *In University of Pennsylvania Law Review, Vol. 165*, s. 43-44.

[86] Tamže, s. 44.

[87] Pozri viac BAROCAS, S. – SELBST, A.: Big Data's Disparate Impact *In 104 Calif. L. Rev, 2016*, s. 692-693.

[88] LESSIG, L.: The Laws of Cyberspace. Draft 3. 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (dostupné 20.12.2017) a LESSIG, L. :. Code: And other Laws of Cyberspace version 2.0. 2. vydanie.. Basic books, 2006.

najvhodnejšou formou regulácie a z tohto dôvodu definoval ďalšie tri modality – morálne normy (etika), trh a architektúru (kód). Z hľadiska zamedzenia algoritmov s predsudkami je vhodne obrátiť pozornosť na architektúru ako modalitu regulácie spoločenských vzťahov. Pod architektúrou v tomto zmysle je potrebné si predstaviť také nastavenie predmetov, ktoré obsahujú nejakú normu a nemožno ju v zásade porušiť napr. kruhový objazd alebo nemožnosť vidieť cez stenu. Z hľadiska technológií túto architektúru reprezentuje kód, ktorý sa odzrkadľuje v technických limitoch softwaru a hardwaru. Na možné riešenia eliminácie predsudkoch v algoritmoch poukazujú aj autori diskutovanej štúdie[89] a z tohto dôvodu považujeme za vhodné túto problematiku nechať na reguláciu prostredníctvom kódu, ktorý by minimalizoval riziko vytvorenia rozhodnutia s predsudkom alebo zaujatosťou s diskriminačným efektom.

3.3. Aplikácia predpovede (právo nebyť predmetom individuálneho automatizovaného rozhodovania)

Policajná smernica podobne ako GDPR upravuje problematiku automatizovaného individuálneho rozhodovania. Na tomto mieste považujeme za vhodné charakterizovať rozdiel medzi automatizovaným individuálnym rozhodovaním a profilovaním vo všeobecnosti. Podľa stanoviska Pracovnej skupiny článku 29 týkajúceho sa profilovania a automatizovaného individuálneho rozhodovania (ďalej len „**Stanovisko**“)[90] možno uviesť tri odlišné prípady: (i) všeobecné profilovanie, (ii) rozhodnutie na základe profilovania a (iii) rozhodnutie urobené výlučne automatizovaným spracúvaním osobných údajov vrátane profilovania, ktoré má právne účinky na dotknutú osobu, ktoré sa dotknutej osoby týkajú alebo dotknutú osobu podobne významne ovplyvňujú. Profilovanie je legálne definované v článku 3 bode 4 Policajnej smernice ako *„akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.“* Profilovaním je napríklad vytvorenie

[89] KROLL, J. - HUEY, J. - BAROCAS, S. - FELTEN, E.- REIDENGERG, J. - ROBINSON, D. - YU, H.: Accountable Algorithms *In University of Pennsylvania Law Review, Vol. 165*, s. 45 a nasl.

[90] Profiling definíca

profilu užívateľa e-shopu na základe predošlých nákupov a jeho správania vo virtuálnom priestore. O rozhodnutie na základe profilovania pôjde v prípade, ak údaje o žiadateľovi o úver spracuje algoritmus, ktorý na základe týchto dát vydá odporúčanie, či úver poskytnúť alebo nie, avšak konečné rozhodnutie urobí zamestnanec banky. Rozhodnutie urobené výlučne automatizovaným spracúvaním osobných údajov vrátane profilovania, ktoré má právne účinky na dotknutú osobu, ktoré sa dotknutej osoby týkajú alebo dotknutú osobu podobne významne ovplyvňujú ilustruje situácia, keď by žiadateľovi o úver došlo rozhodnutie o (ne)poskytnutí úveru priamo od algoritmu, ktorý o ňom spracúval dáta a sám rozhodol o výsledku jeho žiadosti.[91] Stanovisko zároveň potvrdzuje, že rutinná ľudská intervencia môže stále znamenať, že rozhodnutie je urobené výlučne automatizovanými prostriedkami.[92] Napríklad ak policajné zložky používajú algoritmus na predpovedanie budúcej kriminality a ten vyhotovuje správu, na základe ktorej sú policajné hliadky rozmiestnené v rámci mesta alebo vykonávajú zásahy bez toho, aby túto správu vyhodnotil človek, pôjde o prípad individuálneho automatizovaného rozhodovania. Avšak ak by takúto správu následne vyhodnocoval človek, ktorý by následne určil ktoré predpovede uplatní v praxi a ktoré nie, domnievame sa, že v takomto prípade by už nešlo o individuálne automatizované rozhodovanie.

Na prvé dva prípady sa aplikuje všeobecná právna úprava týkajúca sa ochrany osobných údajov v GDPR a Policajnej smernice. V treťom prípade je potrebné zohľadňovať špecifické požiadavky na takýto typ spracovateľskej operácie uvedené v článku 22 GDPR a článku 11 Policajnej smernice. Ani jeden z vyššie uvedených typov spracúvania osobných údajov nie je zakázaný, je však potrebné splniť požiadavky kladené na ich legálne vykonanie.

V zmysle článku 11 ods. 1 Policajnej smernice platí, že členské štáty EÚ vo svojich právnych poriadkoch ustanovia *„aby rozhodnutie založené výlučne na automatizovanom spracúvaní, vrátane profilovania, ktoré má pre dotknutú osobu nepriaznivé právne účinky alebo významné dôsledky, bolo zakázané, pokiaľ nie je prípustné podľa práva Únie alebo práva členského štátu, ktoré sa vzťahuje na prevádzkovateľa a ktorými sú ustanovené primerané záruky ochrany práv a slobôd dotknutej osoby, aspoň právo na ľudský zásah zo strany prevádzkovateľa.“*[93] Automatizované individuálne rozhodovanie možno ilustrovať

[91] Tamže, s. 9.

[92] Tamže, s. 21.

[93] Slovenská implementácie v Zákone o ochrane osobných údajov znie nasledovne: § 66 ods. 1 *„Rozhodnutie príslušného orgánu, ktoré má na dotknutú osobu nepriaznivé právne účinky, nesmie byť založené výlučne na automatizovanom spracúvaní osobných údajov vrátane*

na príklade, keď algoritmus na základe dostupný dát predpovedá, že konkrétna osoba môže spáchať trestný čin a táto predpoveď je tak „silná," že zložky policajného zboru sa rozhodnú preventívne potenciálneho páchateľa upozorniť prípadne ho začať monitorovať alebo obmedziť na jeho osobnej slobode.

Predmetný inštitút reaguje na možnosti využívania nových technológií pri práci policajných zborov ako napr. dolovanie dát (*data mining)*, prediktívna analýza údajov či kombinácie rôznych datasetov. Zároveň je nutné poznamenať, že článok 11 Policajnej smernice je nevyhnutné čítať v kontext ďalších ustanovení Policajnej smernice.[94]

Aplikácia článku 11 Policajnej smernice však nenastáva automaticky, keď ide o policajné profilovanie. Článok 11 sa aplikuje iba vtedy, keď profilovanie je následne využité na vykonanie rozhodnutia, ktoré má pre dotknutú osobu nepriaznivé právne účinky alebo významné dôsledky. Nepriaznivé právne účinky a významné dôsledky nemajú svoju legálnu definíciu v Policajnej smernici ani v Zákone o ochrane osobných údajov. Bygrave ich definuje ako dôsledky, ktoré menia alebo určujú práva a povinnosti jednotlivca.[95] Ak by sa napríklad policajné zložky v Slovenskej republike rozhodli sčítať rómsku populáciu v krajine, nešlo by o automatizované individuálne rozhodovanie. Ak by však už policajné zložky tieto údaje vložili do algoritmu, ktorý by dáta analyzoval a výsledkom by boli kriminologické profily jednotlivcov, táto situácia by mohla byť subsumovaná pod dikciu článku 11 Policajnej smernice.

Článok 11 Policajnej smernice je komponovaný ako zákaz automatizovaného individuálneho rozhodovanie s derogáciu, ak *„nie je prípustné podľa práva Únie alebo práva členského štátu, ktoré sa vzťahuje na prevádzkovateľa a ktorými sú ustanovené primerané záruky ochrany práv a slobôd dotknutej osoby, aspoň právo na ľudský zásah zo strany prevádzkovateľa."* Túto požiadavku ďalej interpretuje recitál 38 Policajnej smernice: *„Dotknutá osoba by mala mať právo na to, aby sa na ňu nevzťahovalo rozhodnutie hodnotiace osobné aspekty s ňou*

profilovania, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, neustanovuje inak. Osobitým predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, musia byť ustanovené primerané záruky ochrany práv dotknutej osoby, najmä právo na overenie rozhodnutia nie automatizovaným spôsobom zo strany príslušného orgánu."

[94] Napr. základné zásady spracúvania osobných údajov podľa článku 4 Policajnej smernice, spracúvanie osobitných kategórií osobných údajov v zmysle článku 10 Policajnej smernice alebo práva dotknutých osôb podľa článkov 13 až 17 Policajnej smernice.

[95] BYGRAVE, L.: Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling In Computer Law & Security Review, 17.1. (2001), s. 17-24.

súvisiace, ktoré je založené výlučne na automatizovanom spracúvaní a ktoré má pre túto osobu nepriaznivé právne účinky alebo významné dôsledky. V každom prípade by takéto spracúvanie ***malo podliehať primeraným zárukám vrátane poskytnutia určitých informácií dotknutej osobe a právu na ľudský zásah, najmä vyjadriť svoj názor, právu dostať vysvetlenie k rozhodnutiu dosiahnutému po takomto posúdení alebo napadnúť toto rozhodnutie****.“* Je otázne, či požiadavku prípustnosti podľa práva EÚ alebo národného právneho poriadku spĺňajú súčasné znenia Zákona o ochrane osobných údajov, Zákona o policajnom zbore či Trestného poriadku alebo je potrebná špecifickejšia právna úprava.[96] Tieto právne predpisy sú skôr všeobecné a neobsahujú žiadne špecifiká týkajúce sa policajného profilovania. Jediným indikátorom je ustanovenie § 69a ods. 4: *„Policajný zbor nezlikviduje osobné údaje, ktoré sa uchovávajú v spisovom materiáli a nespracúvajú sa automatizovane.“* Z tohto ustanovenia je možné vyvodiť, že právna úprava v Zákone o policajnom zbore *a priori* ráta s automatizovaným spracúvaním osobných údajov.

Problematickým sa zdá aj ustanovenie implementácie tzv. primeraných záruk, ktoré v zmysle demonštratívneho výpočtu recitálu 38 zahŕňa informačnú povinnosť voči dotknutej osobe a právo na ľudskú intervenciu, ktoré obsahuje právo dostať vysvetlenie týkajúce sa automatizovaného rozhodovacieho procesu, právo vyjadriť svoj názor na automatizované individuálne rozhodnutie prípadne toto rozhodnutie napadnúť. Ako pragmaticky poukazujú niektoré autori, právo na vysvetlenie automatizovaného rozhodnutia sa však často dostane do konfliktu s právnou ochranou samotného algoritmu v zmysle ochrany obchodného tajomstva alebo práv duševného vlastníctva.[97] Zároveň pri práci policajných zložiek nie je vhodné, aby široká verejnosť poznala princíp fungovania algoritmu predpovedajúceho potenciálnu trestnú činnosť, keďže by to mohlo ohroziť jeho fungovanie a účel výkonu činnosti policajných zložiek pri prevencií prípadne vyšetrovaní protiprávnych konaní.

Článok 11 ods. 2 obsahuje všeobecný zákaz založenia automatizovaného individuálneho rozhodnutia na osobitných kategóriách osobných údajov (tzv. citlivé osobné údaje),[98] pokiaľ sa neuplatňujú vhodné opat-

[96] Zákon č. 301/2005 Z. z. Trestný poriadok.

[97] SAJFERT, J. – QUINTEL, T.: Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, s. 10 (dostupné 1.8.2019).

[98] Článok 10 Policajnej smernice tieto údaje definuje ako osobné údaje, osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov,

renia na zabezpečenie práv a slobôd a oprávnených záujmov dotknutej osoby. Tieto záruky môžu zahŕňať rôzne bezpečnostné opatrenia prípadne zabezpečenie obmedzeného prístupu k týmto dátam.[99] Ako príklad tohto zákazu možno uviesť profilovanie jednotlivcov na základe ich náboženského vyznania a následne robenie rozhodnutí algoritmom. Predmetné profilovanie je článok 11 ods. 2 Policajnej smernice zakázané. Situácia by však bola odlišná, ak by v takom prípade bolo prítomné dôvodné podozrenie, že člen fanatickej náboženskej skupiny môže spáchať teroristický útok. V týchto prípadoch by bolo možné automatizované individuálne rozhodovanie na základe citlivých osobných údajov vykonať.

Článok 11 ods. 3 upravuje absolútny zákaz profilovania vedúceho k diskriminácií na základe osobitných kategórií osobných údajov. Na možnosť algoritmu s predsudkami sme poukázali už v predchádzajúcich častiach predkladaného príspevku. Predmetné ustanovenie len zvýrazňuje možnosť diskriminácie pri policajnom profilovaní v dôsledku využívania sledovacích mechanizmov, nových technológií ako prediktívnej analýzy údajov a podobne.[100]

Článok 11 Policajnej smernice tak bude podľa nášho názoru zohrávať veľkú úlohu pri policajnom profilovaní. Otvorenou otázkou ostáva aplikácie predmetného článku v rámci požiadaviek na zakotvení v práve EÚ alebo národnom právnom poriadku. Ďalším problematickým aspektom je právo na vysvetlenie, ktorými by mala disponovať dotknutá osoba a jeho kolízia s činnosťou policajných zložiek či ochranou práva duševného vlastníctva.

Záver

Policajné profilovanie už viac nie je doménou vedecko-fantastickej literatúry či filmu. Svoje uplatnenie nachádza v reálnej praxi policajných zložiek po celom svete. V prvej časti štúdie sme sa smažili čitateľovi poskytnúť základný prehľad fungovania policajného profilovania, ktoré je vo väčšine prípadov založené na báze využívania prediktívnej analýzy údajov. Berúc do úvahy uplatnenie tejto metódy v Spojených štátoch, existujú tri modely využitia predmetnej metódy a to so zameraním na miesta spáchania majetkovej kriminality, miest spáchania

biometrických údajov na účely individuálnej identifikácie fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

[99] Pozri recitál 37 Policajnej smernice.

[100] Pozri viac FISHER, L.: Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups *In Arizona Law Review, 46 (2004*), s. 621.

násilnej kriminality alebo na osoby zapojené do kriminálnych aktivít. Prirodzene, najväčšie právne riziká súvisia práve s posledným typom využitia prediktívnej analytiky. Úvodnú časť štúdie uzatvára charakteristika použitia policajného profilovania v Spojených štátoch amerických, Českej republiky a Rakúsku. Slovenská republika podľa verejne dostupných zdrojov túto metódu zatiaľ nevyužíva, avšak disponuje dostatočnou dátovou základňou pre jej budúce uplatnenie.

Druhá časť štúdie sa venuje identifikácii základných trecích plôch použitia tejto metódy v kontexte základných ľudských práv a slobôd v zmysle Dohovoru. Základné aplikačné problémy podľa empirických skúsenosti tvoria zvýšenie rasového profilovania, ohrozenie súkromia, výrazné spoliehanie sa na nové technológie a nepochopenie kontextu informácie. Vzhľadom na vyššie uvedené sú tak ohrozené právo na súkromie, zákaz nediskriminácie a právo na spravodlivé súdne konanie. Právo na súkromie v zmysle článku 8 Dohovoru má pomerne široký rozsah a možno pod neho subsumovať viaceré situácie, kde môže nastať jeho porušenie, prácu policajných zložiek nevynímajúc. Toto tvrdenie bolo opakovane potvrdené aj Európskym súdom pre ľudské práva vo viacerých rozhodnutiach. Na úrovni Európskej únie predstavuje základný právny rámec Policajná smernica, ktorá upravuje spracúvanie osobných údajov pri vyšetrovaní trestných činov. Pri policajnom profilovaní môže dochádzať aj ku porušenie zákazu nediskriminácie podľa článku 14 Dohovoru. Dokumentované sú viaceré prípady, keď k tomu skutočne došlo, na čo upozorňuje aj judikatúra ESĽP. Posledným právom, ktoré je v rámci druhej časti analyzované je právo na spravodlivé súdne konanie podľa článku 6 Dohovoru.

Tretia časť sa venuje policajnému profilovaniu v kontexte Policajnej smernice, ktorá pôsobí ako *lex specialis* voči GDPR. V tejto časti je v prvom rade zvýraznené, že na jej aplikáciu musí ísť o osobné údaje, čo bude častokrát v praxi splnené, keďže policajné zložky majú prístup k neverejným databázam na identifikáciu jednotlivých osôb. V rámci tejto časti sme poukázali na možné úskalia vymedzenia účelu a právneho základu na spracúvanie osobných údajov, potreby vykonania posúdenia vplyvu či niektorých špecifík Policajnej smernice a špecificky navrhnutej a štandardnej ochrany osobných údajov. V kontexte kreovania konkrétnej predpovede pri profilovaní je dôraz daný na možnosť tzv. algoritmu s predsudkami, keďže prax ukazuje, že môže dochádzať k situácií, v ktorej algoritmus produkuje výsledky, ktoré majú diskriminačný charakter. Riešením by mohlo byť implementovanie špecifickej technológie, ktorá by vedela rozpoznať predsudok. V závere tretej časti je analyzovaný inštitút automatizovaného individuálneho rozhodovania podľa článku 11 Policajnej smernice. Otázky vyvoláva najmä jeho nut-

nosť a konkrétnosť úpravy v národnom právnom poriadku či práve EÚ a reálna vynútiteľnosť práva na vysvetlenie dotknutej osoby pri policajnom profilovaní.

Použitá literatúra

Monografie, učebné texty, štúdie

1. BALGA, J.: Polícia, etika a právo. 1. vydanie. Bratislava: Akadémia Policajného zboru v Bratislave, 1998.
2. BAUMAN, Z. – LYON, D.: Tekutý dohled. Praha : Broken books, 2013.
3. DRGONEC, J.: Ústava Slovenskej republiky. Veľký komentár. Praha: C.H.Beck, 2015.
4. GÁBRIŠ, T. *Kognitívne sklony v právnej vede a právnej prax* In GÁBRIŠ, T a kol. : Nedogmatická právna veda. Od marxizmu po behaviorálnu ekonómiu. Wolters Kluwer, Praha, 2018, s. 229 - 247.
5. LESSIG, L.: Code: And other Laws of Cyberspace version 2.0. 2. vydanie.. Basic books, 2006.
6. MCCUE, C.: Data Mining and Predictive Analysis Intelligence Gathering and Crime Analysis Second Edition. Butterworth-Heinemann, 2015.
7. PERRY, W. – MCINNIS, B. – PRICE, C. – SMITH, S. – HOLLYWOOD, J. : Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations, https://www.rand.org/pubs/research_reports/RR233.html (dostupné 6.9.2018).
8. SCHABAS, W.: The European Convention on Human Rights. A commentary. 1st edition. Oxford University Press, 2015.
9. ŠINSKÝ, M. (2010). Taxonómia sklonov k chybám. In BAČOVÁ , V. (ed.), Rozhodovanie a usudzovanie. Pohľady psychológie a ekonómie I. Bratislava: Ústav experimentálnej psychológie SAV, s. 162.
10. ZHANG, A.: Data Analytics: Practical Guide to Leveraging the Power of Algorithms, Data Science, Data Mining, Statistics, Big Data, and Predictive Analysis to Improve Business, Work, and Life. Distribuované Amazon Digital Services LLC, 2017. (EPUB verzia).

Periodiká

11. BAROCAS, S. – SELBST, A.: Big Data's Disparate Impact *In 104 Calif. L. Rev, 2016*, s. 692-693.
12. FERGUSON, A.: Policing Predictive Policing *In Washington University Law Review, vol. 94, n. 5*, 2017.

13. MADDEN, M. – GILMAN, M. – LEVY, K. – MARWICK, A.: Privacy, poverty, and Big data: A matrix of vulnerabilities for poor americans In 95 Washington University Law Review, Vol. 53 (2017).
14. SCHWARTZ, P.: Data processing and Government Administration: The Failure of the American Legal Response to Computer *In 43 Hastings Law Journal 1992*, s. 1321 a 1342.
15. KROLL, J. – HUEY, J. – BAROCAS, S. – FELTEN, E. – REIDENGERG, J. – ROBINSON, D. – YU, H.: Accountable Algorithms In University of Pennsylvania Law Review, Vol. 165.

Internetové zdroje

16. LESSIG, L.: The Laws of Cyberspace. Draft 3. 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (dostupné 1.8.2019).
17. SAJFERT, J. – QUINTEL, T. : Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873, (dostupné 1.8.2019).
18. https://www.floridatechonline.com/blog/criminal-justice/4-problems-with-predictive-policing/ (dostupné 1.8.2019).
19. http://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/be-cautious-about-data-driven-policing (dostupné 1.8.2019).
20. http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist (dostupné 1.8.2019).
21. https://www.fbi.gov/news/stories/2016-crime-statistics-released (dostupné 1.8.2019).
22. http://www.predpol.com/ (dostupné 1.8.2019).
23. https://www.joanneum.at/en/policies/reference-projects/cripa-crime-predictive-analytics/ (dostupné 1.8.2019).
24. https://www.minv.sk/?ESISPZ_MV (dostupné 1.8.2019).
25. https://www.minv.sk/?Mapy_trestnych_cinov_v_Slovenskej_republike_za_rok_2016 (dostupné 1.8.2019).

Právne predpisy

26. Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV.
27. Návrh Nariadenia Európskeho Parlamentu a Rady (EÚ) o rámci pre voľný tok iných ako osobných údajov v Európskej únii COM(2017) 495 final 2017/0228(COD).

28. Rada Európskej únie (2008), rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce (rámcové rozhodnutie o ochrane údajov), Ú. v. EÚ L 350, 2008.
29. Charta základných práv EÚ.
30. Dohovor o ochrane základných ľudských práv a slobôd.
31. 460/1992 Zb. Ústava Slovenskej republiky.
32. Zákon č. 300/2005 Z. z. Trestný zákon.
33. Zákon č. 171/2003 Z. z. o policajnom zbore.
34. Zákon č. 18/2018 Z. z. o ochrane osobných údajov.

Judikatúra

35. PL. ÚS 10/2014-78. Nález z 29. apríla 2015.
36. Rozsudok ESĽP vo veci Sisojeva a ostatní proti Lotyšsku, 60654/00.
37. Rozsudok ESĽP vo veci Saman proti Turecku, č. 35292/05.
38. Rozsudok ESĽP vo veci G.S.P. proti Rumunsku, č. 20899/03.
39. Rozsudok ESĽP vo veci Raimondo proti Taliansku z 22. Februára 1994.
40. Rozsudok ESĽP Glor proti Švajčiarsku, no. 13444/04.
41. Rozsudok ESĽP, S. a Marper/Spojené kráľovstvo, č. 30562/04 a 30566/04, 4. decembra 2008.
42. Rozsudok ESĽP, B.B./Francúzsko, č. 5335/06, 17. decembra 2009.
43. Rozsudok ESĽP, Vetter/Francúzsko, č.59842/00, 31. mája 2005.
44. Rozsudok ESĽP vo veci Leander v Švédsko zo dňa 26. marca 1987.
45. Rozsudok ESĽP vo veci Rotaru v Rumunsko č. 28341/95.
46. Rozsudok ESĽP vo veci Amann v Švajčiarsko č. 27798/98.

Ostatné

47. CAVOUKIAN, A.: *Privacy by Design – The Seven Foundational Principles*, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (dostupné 18.3.2018).
48. Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
49. Appendix to Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration, https://rm.coe.int/16807096b9 (dostupné 27.1.2018).
50. Explanatory Report to the Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms.